UNIVERSITY OF TRENTO
Faculty of Law

lawtech

Trento Law and Technology Research Group

Student Paper n. 77

L'ENFORCEMENT DEL DIRITTO D'AUTORE E LA TUTELA DEI DATI PERSONALI: IL NUOVO ART. 17 DIR. 2019/790

NICCOLÒ BULLATO

COPYRIGHT © 2022 NICCOLÒ BULLATO

This paper can be downloaded without charge at:

The Trento Law and Technology Research Group Student Papers Series Index
https://lawtech.jus.unitn.it/main-menu/paper-series/student-paper-series-of-the-trento-lawtech-research-group/2/

Questo paper

Copyright © 2022 NICCOLÒ BULLATO

è pubblicato con Licenza Creative Commons "Attribuzione – Condividi allo stesso modo 4.0 Internazionale (CC-BY-SA 4.0)" Maggiori informazioni circa la licenza all'URL: https://creativecommons.org/licenses/by-sa/4.0/legalcode.

About the author

Niccolò Bullato (niccolo.bullato@gmail.com) graduated in Law at University of Trento under the supervision of Prof. Roberto Caso (June 2022).

The opinion stated in this paper and all possible errors are the Author's only.

KEY WORDS

Copyright – Copyright Directive – Privacy – Automatic Content Recognition – Balancing Rights

Sull'autore

Niccolò Bullato (niccolo.bullato@gmail.com) ha conseguito la Laurea in Giurisprudenza presso l'Università di Trento con la supervisione del Prof. Roberto Caso (Giugno 2022).

Le opinioni e gli eventuali errori contenuti sono ascrivibili esclusivamente all'autore.

PAROLE CHIAVE

Diritto d'autore – Direttiva copyright – Privacy – Automatic Content Recognition – Bilanciamento

ABSTRACT

This paper aims to proceed with a careful analysis of the delicate balance between rights in the field of copyright enforcement. The following considerations are justified by a strong interest in current events, namely the transposition of the new European legislation that involves copyright: Directive (EU) 2019/790 of 17 April 2019 "*on copyright and related rights in the digital single market*". The European regulatory framework has been nationally transposed with Legislative Decree 8 November 2021, n. 177, effective from 12 December 2021.

Considering, with an initial analysis, the provisions of a specific article of the aforementioned Directive, the seventeenth, it immediately emerged that it poses specific doubts of legitimacy in light of fundamental rights, as protected by the Charter of Fundamental Rights of The European Union. Particularly, it seems to clash with the right of respect for private and family life, with the protection of personal data and, in a word, with the right to "*privacy*". A peculiar conflict has therefore been selected, a source of friction between the interests underlying copyright enforcement and those of users' privacy.

Although a "right to privacy" is a recent introduction, or conquest, of contemporary legal society, since an origin of the same cannot be found before the end of the nineteenth century, this paper will try, in its first section, to identify, with an anecdotal approach, some curious historical events demonstrating how, in reality, the copyright enforcement has, since its origins, shown an aptitude to enter into conflict with other instances, which we would now include into the "right to privacy". History can provide a solid basis for understanding modern dynamics, of instances that, from the *Stationers* of the sixteenth-century London, are proposed, in a digital key, in the lobbying activities that led to the approval of the new Directive 2019/790. These protection strategies, evolved with the change of technology, maintained a deep connection with their historical roots of emergence. Therefore, this paper will report stories of "pirates", of business and commerce, of self-defense and of private police bodies that will be transformed from *physical* into *bits*.

From the analogical world outlined in the first chapter, this paper will proceed to the digital one represented by the "*file-sharing*" on "*peer-to-peer*" networks. Taking up the historical trends, this paper will highlight the strategies that emerge in the digital world so that copyright holders can assert their needs in the dynamics of the Web, defining all the instances in which the copyright enforcement clashes with the importance of privacy protection. In this, the comparative analysis of both US and Euro-Italian regulations and court rulings will be particularly useful.

Among the strategies implemented by copyright holders for the enforcement of their rights, one is worthy of independent discussion, namely the use of *Digital Rights Management* systems. The third chapter will therefore be focused on them and on their relations with the protection of personal data, recalling technologies such as *hashing*, *watermarking* or *fingerprinting*, anticipating considerations on that particular form of enforcement through electronic systems represented by the *Automatic Content Recognition*, connecting to the fourth chapter.

Ultimately, this paper will focus on the analysis of Directive 2019/790, and particularly on its article 17, believing that all the considerations in terms of balancing rights carried out for the entire extension of this paper will merge into this provision. An attempt will then be made to provide interpretative suggestions of the new legislation, in order to highlight the

shadows and criticalities in relation to the compatibility with the fundamental rights of the European Charter.

This paper will therefore try to highlight at least the complexities that legal practitioners and citizens of the world are called to face when they approach the dynamics of the digital world, without claiming to be able to trace any magical criterion that solves the complexity of reality or an effective algorithm that reduces legal thought to a sum of numbers. At most, this paper will try to emphasize the most problematic characteristics that can be found in the clash between the copyright enforcement and the protection of users' privacy, hoping to provide useful considerations to those who rule the world, legislators, courts, and economic operators, aimed at suggesting that solutions to these problems cannot be found by forgetting the achievements of modern civilization in the field of fundamental rights. The truth, according to Ann Cavoukian, is that privacy is the foundation of our freedom: if we value freedom, we value privacy[1].

[1] Ann Cavoukian, interviewed by Forbes, in H. JONES, *Will Privacy First Be The New Normal? An Interview With Privacy Guru, Dr. Ann Cavoukian*, in *Forbes.com*, 13 august 2018, accessible at: «https://www.forbes.com/sites/cognitiveworld/2018/08/13/will-privacy-first-be-the-new-normal-an-interview-with-privacy-guru-ann-cavoukian/?sh=132b577925dc» (Last access: 10 may 2022).

ABSTRACT

Il presente elaborato intende procedere ad un'attenta analisi del delicato bilanciamento fra diritti richiesto ogniqualvolta l'interprete voglia procedere ad affermare un qualcosa di significante in materia di *enforcement* del diritto d'autore. Le considerazioni che seguiranno sono giustificate da un interesse di stretta attualità, ossia il recepimento della nuova normativa che ha coinvolto il diritto d'autore: la Direttiva (UE) 2019/790 del 17 aprile 2019 "*sul diritto d'autore e sui diritti connessi nel mercato unico digitale*". L'articolato normativo europeo è stato trasposto nazionalmente con il Decreto Legislativo 8 novembre 2021, n. 177, in vigore dal 12 dicembre 2021.

Nel considerare, con una prima analisi, quanto dispone uno specifico articolo della citata Direttiva, il diciassettesimo, è subito emerso come esso ponga peculiari interrogativi di legittimità alla luce dei diritti fondamentali, come tutelati dalla Carta di Nizza, ed in particolare con il diritto alla tutela della vita familiare e personale, al corretto trattamento dei dati personali e, in una parola, alla "privacy". È stato dunque prescelto un peculiare conflitto che si avverte quotidianamente con rinnovata prepotenza, quel punto di frizione fra gli interessi sottesi al diritto d'autore e quelli alla privacy degli utenti.

Sebbene non si nasconda che un "diritto alla privacy" sia una recente introduzione, o conquista, della società giuridica contemporanea, non potendosi rinvenire un'origine dello stesso prima del finire del XIX secolo, si tenterà, nella prima parte della presente dissertazione, di individuare, con approccio aneddotico, alcune vicende o momenti curiosi della storia che dimostrino come, in realtà, *l'enforcement* del diritto d'autore abbia sin dalla sua origine mostrato un'attitudine ad entrare in conflitto con altre istanze, che noi oggi faremmo ricadere sotto l'alveo del diritto alla riservatezza. Si è infatti convinti che la storia possa fornire una solida base di comprensione di moderne dinamiche, di istanze che, dagli *Stationer* della Londra seicentesca, si ripropongono, in chiave digitalizzata, nelle attività lobbistiche che hanno condotto all'adozione della nuova Direttiva 2019/790. Sono linee di tendenza che si muovono *nell'enforcement* del diritto d'autore sin dalle sue primissime origini e strategie di tutela che, evolvendosi con il cambio di tecnologia, mantengono una profonda connessione con le radici storiche di loro emersione. Quella che verrà segnalata sarà una storia di privati e di "pirati", del mondo degli affari e del commercio, di autotutela e di corpi di polizia privata che da fisici si trasformano in *bit*.

Dal mondo analogico che si osserverà tratteggiato nel primo capitolo, si passerà a quello digitale rappresentato, in emblema, dal fenomeno del "*file-sharing*" su reti "*peer-to-peer*". Riprendendo le tendenze storiche, si avrà modo di notare quali strategie emergano nel mondo digitale affinché i titolari dei diritti d'autore possano far valere le loro esigenze nella dinamica del Web, segnalando tutti i momenti in cui *l'enforcement* del diritto d'autore si scontra con l'importanza della tutela della privacy. In questo, particolare utilità deriverà dall'analisi comparata delle normative e delle pronunce giurisprudenziali tanto statunitensi quanto euro-italiane.

Fra le strategie attuate dai titolari dei dritti d'autore per *l'enforcement* delle loro prerogative, se ne segnala una meritevole di autonoma trattazione, ossia il ricorso ai sistemi di *Digital Rights Management*. Su di essi e sulle loro relazioni con il diritto alla privacy ed alla tutela dei dati personali si avrà modo di dedicarsi nel corso del terzo capitolo in cui, richiamando tecnologie quali la crittografia, il *watermarking* od il *fingerprinting,* si anticiperanno

considerazioni su quella peculiare forma di *enforcement* mediante sistemi elettronici rappresentata dall'*Automatic Content Recognition*, ponte di collegamento con il quarto capitolo.

In ultima istanza, infatti, si è deciso di concentrarsi sull'analisi della Direttiva 2019/790, sotto l'angolo, tanto privilegiato quanto esclusivo, dell'articolo 17, ritenendo che in esso si congiungano e si fondano tutte le considerazioni in chiave di bilanciamento compiute per l'intera estensione del presente elaborato. In tale contesto si tenterà di fornire indicazioni interpretative della nuova normativa, per poi metterne in luce le ombre e le criticità in relazione alla compatibilità con i diritti fondamentali della Carta di Nizza.

In questo contributo, dunque, si tenterà di mettere in luce quantomeno le complessità che gli operatori del diritto, ed i cittadini del mondo, sono chiamati ad affrontare ove si accostino alle dinamiche che permeano il mondo digitale, senza avere la pretesa di poter tracciare alcun magico criterio che risolva la complessità del reale od un efficace algoritmo che riduca il pensiero giuridico ad una somma di numeri. Al più si tenterà di porre l'accento su quali sono le caratteristiche più problematiche che si rinvengono nello scontro fra *l'enforcement* del diritto d'autore e la tutela della privacy degli utenti, nella speranza di fornire delle utili considerazioni volte a non far dimenticare a coloro che reggono il mondo, legislatori, Corti, e operatori economici, che le soluzioni non possono essere trovate dimenticandosi delle conquiste della moderna civiltà in campo di diritti fondamentali. La verità, secondo Ann Cavoukian, è che la privacy è il fondamento della nostra libertà: se vogliamo dunque dare il giusto valore alla libertà, dobbiamo darlo alle esigenze della privacy[2].

[2] Così si è espressa Ann Cavoukian, intervistata da Forbes, le cui dichiarazioni sono rinvenibili presso: H. JONES, *Will Privacy First Be The New Normal? An Interview With Privacy Guru, Dr. Ann Cavoukian*, in *Forbes.com*, 13 agosto 2018, liberamente accessibile presso: «https://www.forbes.com/sites/cognitiveworld/2018/08/13/will-privacy-first-be-the-new-normal-an-interview-with-privacy-guru-ann-cavoukian/?sh=132b577925dc» (Ultimo accesso: 10 maggio 2022).

INDICE

INTRODUZIONE

Il presente elaborato intende procedere ad un'attenta analisi del delicato bilanciamento fra diritti richiesto ogniqualvolta l'interprete voglia procedere ad affermare un qualcosa di significante in materia di *enforcement* del diritto d'autore. Le considerazioni che seguiranno sono giustificate da un interesse di stretta attualità, ossia il recepimento della nuova normativa che ha coinvolto il diritto d'autore: la Direttiva (UE) 2019/790 del 17 aprile 2019 "*sul diritto d'autore e sui diritti connessi nel mercato unico digitale*". L'articolato normativo europeo è stato trasposto nazionalmente con il Decreto Legislativo 8 novembre 2021, n. 177, in vigore dal 12 dicembre 2021.

Nel considerare, con una prima analisi, quanto dispone uno specifico articolo della citata Direttiva, il diciassettesimo, è subito emerso come esso ponga peculiari interrogativi di legittimità alla luce dei diritti fondamentali, come tutelati dalla Carta di Nizza, ed in particolare con il diritto alla tutela della vita familiare e personale, al corretto trattamento dei dati personali e, in una parola, alla "privacy". È stato dunque prescelto un peculiare conflitto che si avverte quotidianamente con rinnovata prepotenza, quel punto di frizione fra gli interessi sottesi al diritto d'autore e quelli alla privacy degli utenti.

Sebbene non si nasconda che un "diritto alla privacy" sia una recente introduzione, o conquista, della società giuridica contemporanea, non potendosi rinvenire un'origine dello stesso prima del finire del XIX secolo, si tenterà, nella prima parte della presente dissertazione, di individuare, con approccio aneddotico, alcune vicende o momenti curiosi della storia che dimostrino come, in realtà, *l'enforcement* del diritto d'autore abbia sin dalla sua origine mostrato un'attitudine ad entrare in conflitto con altre istanze, che noi oggi faremmo ricadere sotto l'alveo del diritto alla riservatezza. Si è infatti convinti che la storia possa fornire una solida base di comprensione di moderne dinamiche, di istanze che, dagli *Stationer* della Londra seicentesca, si ripropongono, in chiave digitalizzata, nelle attività lobbistiche che hanno condotto all'adozione della nuova Direttiva 2019/790. Sono linee di tendenza che si muovono *nell'enforcement* del diritto d'autore sin dalle sue primissime origini e strategie di tutela che, evolvendosi con il cambio di tecnologia, mantengono una profonda connessione con le radici storiche di loro emersione. Quella che verrà segnalata sarà una storia di privati e di "pirati", del mondo degli affari e del commercio, di autotutela e di corpi di polizia privata che da fisici si trasformano in *bit*.

Dal mondo analogico che si osserverà tratteggiato nel primo capitolo, si passerà a quello digitale rappresentato, in emblema, dal fenomeno del "*file-sharing*" su reti "*peer-to-peer*". Riprendendo le tendenze storiche, si avrà modo di notare quali strategie emergano nel mondo digitale affinché i titolari dei diritti d'autore possano far valere le loro esigenze nella dinamica del Web, segnalando tutti i momenti in cui *l'enforcement* del diritto d'autore si scontra con l'importanza della tutela della privacy. In questo, particolare utilità deriverà dall'analisi comparata delle normative e delle pronunce giurisprudenziali tanto statunitensi quanto euro-italiane.

Fra le strategie attuate dai titolari dei dritti d'autore per *l'enforcement* delle loro prerogative, se ne segnala una meritevole di autonoma trattazione, ossia il ricorso ai sistemi di *Digital Rights Management*. Su di essi e sulle loro relazioni con il diritto alla privacy ed alla tutela dei dati personali si avrà modo di dedicarsi nel corso del terzo capitolo in cui,

richiamando tecnologie quali la crittografia, il *watermarking* od il *fingerprinting,* si anticiperanno considerazioni su quella peculiare forma di *enforcement* mediante sistemi elettronici rappresentata dall'*Automatic Content Recognition*, ponte di collegamento con il quarto capitolo.

In ultima istanza, infatti, si è deciso di concentrarsi sull'analisi della Direttiva 2019/790, sotto l'angolo, tanto privilegiato quanto esclusivo, dell'articolo 17, ritenendo che in esso si congiungano e si fondano tutte le considerazioni in chiave di bilanciamento compiute per l'intera estensione del presente elaborato. In tale contesto si tenterà di fornire indicazioni interpretative della nuova normativa, per poi metterne in luce le ombre e le criticità in relazione alla compatibilità con i diritti fondamentali della Carta di Nizza.

In questo contributo, dunque, si tenterà di mettere in luce quantomeno le complessità che gli operatori del diritto, ed i cittadini del mondo, sono chiamati ad affrontare ove si accostino alle dinamiche che permeano il mondo digitale, senza avere la pretesa di poter tracciare alcun magico criterio che risolva la complessità del reale od un efficace algoritmo che riduca il pensiero giuridico ad una somma di numeri. Al più si tenterà di porre l'accento su quali sono le caratteristiche più problematiche che si rinvengono nello scontro fra *l'enforcement* del diritto d'autore e la tutela della privacy degli utenti, nella speranza di fornire delle utili considerazioni volte a non far dimenticare a coloro che reggono il mondo, legislatori, Corti, e operatori economici, che le soluzioni non possono essere trovate dimenticandosi delle conquiste della moderna civiltà in campo di diritti fondamentali. La verità, secondo Ann Cavoukian, è che la privacy è il fondamento della nostra libertà: se vogliamo dunque dare il giusto valore alla libertà, dobbiamo darlo alle esigenze della privacy[3].

[3] Così si è espressa Ann Cavoukian, intervistata da Forbes, le cui dichiarazioni sono rinvenibili presso: H. JONES, *Will Privacy First Be The New Normal? An Interview With Privacy Guru, Dr. Ann Cavoukian*, in *Forbes.com*, 13 agosto 2018, liberamente accessibile presso: «https://www.forbes.com/sites/cognitiveworld/2018/08/13/will-privacy-first-be-the-new-normal-an-interview-with-privacy-guru-ann-cavoukian/?sh=132b577925dc» (Ultimo accesso: 10 maggio 2022).

CAPITOLO PRIMO

STORIA DI PIRATI: L'*ENFORCEMENT* DEL DIRITTO D'AUTORE E L'INVASIONE DELLA VITA PRIVATA

Su temi quali la nascita del diritto d'autore e le concezioni filosofiche ad essa sottese si sono cimentati alcuni fra gli autori più illustri della storia come Kant[4], Fichte[5], Manzoni[6] e persino Jefferson[7], sentendo tutti l'esigenza di giustificare l'esistenza del diritto d'autore e l'importanza della sua protezione. L'intento del presente elaborato è illustrare le principali dinamiche legate all'interazione fra il *copyright enforcement* e la tutela della *privacy* nella dimensione digitale. In prospettiva comparata, per comprendere sincronicamente le linee di forza di questa materia, non si può prescindere da alcune notazioni diacroniche, costituendo la storia preziosa testimonianza dell'emersione di tendenze ancora oggi riscontrabili. Se vogliamo credere a Cicerone, con una certa qual riverenza, e ricordare i suoi insegnamenti, rammentiamo che "*historia vero testis temporum, lux veritatis, vita memoriae, magistra vitae, nuntia vetustatis*"[8]. L'approccio storico di cui si vuole fregiare questa prima sezione intende procedere in forma aneddotica, richiamando alla memoria cinque vicende passate, particolarmente significative, che segnano lo svilupparsi di linee direttrici nell'*enforcement* del *copyright* che ancora oggi non hanno terminato di svolgere il loro ruolo nella sempiterna lotta di cui questa dissertazione si prefigge di dare contezza.

Si è variamente tentato di affermare lontane radici del diritto d'autore, forse vanamente. Senza entrare nel merito di copiosi dibattiti, per i fini del presente elaborato apparirebbe un mero vezzo stilistico ricercare presunte origini in passi del Digesto per il tramite di oscure interpretazioni di frammenti passati. Si correrebbe il rischio, infatti, come avverte Galgano[9], di incorrere in quello che egli ha brillantemente definito "falso diritto romano", in una tanto inesatta quanto ingenua attualizzazione dell'esperienza antica[10].

---

[4] I. KANT, *L'illegittimità della ristampa dei libri,* 1785, con traduzione di M. C. PIEVATOLO in *Bollettino telematico di filosofia politica,* liberamente accessibile presso: «https://btfp.sp.unipi.it/dida/kant_7/ar01s06.xhtml» (Ultimo accesso: 10 maggio 2022).

[5] J.G. FICHTE, *Prova dell'illegittimità della ristampa dei libri. Un ragionamento e una parabola,* con traduzione di M. C. PIEVATOLO in *Bollettino telematico di filosofia politica*, liberamente accessibile presso: «https://btfp.sp.unipi.it/dida/kant_7/ar01s06.xhtml» (Ultimo accesso: 10 maggio 2022).

[6] A. MANZONI, *Lettera al signor Professore Girolamo Boccardo intorno ad una questione di così detta proprietà letteraria, riveduta e corretta dall'autore,* Milano, Redaelli, 1861; per ulteriori informazioni e riferimenti bibliografici si veda anche L. MOSCATI, *Alessandro Manzoni avvocato: la causa contro le Monnier e le origini del diritto d'autore in Italia,* Bologna, 2017, accessibile liberamente presso: «https://www.academia.edu/35712441/Alessandro_Manzoni_avvocato_la_causa_contro_le_Monnier_e_le_origini_del_diritto_dautore_in_Italia» (Ultimo accesso: 10 maggio 2022).

[7] T. JEFFERSON, *Letter to Isaac McPherson,* Monticello, 13 agosto 1813, liberamente accessibile presso: «https://founders.archives.gov/documents/Jefferson/03-06-02-0322» (Ultimo accesso: 10 maggio 2022).

[8] CICERONE, De Oratore, II, 9, 36, traducendo: "La storia in verità è testimone dei tempi, luce della verità, vita della memoria, maestra di vita, messaggera dell'antichità".

[9] F. GALGANO, Storia del diritto privato romano, Torino, 2017, 1 e ss.

[10] Nello stesso senso si veda anche la critica mossa da R. ORESTANO, *Diritto, incontri e scontri,* Bologna, 1981, 1 e ss.; U. IZZO, *Alle origini del copyright e del diritto d'autore. Tecnologia, interessi e cambiamento giuridico,* Roma, 2010; G. SANTUCCI, *Diritto romano e diritti europei, Continuità e discontinuità nelle figure giuridiche,* Bologna, 2018, 41-42; G. SANTUCCI, *Diritti dell'autore in Roma antica?*, in *Index*, 2011, 143.
Nella stessa direzione anche la conclusione raggiunta da S.MESSINA, *Le Plagiat litéraire et artistique dans la doctrine, la legislation comparée et la jurisprudence internationale,* in *Recueil des cours de l'Accadémie de droit international de la Haye*, 1935, il quale nota come il pensiero giuridico romano non avesse preso in considerazione il problema della

Sicuramente suggestivi i richiami al principio di accessione, al *"litterae chartulis cedunt"*[11], all' *"impones plagiario pudorem"* [12], agli "*scripta furfantes"*[13], eppure, ai fini di questo contributo, sembra lecito soprassedere oltre al loro mero richiamo.

Non sarebbe interpretativamente onesto ricercare fonti per l'*enforcement* del diritto d'autore e la tutela di dati personali nelle maestose Istituzioni di Gaio. Nonostante i tentativi di ricerca, infatti, in esso alcuna significativa traccia può essere scorta persino dell'esistenza stessa di un problema di proprietà intellettuale. Si ricordi difatti come, nell'esaminare l'istituto dell'accessione quale modo di acquisto a titolo originario della proprietà, il giurista romano afferma che ove due *res* appartenenti a diversi soggetti si dovessero fondere diventando un tutt'uno inseparabile, l'acquisto della proprietà della *res* risultante dalla fusione dovrà essere concesso al proprietario della cosa principale in cui l'accessoria si è unita in base al principio *accessorium sequitur principale*. Nel caso della scrittura, dunque, Gaio riteneva che fosse il *dominus* della carta, in quanto *res principale*, ad ottenere la proprietà di ciò che altri vi potevano aver scritto applicando il principio per cui *superficies solo cedit*. Le conclusioni oggi sarebbero di senso diametralmente opposto all'impostazione Gaiana, dimostrazione del fatto che cercare radici di un diritto di proprietà intellettuale nel diritto romano è probabilmente operazione stilistica ma priva di fecondità ermeneutica.

Per non essere sordi alle voci della dottrina, tuttavia, si deve dar conto di come altri autori[14] hanno invece diversamente analizzato il concetto di plagio con peculiare enfasi sulla parola latina "*plagiarius*" che originariamente significava "ladro di schiavi". Correttamente tali autori ricordano che metaforicamente venne usata da Marziale in uno dei suoi epigrammi per accusare un coevo poeta di essersi attribuito indebitamente la paternità di versi dell'autore. Si deve però procedere con cautela, non attribuendo alle parole degli antichi significati che non erano loro propri. E nella stessa linea interpretativa si ricorda anche il genere del c.d.

---

proprietà intellettuale in quanto tale questione semplicemente non poteva porsi dati i limiti alla duplicazione dello scritto in epoca romana e rimasti senza significative differenze fino all'invenzione della stampa. In senso critico si pone invece U. BARTOCCI, *Aspetti giuridici dell'attività letteraria in Roma antica. Il complesso percorso verso il riconoscimento dei diritti degli autori,* Torino, 2009.

[11] Gai 2. 27 "*Eadem ratione probatum est, quod in cartulis sive membranis meis aliquis scripserit, licet aureis litteris, meum esse, quia litterae chartulis sive membranis cedunt. Itaque si ego eos libros easve membranas petam nec impensam scripturae solvam, per exceptionem doli mali summoveri potero*"

[12] MARZIALE, Epigramma, I, 52:
«*Commendo tibi, Quintiane,*
nostros nostros dicere si tamen libellos
possum, quos recitat tuus poeta:
si de servitio gravi queruntur,
adsertor venias satisque praestes,
et, cum se dominum vocabit ille,
dicas esse meos manuque missos.
hoc si terque quaterque clamitaris,
impones plagiario pudorem».

[13] VITRUVIO, De Architectura, Libro VII, Prefazione, 1-3, citando nel testo originale: "*Itaque quemadmodum his gratiae sunt agendae, contra, qui eorum scripta furantes pro suis praedicant, sunt vituperandi, quique non propriis cogitationibus scriptorum nituntur, sed invidis moribus aliena violantes gloriantur, non modo sunt reprehendendi, sed etiam, qui impio more vixerunt, poena condemnandi*."

[14] R. A. POSNER, *Il piccolo libro del plagio,* Roma, 2007; U. BARTOCCI, *Aspetti giuridici dell'attività letteraria in Roma antica. Il complesso percorso verso il riconoscimento dei diritti degli autori,* Torino, 2009; R. TERRY, *Plagiarism*: *A Literary Concept in England to 1775*, in *English*, vol. 56, (2007), 1, 2.

centone[15] che, pur originando dall'unione di frasi di autori od opere diversi, non veniva invece considerato con disvalore.

La storia da cui partire allora si deve intendere più recente. In un approccio di "*law and technology"* si rende opportuno volgere lo sguardo ad alcune fra le invenzioni che hanno rivoluzionato il modo di comprendere il diritto d'autore, di combattere la pirateria e di invadere l'altrui sfera di personalità, ma soprattutto hanno mutato la società. Per questa ragione si procede di seguito a proporre cinque vicende scelte in cui storicamente *l'enforcement* del diritto d'autore ha mostrato la sua potenza ed invasività.

1. Gutenberg e l'invenzione della stampa: la pirateria del libro stampato

Il concetto specifico di plagio intellettuale[16] si affaccia in Europa con l'avvento dell'età moderna, o meglio, di quell'era che convenzionalmente siamo soliti chiamare "moderna". Il termine ed il suo annesso significato si lega a trasformazioni culturali, sociali e chiaramente tecnologiche innescate da Johannes Gutenberg[17] con l'invenzione della macchina da stampa. È infatti la tecnologia che permette di connotare il diritto d'autore come un diritto moderno, è la irriproducibilità tecnica[18] del testo che impedisce, prima di questo momento, una sua concreta protezione.

I primi vagiti dell'esperienza giuridica che darà vita al diritto d'autore si devono collocare quindi in un momento che può essere inteso come rivoluzionario. Le ragioni furono principalmente di ordine economico in quanto sarebbe stato logicamente impensabile, prima dell'introduzione della stampa, creare un mercato di larga scala per il commercio del libro.

È infatti affermazione comune in campo microeconomico che per la massimizzazione del profitto sia essenziale scegliere il livello di produzione che consente di rendere massima la differenza fra ricavi e costi[19]. L'innovazione tecnologica permise l'abbattimento dei costi e dei tempi di produzione e consentì il fiorire e la diffusione di opere dell'ingegno.

Incidentalmente, occorre notare come la stampa a caratteri mobili consista nell'uso di elementi tipografici mobili per riprodurre su carta dei testi. L'innovazione significativa fu segnata dal passaggio dalla xilografia, per la qual tecnica le matrici venivano ricavate da un

---

[15] Per centone si fa riferimento ad un testo composto unendo frasi di autori od opere diversi, unite a formare un'opera originale. Il termine deriva dal latino *cento* ed a sua volta dal greco *κέντρων*. Fra le composizioni più famose in questo genere si ricordano ad esempio il Centone nuziale di Ausonio, del 369 d.C., costituito esclusivamente da brani di origine Virgiliana oppure i greci "Centoni omerici" (Homerocentona). Per maggiori informazioni si faccia riferimento a B. MORONI, *L'imperatore ed il letterato nel "Cento Nuptialis" di Ausonio,* in *ACME, Annali della facoltà di lettere e filosofia dell'Università degli Studi di Milano,* 2006, Volume LIX, Fascicolo III (Settembre-Dicembre), liberamente accessibile presso: «*https://www.ledonline.it/acme/allegati/Acme-06-III-03-Moroni.pdf*» (Ultimo accesso: 10 maggio 2022).

[16] Per maggiori informazioni sul concetto di plagio si faccia riferimento al recente contributo di G. DORE, *Plagio e diritto d'autore. Un'analisi comparata e interdisciplinare*, Milano, 2021, accessibile presso: «https://zenodo.org/record/5961499#.YnifBy2uZ-W» (Ultimo accesso: 10 maggio 2022). In particolare, l'autrice brillantemente nota che (*pag.* XII) "*Il plagio è influenzato dalle incessanti trasformazioni sociali e tecnologiche che caratterizzano il diritto d'autore contemporaneo e sfidano le sue regole convenzionali, specialmente nella sua interpretazione giurisprudenziale. Le difficoltà di individuare e sanzionare le condotte plagiarie crescono di pari passo con l'evoluzione della tecnica e delle arti, considerata l'estensione della tutela a sempre più nuove e complesse opere dell'ingegno*".

[17] Johannes Gensfleisch zum Gutenberg, Magonza, 1400 circa – Magonza, 3 febbraio 1468

[18] Maggiori riferimenti a questo concetto possono essere rinvenuti in U. IZZO, *Alle origini del Copyright e del diritto d'autore*, Roma, 2010*,* 10 e ss.

[19] R.S. PINDYCK, D.L. RUBINFELD, *Microeconomia*, IX edizione, Milano-Torino, 2018

unico blocco ligneo, ad una lega tipografica metallica in cui i singoli caratteri potevano essere allineati in diverse combinazioni, inchiostrati e dunque passati su carta. La macchina sfruttava la tecnologia della pressa a vite, già previamente utilizzata in campo vinicolo, per esercitare un'uniforme pressione sulla carta in modo da riprodurre quanto allineato nella matrice. In seguito ai primi tentativi di Gutenberg a Magonza, verso la metà del XV secolo la stampa di incunaboli si era rapidamente diffusa in tutta l'Europa occidentale. Essa era percepita come una attività pratica, un mestiere la cui popolarità cresceva a grande velocità: un'attività artigianale, e come tale si strutturò e prese forma[20].

Era certamente ancora viva l'idea di un ordine sociale, di un posto da ricoprire nella comunità, di una strutturazione gerarchica del vivere comunitario che sin da Carlo Magno voleva rispecchiare l'ordine dei cori celesti, così come esplicitato dallo Pseudo-Dionigi l'Areopagita[21]. Non sorprende, dunque, che gli uomini dell'epoca sapessero che per organizzare e gestire al meglio i rispettivi mestieri, il modello principe era quello corporativo. Quindi le professioni legate alla stampa andarono ad organizzarsi in gilde ed associazioni similari a quelle di altri settori, gestendo il processo creativo ed il commercio libresco. La nuova tecnologia si catalizzò nelle mani di questo nuovo ceto produttivo: le corporazioni di stampatori[22]. Ben presto tali organizzazioni ottennero dai sovrani e dalle autorità del tempo varie prerogative atte a favorire lo sviluppo dei propri centri di stampa.

L'attenzione delle autorità non tardò a manifestarsi: la Chiesa ed i sovrani elaborarono infatti meccanismi per rendere maggiormente affidabili tali comunità e fra le varie novità così introdotte, a titolo di esempio, si fece largo anche l'Indice dei libri proibiti[23]. Quindi, quando l'invenzione di Gutenberg rese tangibili i guadagni derivanti dalla riproduzione delle opere letterarie, la nascente industria del libro subì il controllo della Chiesa e delle Università[24].

Eppure, lo scrigno offerto a Porzia dal Principe del Marocco insegna che anche in questa vicenda: "*All that glisters is not gold, Often have you heard that told* [25]". Come ricorda Adrian Johns[26], gli stampatori divennero esasperati dal moltiplicarsi di rivendicazioni spurie di paternità ed autenticità dei libri che comparivano nel mercato, minacciando i ricavi conseguibili nel momento in cui l'elemento falso poteva facilmente scalzare l'autentico.

---

[20] Circa la struttura delle prime corporazioni di stampatori si può far riferimento ad U. IZZO, *Alle origini del copyright e del diritto d'autore. Tecnologia, interessi e cambiamento giuridico,* Roma, 2010, con particolare enfasi sulla struttura della Stationers' Company londinese.

[21] Il riferimento è al Corpus Dionysianum o Areopagiticum ed in particolare al *De coelesti hierarchia*, in cui le gerarchie angeliche vengono divise in tre cori celesti a loro volta divisi in altrettanti ordini.

[22] Per riferimenti all'attività dei primi stampatori, soprattutto in Inghilterra si veda H. S. BENNETT, *English Books & Readers,* in *Cambridge University Press*, Cambridge, 1989.

[23] Per ulteriori notazioni ed esemplificazioni a carattere storico si veda: D. T. POTTINGER, *The French Book Trade in the Ancien Régime 1500-1791*, Oxford University Press, London, (1958); A. GRAFTON, *How Revolutionary was the Print Revolution, The American Historical Review*, Volume 107, Issue 1, (200*2), liberamente accessibile presso: «https://doi.org/10.1086/ahr/107.1.84»* (Ultimo accesso: 10 maggio 2022). Con riferimento all'Indice dei Libri Proibiti si faccia riferimento a D. QUAGLIONI, *I concili del medioevo e dell'età moderna,* in *Storia dei Concili*, Cinisello Balsamo, 1995, con particolare riferimento alle misure adottate dal Pontefice Leone X nel 1514 in occasione del Concilio Lateranense V ove si elaborarono misure volte a garantire l'esame preventivo dei libri da mandare in stampa.

[24] A. BIRRELL, *Seven lectures on the Law and History of Copyright in Books,* Putnam-G.P. Cassel & Sons, New York-London, 1899, liberamente accessibile presso: «https://babel.hathitrust.org/cgi/pt?id=hvd.32044025695370&view=1up&seq=58» (Ultimo accesso: 10 maggio 2022).

[25] W. SHAKESPEARE, *Il mercante di Venezia,* atto secondo scena settima.

[26] A. JOHNS, *Pirateria: storia della proprietà intellettuale da Gutenberg a Google*, Torino, 2011, 33 e ss.

Il Don Chisciotte[27] fornisce uno spaccato satirico ma significativo di questa realtà nel suo secondo volume. La seconda parte dell'opera, infatti, principia con un "Prologo" al lettore, nel quale Cervantes allude al "Secondo Don Chisciotte"[28], uno scritto apocrifo firmato sotto pseudonimo da Alonso Fernández de Avellaneda. Quando Don Chisciotte giunge a Barcellona entra in una stamperia ove dei lavoratori stanno correggendo il libro dell'impostore. Quando alla fine della storia l'eroe viene ucciso dal suo autore, Cervantes emblematicamente afferma: "*Tra la compassione ed il pianto dei circostanti egli dunque esalò lo spirito, e voglio dire, morì: ed il curato ottenne dal notaio la legale testimonianza che "Alonso Chisciano il buono, chiamato comunemente don Chisciotte della Mancia, era passato da questa presente vita, e morto naturalmente." Si volle questa giurata prova per togliere l'occasione che qualche altro autore, diverso da Cide Hamete Ben-Engeli, lo facesse risuscitare con falsità e dettasse interminabili storie delle sue prodezze. E questo fu il fine dell'ingegnoso Idalgo della Mancia, la cui patria non volle Cide Hamete rendere chiaramente nota per lasciare che tutti i paesi e i villaggi della Mancia contendessero tra loro per affigliarselo e tenerlo per suo, come contesero per Omero le sette città della Grecia"*[29]. L'autore in questo passaggio compie una scelta consapevole, decide di far morire il suo personaggio per assicurarsi che nessun altro episodio falso possa esser messo in circolazione: tale era il contesto libraio dell'epoca.

Quale potesse essere il rimedio ad una storia di plagio e pirateria nemmeno il genio di Cervantes riuscì a comprendere. Eppure, un'indicazione, mascherata da critica tagliente verso la falsità delle ristampe, viene offerta dall'autore ai lettori: "*I libri che sono stampati con licenza regia e con approvazione di coloro al giudizio dei quali furono sottoposti; i libri che con generale diletto sono letti e celebrati dai grandi e dai piccoli […] dovrebbero essere dunque una bugia!*[30]". Il meccanismo cui si riferisce l'autore è quello dell'autorizzazione, una licenza rilasciata dalle autorità canoniche o secolari, spesso necessaria per la pubblicazione di un libro, compendiata con meccanismi similari quali le patenti ed i registri.

Quanto alle patenti si può limitare la disamina all'affermare che esse erano essenzialmente delle lettere di produzione regia che durante il periodo medioevale venivano variamente impiegate per copiose differenti finalità. In via di esemplificazione potrebbe farsi riferimento alla più antica forma di tutela della stampa. Il richiamo è alla Serenissima Repubblica di Venezia la quale, il 18 settembre 1469, concesse al tedesco Giovanni da Spira un particolare privilegio di stampa.[31]

I moderni diritti autorali possono essere ricondotti storicamente alla nascita di privilegi monopolistici concessi agli stampatori dai sovrani. Il presupposto su cui si basava tale concessione riposava sul conferire a coloro che possedevano le presse per produrre libri un monopolio che permettesse il controllo delle stampe. La concessione di tale potere tuttavia chiedeva in cambio di permettere alle autorità di ingerire nelle scelte produttive dell'artigiano, procedendo a censurare ed a tassare le opere prodotte. Sarà solo a partire dal XVIII secolo che si passerà da queste forme di privilegio a veri diritti di esclusiva in capo all'autore[32].

---

[27] M. CERVANTES, *Don Chisciotte della Mancia,* Rizzoli, Milano, 2007.

[28] Il riferimento è ad Alonso Fernández de Avellaneda, autore di "*Segundo tomo del ingenioso hidalgo Don Quijote de la Mancha*".

[29] M. CERVANTES, *Don Chisciotte della Mancia,* cit.; il riferimento è tratto dal tomo secondo, capitolo settantadue.

[30] CERVANTES, *ibidem*, Il riferimento è tratto dal capitolo cinquantesimo

[31] U. IZZO, *Alle origini del copyright e del diritto d'autore. Tecnologia, interessi e cambiamento giuridico,* cit., 16 e ss.

[32] Per maggiori riferimenti si veda R. CASO*, Alle origini del Copyright e del droit d'auteur: spunti in chiave di diritto e tecnologia,* in U. Izzo, *Alle origini del copyright e del diritto d'autore. Tecnologia, interessi e cambiamento giuridico*, disponibile presso: «https://ssrn.com/abstract=2254259» (Ultimo accesso: 10 maggio 2022) o «http://dx.doi.org/10.2139/ssrn.2254259» (Ultimo accesso: 10 maggio 2022).

Il tramonto degli incunaboli, come ricorda Umberto Izzo[33], prelude ad una produzione editoriale sempre più intensa avente come conseguenza anche un innalzamento della scolarizzazione delle popolazioni europee[34]. I sovrani ben presto avvertirono l'esigenza di porre freni all'insediamento di attività di stampa per limitare il circolare di idee non controllate. È il momento storico della Controriforma e dei suoi fervori che resero manifesto il problema della regolazione del flusso di conoscenza non più costretto entro i laboriosi e lenti sforzi dell'amanuense[35]. Per le monarchie europee il pericolo della nuova tecnologia di stampa doveva essere affrontato con un sistema di controllo preventivo dell'attività editoriale e con una effettiva vigilanza sui contenuti stampati[36].

Il sistema delle lettere patenti e delle autorizzazioni in alcuni contesti poteva associarsi anche con quello del registro. Esso si presentava fisicamente come un libro in cui gli stampatori di uno stesso luogo, della stessa città, iscrivevano i titoli delle opere che intendevano portare alle stampe e in tal modo, ove il registro fosse reputato affidabile, ingenerava un tal rispetto da parte della comunità di appartenenza da creare una sorta di proprietà *de facto* dell'opera in capo allo stampatore che per primo iscriveva il titolo nel registro. Questo sistema è di interesse notevole in quanto non derivava la sua autorità solamente dal sovrano, ma anche e soprattutto dall'autoregolazione dei professionisti del settore. Il registro costituisce un elemento centrale per il primo aneddoto riguardante i sistemi di *enforcement* del diritto d'autore attuati dalla Stationers' Company, ed in un paiolo ribollente di scontri ed interessi economici confliggenti riecheggia il monito del Macbeth: *"Something wicked this way comes*[37]".

1.1. Lo Stationer's Register ed il potere di perquisire

La storia della pirateria non è una mera questione teorica, tocca strategie di controllo e consuetudini nate dalle pratiche seguite meticolosamente per generazioni ben prima di essere trasposte in atti aventi forza di legge. Le convenzioni che nacquero nel mondo del libro all'inizio dell'età moderna volevano regolamentare ciò che ad allora veniva chiamato "proprietà". I principi che vennero a svilupparsi, anche se non presentavano veste o valore legale, erano rispettati dagli stampatori sentendosi vincolati alla loro ottemperanza. Quando nacque la pirateria nel mondo libresco, coloro che vi si opposero e vollero combatterla si richiamarono a questi principi e consuetudini di correttezza.

In seguito all'introduzione della stampa in Inghilterra ad opera di William Caxton, a Londra nacque un'istituzione di governo del settore librario: la "Company of Stationers". Nel 1557 la Regina Maria I Tudor (Maria la Cattolica o, come meglio conosciuta, *Bloody Mary*) decise che chiunque volesse stampare un'opera a fini di lucro dovesse essere membro della corporazione. Tale patente reale conferiva un potere di carattere monopolistico alla Stationers' Company, un privilegio per mezzo del quale, allo stesso tempo, la Corona si

---

33 U. IZZO, *Alle origini del copyright e del diritto d'autore. Tecnologia, interessi e cambiamento giuridico,* cit. 15 e ss.

34 Sulla relazione esistente fra stampa e scolarizzazione nel XVI secolo si faccia riferimento a C. CIPOLLA, *Literacy and Developement in the west,* Londra, 1969.

35 Per una copiosa analisi degli effetti della censura nello sviluppo della vita intellettuale e sulla diffusione dell'industria del libro nei paesi investiti dalla Controriforma si veda A. ROTONDÒ, *La censura ecclesiastica e la cultura,* in *Storia d'Italia,* Volume V, Torino, 1973.

36 Come ad esempio ricorda H. RANSOM, *The First Copyright Statute: An Essay on An Act for the Encouragement of Learning, 1710,* Austin, TX: U of Texas P, 1956, sin dal 1524 il vescovo di Londra produsse una serie di omelie rivolte agli stampatori predicando una massima attenzione nella pubblicazione di testi contenenti le eresie luterane.

37 W. SHAKESPEARE, *Macbeth*, atto quarto scena prima

assicurò il controllo sui processi di pubblicazione e vendita dei testi scritti. La Stationer's Charter attribuì dunque alla Stationers' Company il potere centralizzato di esercitare i poteri regi di soppressione dei libri proibiti [38], potendo altresì godere dell'assistenza della giurisdizione penale della Star Chamber[39].

Il compito della corporazione era di impedire la produzione e la commercializzazione di stampe abusive. Per tal fine essa creò e fece rispettare delle convenzioni capaci di definire la condotta dei lavoratori nel mondo editoriale. Fra le regole più complesse e controverse si annoveravano quelle sulla registrazione dei titoli da dare alla stampa.

Presso lo Stationers' Hall, palazzo confinante con la Cattedrale di Saint Paul a Londra, i membri della congregazione dovevano recarsi per riportare sul registro ivi conservato i titoli delle opere che stavano pubblicando. Esso divenne il presidio principe di un complesso sistema di attribuzione di proprietà tale per cui i titoli registrati iniziavano ad essere considerati *de facto* di proprietà di chi li aveva registrati. Infatti, tali titoli venivano immessi nel registro sotto il nome di un membro della corporazione, non sotto il nome dell'autore. Per convenzione, il membro che per primo aveva registrato il libro acquisiva il "*copyright*", ovvero il diritto esclusivo di riproduzione dell'opera indicata[40]. Il certosino regime applicato dalla Stationers' Company, pur non riuscendo ad estinguere l'insopprimibile energia della pirateria, contribuì tuttavia a radicare negli associati l'idea che l'editore di un determinato testo effettivamente conseguisse, per mezzo della registrazione, un monopolio perpetuo nello sfruttamento economico dell'opera registrata, tutelato da un apparato di rimedi interni alla corporazione e potendo invocare a proprio presidio la temuta Star Chamber.

Ottenuta dunque un'autorizzazione alla stampa da parte delle autorità regie od ecclesiastiche, registrato il titolo sul libro degli Stationer, si procedeva alla stampa nella convinzione che i costi sostenuti fra tributi, fabbricazione e commercializzazione sarebbero stati ripagati dal privilegio monopolistico così ottenuto, massimizzando di conseguenza i profitti. Ove uno stampatore rivale avesse pubblicato lo stesso testo in violazione di questo privilegio si sarebbero attivate numerose possibili strategie di contrasto.

La gilda stessa vigilava sulle principali violazioni del registro avendo strutturato al suo interno un proprio tribunale composto da membri scelti (*Court of Assistants*). Il tribunale degli Stationer soleva riunirsi mensilmente nella sede dell'associazione; una volta riportato il caso alla Corte si sarebbe potuto procedere ad indagini per individuare la scorrettezza e, ove ritenuta esistente, un risarcimento sarebbe stato comminato. L'apparato di regole degli Stationer, sociali prima che giuridiche, era infatti principalmente garantito dalla giurisdizione disciplinare dell'editoria inglese, delegata all'*enforcement* di queste regole dalla Corona stessa[41].

---

[38] U. IZZO, *Alle origini del copyright e del diritto d'autore. Tecnologia, interessi e cambiamento giuridico,* cit. 22 e ss. Per maggiori informazioni sulla storia della Stationers' Company e della Stationers' Charter si consulti altresì il sito «https://www.stationer.org» (Ultimo accesso: 10 maggio 2022).

[39] La Star Chamber (Camera Stellata) era una Corte inglese che aveva sede presso il Palazzo di Westminster, composta da consiglieri privati e giudici di common law con giurisdizione in materia sia civile che penale. La Star Chamber fu originariamente istituita per garantire la corretta applicazione delle leggi contro le persone socialmente e politicamente importanti, a tal punto in vista da far dubitare dell'imparzialità dei tribunali ordinari, possibilmente intimiditi nel giudizio contro tali personalità. La Camera Stellata, tuttavia, divenne presto emblema di oppressione sociale e politica a causa di un abuso discrezionale del potere conferitole.

[40] Per maggiori riferimenti si veda W. W. GREG, *Some Aspects and Problems of London Publishing between 1550 and 1650,* Clarendon Press, Oxford, 1956; U. IZZO, *Alle origini del copyright e del diritto d'autore. Tecnologia, interessi e cambiamento giuridico,* cit.

[41] E. A. POSNER, *Law and Social Norms, Harvard University Press Cambridge*, Massachusetts, 2000; J. ARMOUR, *Review of Law and Social Norms,* in *Journal of Law and Society*, vol. 30, no. 4, [Cardiff University, Wiley], 2003, 609 e ss., liberamente accessibile presso: «http://www.jstor.org/stable/1410375» (Ultimo accesso: 10 maggio 2022);

Il sistema creato dagli Stationer era la base di un codice di condotta e di autogoverno del settore e questo codice veniva regolarmente fatto rispettare fra i membri della corporazione al fine di assicurare un'alta reputazione agli artigiani del settore. Il controllo e la "*compliance*" alle consuetudini erano affidati a dei sorveglianti. Ed ecco che si spiega il monito del Macbeth, quel "*something wicked*" che si annida nelle aule della Stationers' Hall. A tali controllori erano attribuiti svariati poteri, fra cui l'autorità di entrare nelle case dei membri e nelle loro officine, spesso domestiche, per perquisirle. Era un potere, come ricorda Adrian Johns[42], superiore persino a quello accordato dalla Magna Carta ai rappresentati dello Stato. Le irregolarità che potevano essere riscontrate potevano essere di tre fattispecie: (a) il volume poteva essere mal rilegato, avere errori di stampa od una carta di bassa qualità; (b) il volume poteva avere un contenuto blasfemo, sedizioso ovvero ancora osceno; (c) il libro poteva violare il registro.

Mentre le prime due tipologie di "illecito", *latu sensu*, riguardavano la corporazione nei suoi rapporti con la società e la collettività dei fruitori dei beni, tanto da poter inficiare la reputazione della categoria, la terza irregolarità riguardava i rapporti interni alla categoria stessa ed i conflitti fra Stationer. La Stationers' Company si dimostrò sin da subito capace di esercitare un ruolo effettivo di polizia, vigilando attentamente sugli interessi della corporazione al fine di reprimere la produzione e la commercializzazione di libri pirata.

La Charter attribuiva infatti agli Stationer il potere di emanare "*ordinances, provisions, and statutes for the governance of the art or mystery of Stationers*", nonché il potere di sorvegliare la stampa illegale con penetranti poteri di stampo poliziesco: "*shall very lawfull as well search, as often as they please, any place, shop, house, chamber or building of any stamper, printer, binder or feller of any manner of books within kingdom of England*". In aggiunta, si cumulava altresì il potere sanzionatorio consistente nel "*seizing, taking, or burning the foresaid books or things, or any of them printed or to be printed contrary to the form of any statute, act, or proclamation* [...]"[43]

Henry Stanley Bennett in merito aggiunge che "*the company was able to prohibit printing by any excepts its own members of those few who had a right given to them by royal warrant. The company was empowered to seek out unauthorised printers, to seize any printed or bound stock which had been produced contrary to the form of any statute, act, or proclamation made or to be made. The material they seized they could burn, put the printers in prison, and levy a fine of 100s on each of them*[44]". Tali poteri erano esercitabili da parte della Company direttamente e con ampia discrezionalità.

P.R. MILGROM, D. C. NORTH, B. R. WEINGAST, *The Role of Institutions in the Revival of Trade: The Law Merchant, Private Judges and the Champagne Fairs,* in *Economics and Politics*, 2, 1990, liberamente accessibile presso: «https://web.stanford.edu/~milgrom/publishedarticles/The%20Role%20of%20Institutions%20in%20the%20Revival%20of%20Trade,%201990.pdf» (Ultimo accesso: 10 maggio 2022).

[42] A. JOHNS, *Pirateria: storia della proprietà intellettuale da Gutenberg a Google*, Torino, 2011, 31 e ss.

[43] Sezioni così riprese da E. ARBER, *A Transcript of the Registers of the Company of Stationers of London, 1554-1640 A.D.,* Stationer's Company, Londra, 1875-77. Sui poteri della Company si faccia riferimento anche a H.S. BENNETT, *English Books & Readers 1558 to 1603,* Cambridge University Press, Cambridge, 1989; traducendo liberamente il testo: "*ordinanze, disposizioni e statuti per il governo dell'arte o del mistero degli stampatori*"; "*sarà ritenuto lecito anche perquisire, con la frequenza che si vuole, ogni luogo, negozio, casa, camera o edificio di qualsiasi stampatore, rilegatore o venditore di qualsiasi tipo di libri all'interno del regno d'Inghilterra"; "sequestrare, prendere o bruciare i predetti libri o cose, o alcuno di essi stampati o da stampare contrari alla forma di qualsiasi statuto, atto o proclama*".

[44] H.S. BENNETT, *English Books & Readers 1558 to 1603*, cit, traducendo: "*la gilda era in grado di vietare la stampa, ad eccezione dei propri membri, di quei pochi che avevano un diritto conferito loro da un mandato reale. La corporazione era autorizzata a cercare tipografi non autorizzati, a sequestrare qualsiasi materiale stampato o rilegato che fosse stato prodotto in contrasto con la forma di qualsiasi statuto, atto o proclama. Il materiale sequestrato lo potevano bruciare, mettere in prigione i tipografi e imporre una multa di 100 scellini a ciascuno di loro".*

L'ampia delega di potere lasciata dalla Corona alla Stationers' Company rende il sistema della copia sostanzialmente estraneo alle dinamiche di Common Law, le regole di dettaglio erano dettate direttamente dalla corporazione stessa senza alcun necessario riconoscimento statutario, imponendosi quali norme sociali[45]. Esse si affermarono attraverso un'indefessa applicazione di regole governate e ritualizzate dagli operatori economici che da questo sistema riuscivano a trarre la loro ricchezza.

Il riferimento storico, dunque, rileva direttamente nei rapporti fra *enforcement* del diritto d'autore e la tutela della vita privata. Siamo lungi dall'affermazione di un diritto alla riservatezza, alla protezione dell'identità personale e della *privacy*, eppure l'esempio che dalla storia si riesce a trarre con certezza è che sin dalle origini del moderno diritto d'autore, dai primi vagiti del *copyright*, la richiesta di tutela di una proprietà, ancorché *de facto,* ha avuto influenze in termini di ingerenza nella dimensione fisica, spaziale dell'individuo.

Una prima notazione che potrebbe essere tratta da questo racconto concerne il fatto che la tutela del diritto monopolistico dello *Stationer* sia una tutela privata, fatta da una "polizia" interna della corporazione con poteri ed attribuzioni proprie particolarmente invasive. Tale notazione può essere a sua volta sdoppiata in due linee direttive di un ragionamento che proseguirà per l'intero elaborato ed altrettante strategie comportamentali che torneranno nel corso dei secoli e sono ancora oggi non infrequenti. La prima questione riguarda la dimensione privatistica in cui si muove l'autotutela degli stampatori. Sicuramente l'attribuzione di tale potere ha una origine pubblicistica, data dalla Charter del 1557, tuttavia l'esercizio del potere è rimesso in via pressoché esclusiva alle dinamiche interne della corporazione. La dimensione privata percorre tutta la storia *dell'enforcement* del diritto d'autore con forme e pratiche di autotutela congegnate dai privati per essere usate contro altri privati. Si pensi all'implementazione dei sistemi di *Digital Rights Management* od ai moderni sistemi di gestione dei contenuti caricati dagli utenti delle piattaforme online. La seconda questione, connessa alla prima, è che questa forza privata assume connotazioni poliziesche, con poteri di perquisire, di ispezionare, di entrare nelle abitazioni dei pirati. Ma è poi così diversa, per chi la subisce, una perquisizione compiuta dagli Stationer rispetto ad una società privata che entra nel computer di un utente? Ed ancora: è così diverso il sorvegliante della Stationers' Company dalla Logistep[46] che individua gli indirizzi IP degli utenti? Sebbene i tempi mutino e con essi gli strumenti, la strategia rimane nei suoi connotati essenziali la medesima. Allora l'esempio dell'autotutela della Stationers' Company e del potere dei suoi sorveglianti di ispezione e perquisizione, depurato dalle circostanze storiche e contingenti che lo connotano, può diventare un primo emblema di un problema che non verrà confinato alla prima età moderna ma permarrà fino ai nostri giorni, al mondo digitale, alle reti *peer-to-peer* ed alla logica della sorveglianza privata.

2. Nehemiah Grew: il farmaco contraffatto

[45] E. A. POSNER, *Law and Social Norms, Harvard University Press Cambridge*, Massachusetts, 2000; J. ARMOUR, *Review of Law and Social Norms,* in *Journal of Law and Society*, vol. 30, no. 4, [Cardiff University, Wiley], 2003, 609 e ss., liberamente accessibile presso: «http://www.jstor.org/stable/1410375» (Ultimo accesso: 10 maggio 2022) *;* P.R. MILGROM, D. C. NORTH, B. R. WEINGAST, *The Role of Institutions in the Revival of Trade: The Law Merchant, Private Judges and the Champagne Fairs,* in *Economics and Politics*, 2, 1990, liberamente accessibile presso: «https://web.stanford.edu/~milgrom/publishedarticles/The%20Role%20of%20Institutions%20in%20the%20Revival%20of%20Trade,%201990.pdf» (Ultimo accesso: 10 maggio 2022).

[46] Chiaro riferimento alla vicenda connessa al Caso Peppermint, per la cui approfondita analisi si rinvia al successivo capitolo.

L'analisi proposta nel presente elaborato non si vuole limitare alle origini del *copyright* ed alla sua dimensione più fenotipica, ossia quella libresca, ma si estende anche ad altri ambiti delle arti, fra cui merita di essere segnalata la farmacologia. Questo solo apparente volo pindarico dalla tutela del libro stampato alla tutela del farmaco può destare stupore, tuttavia, la connessione si dimostra meno peregrina di quanto non sembri di primo acchito.

Adrian Johns[47] ricorda come i dubbi sull'attendibilità e la paternità della parola stampata, ambito che condusse al conio della parola "pirateria", in realtà si innestavano in una logica più generalizzata di timore nei confronti di oggetti creati dall'uomo, soprattutto per quanto il popolo introduceva nel proprio corpo: cibo, vino e medicine.

Celebri sono diventate le vicende riguardanti, fra i molti possibili esempi, il latte o la farina[48]. Secondo alcune ricerche diventate famose in epoca vittoriana, ove il latte fosse in procinto di rancidire si consigliava di aggiungere una piccola quantità di acido borico o di formalina per renderlo nuovamente utilizzabile e commestibile. La stessa celebre Mrs. Beeton[49] incoraggiava questa prassi con conseguenze disastrose sulla salute dei lettori dovute all'adulterazione degli alimenti, portando persino a morte per avvelenamento soprattutto fra gli infanti. Anche i panificatori, per far fronte ad una sempre crescente richiesta alimentare da parte della popolazione, iniziarono sempre più spesso ad aggiungere alle formulazioni alimentari elementi quali l'allume o l'intonaco. Furono i farmaci però a destare le maggiori preoccupazioni.

La connessione fra farmacie e stamperie è sorprendentemente stringente: come i libri, anche i prodotti farmaceutici erano creati artigianalmente da corporazioni di mestieri assai simili alla Stationers' Company. Inoltre, medicine e carta stampata, o più precisamente giornali, condividevano alcuni significativi spazi fisici: le librerie spesso vendevano farmaci e gli stampatori si guadagnavano da vivere pubblicizzando i medicinali. Ad esempio, Adrian Johns[50] ricorda come nell'Inghilterra del XVIII secolo lo stampatore John Newbery vendesse un elisir di sua produzione nel proprio laboratorio, od anche come i giornali di William Rayner vivessero grazie alla pubblicità di una "tintura pettorale" da lui acquistabile. Questo genere di associazione si fece molto comune in tutta Europa, tanto che i medici si fecero persuasi che per commercializzare un farmaco dovessero essere assistiti da un libraio[51].

Ancora oggi assistiamo a feroci disquisizioni su proprietà e pirateria che scoppiano in campo biomedico, i farmaci contraffatti si diffondono a macchia d'olio soprattutto nei paesi in via di sviluppo e le "farmacie online" ne facilitano la distribuzione[52].

---

[47] A. JOHNS, *Pirateria: storia della proprietà intellettuale da Gutenberg a Google*, cit., 99-114.

[48] Per maggiori informazioni: H.E ANNETT, *Boric Acid And Formalin As Milk Preservatives*, Thompson-Yates Laboratory, University College, Liverpool, (2003), liberamente accessibile presso: «https://www.sciencedirect.com/science/article/abs/pii/S0140673601015161» (Ultimo accesso: 10 maggio 2022).

[49] I. BEETON, *Mrs Beeton's Book of Household Management*, S. O. Beeton Publishing, Londra, 1861, liberamente accessibile presso: «https://archive.org/details/b20392758/page/n13/mode/2up» (Ultimo accesso: 10 maggio 2022).

[50] A. JOHNS, *Pirateria: storia della proprietà intellettuale da Gutenberg a Google, cit., 99-114*

[51] Per ulteriori descrizioni sulla vendita dei farmaci tramite la rete libraia si vedano anche "Isaiah Thomas Papers", American Antiquarian Society, citati in A. JOHNS, *Pirateria: storia della proprietà intellettuale da Gutenberg a Google,* cit. 127 e ss.

[52] Si veda in merito alle strategie IMPACT dell'OMS per far fronte a questo problema: D. DI GIORGIO, *Farmaci Contraffatti: Il fenomeno e le attività di contrasto*, in *AIFA*, 2010, disponibile presso «https://www.aifa.gov.it/documents/20142/0/Farmaci_Contraffatti_2010.pdf» (Ultimo accesso: 10 maggio 2022).

2.1. La lotta per il sale: il "*Tractatus de Salis Cathartici Amari in Acquis Ebeshamensibus*"

L'aneddoto riguardante il farmaco chiama in causa un attore fondamentale: Nehemiah Grew (1641-1712). Egli divenne famoso come botanico, medico e microscopista inglese che, con l'italiano Marcello Malpighi, è considerato tra i fondatori della moderna scienza dell'anatomia vegetale. Fra le sue opere principali, la più considerevole è sicuramente la sua "Anathomy of Plants" del 1679, tuttavia è di un'opera minore che si deve tessere la narrazione: il suo "*Tractatus de Salis Cathartici Amari in Acquis Ebeshamensibus*" (1695).

Le sventure che riguardarono la vita di Grew sono l'emblema dei rischi che ogni autore correva in quel periodo[53]. Un rivale, infatti, si appropriò di questa sua opera, la tradusse dal latino, la ristampò e la pubblicò con tali mutamenti da alterarne il significato e da renderla un'opera potenzialmente pericolosa. Eppure, al centro della disputa non vi era solamente una questione di proprietà letteraria, ma quello che forse potremmo definire il primo brevetto per un farmaco fabbricato nel mondo anglofono: il sale era l'oggetto della contesa. Prima di plagiare il volume, i pirati si appropriarono della sostanza: ossia un sale ottenuto ed estratto da una sorgente termale nelle periferie di Londa, ad Epsom nel Surrey.

Grew, infatti, aveva tentato di sfruttare una grande moda: quella delle acque termali. Le loro proprietà erano risapute sin dai tempi Rinascimentali, tuttavia il problema era che i benefici potevano essere goduti solo localmente. Per rimediare a questa inconvenienza Grew, assistito dalla Royal Society decise di cimentarsi in lunghi processi di distillazione delle acque della sorgente di Epsom. L'acqua di tale località aveva delle proprietà leggermente purganti, consentendo di liberare il corpo dalle impurità e regolarizzare gli "umori"[54]. Tuttavia, l'acqua della fonte tendeva a marcire rapidamente se non veniva bevuta subito ed inoltre i farmacisti dell'epoca erano soliti adulterare i prodotti diluendoli per far durare le riserve. L'estrazione del sale dalle acque avrebbe invece consentito a Nehemiah Grew una più lunga conservazione ed una distribuzione priva di pericoli per il consumatore. Mantenendo inoltre segreto il processo di estrazione, avrebbe goduto di una sorta di monopolio nella produzione di tal sale. Per sostenere la sua iniziativa non solo produsse una massiccia campagna pubblicitaria per mezzo della stampa, ma confezionò altresì un trattato in lingua latina esponendone i risultati.

Come accadeva per i libri, anche per i farmaci non mancavano pirati disposti a produrre la loro versione del sale di Epsom. Furono i fratelli Francis e George Moult che produssero talmente tanto sale da saturare il mercato inglese, irlandese e scozzese[55]. Era chiaro che la disputa intorno alla paternità del sale divenne ben presto una disputa sulla identificazione della sostanza ed il problema divenne quello della adulterazione della sostanza. Adrian Johns racconta in merito che un medico londinese, Josiah Peter, amico di Grew, minacciò persino i Moult di far loro causa non solo per aver infangato il buon nome dell'amico, ma per aver messo in pericolo la vita dei sudditi del Re. Solo in seguito a numerose contese per mezzo della stampa locale, Grew si decise ad appellare l'autorità del Re in suo soccorso. Egli chiese

---

[53] Una più completa analisi dell'intera vicenda è rinvenibile in A. JOHNS, *Pirateria: storia della proprietà intellettuale da Gutenberg a Google,* cit., 99-114, 127-132

[54] Per ulteriori riferimenti si veda anche A. SAKULA *Doctor Nehemiah Grew (1641-1712) and the Epsom salts,* in *Clio Med. 1984*; 19(1-2):1-21. PMID: 6085985, liberamente accessibile presso «https://pubmed.ncbi.nlm.nih.gov/6085985/» (Ultimo accesso: 10 maggio 2022).

[55] A. JOHNS, *Pirateria: storia della proprietà intellettuale da Gutenberg a Google*, cit. 127-132.

un brevetto reale per il modo di produzione del suo sale ed ottenuta l'autorizzazione fece circolare una missiva fra i medici londinesi denunciando l'operato dei Moult.

Alla fine della vicenda in realtà apparve chiaro come i Moult avessero vinto la battaglia: alcun processo in merito venne mai celebrato né la loro attività di commercializzazione del sale venne interrotta[56]. Questo è supportato altresì dal fatto che la stessa Royal Society ricordò George Moult come un membro onorato e rispettabile della comunità scientifica.

Il problema dell'adulterazione del farmaco diede vita a quanto ora preme maggiormente ricordare. A causa della contraffazione dei farmaci veniva a mancare la fiducia negli specialisti del settore. Quando i farmacisti si costituirono in una categoria a parte[57] divenne motivo di principale preoccupazione quello di combattere queste forme di adulterazione ed esercitare un controllo stringente sui farmaci non autentici. Questo divenne una delle maggiori spinte per la introduzione della Apothecaries' Company nel 1617[58].

L'associazione prese ad esempio il modello di gestione già in precedenza analizzato in merito alla Stationers' Company per il settore della carta stampata. L'Apothecaries' Company, dunque, procedette anch'essa a numerose ispezioni e perquisizioni presso i membri dell'associazione confiscando i materiali contraffatti e le sostanze illecite rinvenibili nelle officine e nelle case delle persone. Fu in questo panorama che lo scontro fra Grew ed i Moult si inserì.

Anche questo secondo aneddoto, *mutatis mutandis*, ricorda le medesime affermazioni già analizzate nel paragrafo precedente. La dimensione privatistica della condotta della Company ancora una volta sfocia in comportamenti molto invasivi per ragione di *enforcement* di diritti, l'autotutela alberga anche in questo settore e la dimensione più intima connessa alla casa ed alla persona viene toccata. Le conclusioni che possiamo trarne sono equiparabili a quelle del precedente esempio e le implicazioni analoghe. Due *companies* che nascono come corporazioni di artigiani assumono dei poteri para-pubblicistici fortemente invasivi ma non sarà l'ultima volta che un tale fenomeno si verificherà, è infatti vero che "*Quod fuit, ipsum est, quod futurum est. Quod factum est, ipsum est, quod faciendum est: nihil sub sole novum*[59]*"*.

Analizzando entrambi gli aneddoti sopra riportati possono trarsi ancora ulteriori notazioni. In primo luogo, deve essere notata la rilevanza delle norme sociali[60] in materia di diritto d'autore. La dinamica giuridica conosce da sempre questa fonte di produzione del diritto, variamente identificata sotto il nome di "usi", consuetudini o norme informali. Sono le norme informali, le norme che si sviluppano dalla pratica degli Stationer e dei farmacisti ad ingenerare un sentimento di obbedienza nei confronti dei consociati tale da farle apparire come norme giuridiche, quindi vincolanti. Questo non è indifferente alla nostra analisi in

---

[56] A. SAKULA *Doctor Nehemiah Grew (1641-1712) and the Epsom salts,* in *Clio Med. 1984*; 19(1-2):1-21. PMID: 6085985, cit.; A. Johns, *Pirateria: storia della proprietà intellettuale da Gutenberg a Google, cit., 99-144.*

[57] Per maggiori informazioni sulla Apothecaries' Company si veda: P. HUNTING, *A History of the Society of Apothecaries*, in *Worshipful Society of Apothecaries of London*, Londra, 1998.

[58] Si veda altresì l'articolo apparso sul *Journal of the Royal Society of Medicine*, 1999 volume 92, redatto da N. WEIR come recensione del volume, edito dalla Society of Apothecaries: "*A History of the Society of Apothecaries"* di P. HUNTING, liberamente accessibile presso: «https://journals.sagepub.com/doi/pdf/10.1177/014107689909200321» (Ultimo accesso: 10 maggio 2022).

[59] Ecclesiaste o Qohelet, 1,9-10

[60] Per ulteriori informazioni si faccia riferimento a R. CASO, *Il diritto d'autore dell'era digitale,* in G. PASCUZZI (a cura di*), Il diritto dell'era digitale. Tecnologie informatiche e regole privatistiche, II ed., Bologna, 2006,* 145 e ss.

quanto le norme informali oggi giocano un ruolo chiave nel controllo dell'informazione digitale[61].

In secondo luogo, può risultare utile anche richiamare un essenziale contributo della moderna dottrina d'oltreoceano[62] che fa oggi riferimento ad una dimensione della privacy intellettuale che riguarda la riservatezza all'interno degli spazi fisici. All'interno delle società occidentali, la tradizione e la prassi sociale riservano alcuni tipi di "spazio privato" all'individuo od al nucleo familiare. Primo fra questi spazi è certamente la casa, che è concepita come un luogo di rifugio dagli occhi del mondo esterno. Secondo questa dottrina, il diritto alla privacy si confonde con altri diritti, si inserisce nelle zone d'ombra e di confine dell'ordinamento e spesso si coniuga con i diritti basati sulla proprietà che consentono di controllare l'accesso alle case o agli uffici privati. Regole e tradizioni sulla libertà all'interno degli spazi privati riguardano non solo gli interessi di proprietà, ma anche, ad esempio, garanzie di libertà nel consumo letterario. È su questa dimensione della privacy che *l'enforcement* del diritto d'autore nei due racconti finora analizzati è andato ad incidere pesantemente, con una indebita compressione della prima per far spazio al secondo.

3. Gli spartiti musicali: James Frederick Willetts

Sul finire del XIX secolo ed il principiare del XX secolo, l'industria musicale si presentava principalmente dedita alla vendita di spartiti musicali. In epoca edoardiana i pirati riuscirono a raggiungere livelli tali di capacità di riproduzione degli spartiti da mettere in severa crisi l'industria di riferimento. La riproduzione illecita di partiture non costituisce una novità, è infatti presente in tutta Europa sin dal XVII secolo ma mai prima di allora aveva davvero costituito un problema di tali proporzioni. Inoltre, fino al 1770, la musica non era considerata all'interno dell'ambito protetto del *copyright*; dunque, la pirateria non poteva ritenersi esistente ed i ristampatori potevano riprodurre tutte le partiture che desideravano. Solo con il romanticismo e l'esaltazione del genio artistico, la dimensione assunse connotazioni morali di scorrettezza ed i ristampatori vennero etichettati come ladri e furfanti[63].

Prima di affrontare le vicende storiche riguardanti gli spartiti musicali, considerabili come anello di congiunzione tra una dimensione ancora legata alla stampa e la più attuale sfida posta dai mezzi di riproduzione analogica, si ritiene necessario brevemente ripercorrere alcuni passaggi storici che dalla Charter del 1557 hanno condotto gli Stationer a perdere progressivamente potenza.

---

[61] Si pensi ad esempio alla licenza GNU GPL nell'ambito dello sviluppo del software o alle licenze Creative Commons usate per formalizzare e per garantire l'accesso alla conoscenza scientifica. Per maggiori informazioni circa la rilevanza delle norme sociali nel campo del diritto d'autore si faccia riferimento a E. A. POSNER, *Law and Social Norms, Harvard University Press Cambridge*, Massachusetts, 2000; J. ARMOUR, *Review of Law and Social Norms,* in *Journal of Law and Society*, vol. 30, no. 4, [Cardiff University, Wiley], 2003, 609 e ss., liberamente accessibile presso: «http://www.jstor.org/stable/1410375» (Ultimo accesso: 10 maggio 2022)*;* P.R. MILGROM, D. C. NORTH, B. R. WEINGAST, *The Role of Institutions in the Revival of Trade: The Law Merchant, Private Judges and the Champagne Fairs,* in *Economics and Politics*, 2, 1990, liberamente accessibile presso: «https://web.stanford.edu/~milgrom/publishedarticles/The%20Role%20of%20Institutions%20in%20the%20Revival%20of%20Trade,%201990.pdf» (Ultimo accesso: 10 maggio 2022).

[62] J. E. COHEN., *DRM and Privacy,* 18 *Berkeley Tech. L.J.* 575-617 (2003), Georgetown Law Faculty Publications and Other Work, liberamente accessibile presso: «https://scholarship.law.georgetown.edu/facpub/60» (Ultimo accesso: 10 maggio 2022).

[63] A. JOHNS, *Pirateria: storia della proprietà intellettuale da Gutenberg a Google,* cit, 428-463.

Le derive autoritarie della Star Chamber ben presto richiesero al Parlamento inglese di porre fine al suo tirannico potere[64]. Questo avvenne nel 1640. Da tale momento la stampa si trovò, non per molto, libera da ogni controllo coercitivo e gli stampatori clandestini dilagarono. La situazione di anarchia ebbe tuttavia vita breve in quanto nel 1643 iniziò una forte pressione lobbistica da parte degli Stationer per dar vita ad una restaurazione del loro originario potere. Con la dissoluzione della parentesi repubblicana di Cromwell e la restaurazione di Carlo II Stuart del 1660, nel 1662 venne pubblicato il *Licensing of the Press Act*[65] che disattese in parte le speranze ripristinatorie degli originari privilegi degli Stationer. Con questa novella il sistema del registro degli Stationer divenne oggetto di un espresso obbligo legislativo assistito da sanzioni penali e patrimoniali; tuttavia, la registrazione non venne riconosciuta come titolo costitutivo di un diritto monopolistico *erga omnes*[66]. Questa questione, rimasta aperta con l'atto del 1662 e di nevralgica importanza, diventerà terreno di principale scontro nei successivi decenni[67]. Il mancato riconoscimento di un diritto d'esclusiva sull'opera rese insoddisfatti gli Stationer che proseguirono nei decenni successivi in una intensa attività di lobbismo, la quale condusse all'emanazione dello *Statue of Anne* nel 1710.

Il punto cruciale, tuttavia, è che dal 1662 gli ispettori della Stationers' Company persero in parte il loro potere di polizia privata in quanto le loro ispezioni, ove fossero compiute su soggetti estranei alla corporazione, sarebbero state assoggettate al vaglio giurisdizionale del King's Bench, pur rimanendo invece intatto e pervasivo nei confronti degli associati. Nonostante le criticità, per gli Stationer questo atto consentiva di poter tornare alla loro consueta attività confidando nell'efficacia repressiva nei confronti delle edizioni pirata offerta dallo statuto. In tale rinnovato contesto la Court of Chancery e la giurisdizione di Equity fondarono il principale foro per la difesa dei diritti degli stampatori.

Le principali statuizioni dello Statue of Anne del 1710 vennero riprese nel successivo Copyright Act del 1842. Solo nel 1911 la legislazione subirà profonde modificazioni a causa dell'implementazione della Convenzione di Berna. Nello specifico, la Legge del 1911 procedette ad abolire la necessità di registrazione presso la Stationers' Hall e stabilì che il diritto d'autore dovesse essere conferito al momento della creazione di un'opera. Tuttavia, poiché l'Atto del 1911 è entrato in vigore in momenti diversi nei diversi paesi del

---

[64] Nel 1641 il Parlamento, infiammato dal severo trattamento subito da alcuni dissidenti religiosi tra cui John Lilburne, William Prynne, ed Henry Burton, abolì la Star Chamber per mezzo dell'*Habeas Corpus Act* del 1640. L'occasione può essere anche considerata come una rivincita del Parlamento nei confronti della Monarchia dopo che, nel 1616, nell'ambito del caso *Lord Ellesmore contro Sir Coke*, si era stabilita la preminenza del sistema di equity sul common law.

[65] Per maggiori riferimenti e commenti si veda R. DEAZLEY, *Commentary on the Licencing Act 1662,* in *Primary Sources on Copyright* (1450-1900), eds L. Bently & M. Kretschmer, liberamente accessibile presso: «https://www.copyrighthistory.org/cam/tools/request/showRecord.php?id=commentary_uk_1662» (Ultimo accesso: 10 maggio 2022). Il provvedimento rubricato "*Act for Preventing the Frequent Abuses in Printing Seditious Treasonable and Unlicensed Books and Pamphlets and for Regulating Printing and Printing Presses*" è consultabile presso: «https://press-pubs.uchicago.edu/founders/documents/amendI_speechs1.html» (Ultimo accesso: 10 maggio 2022).

[66] C. S. CLEGG, J. GREENE, *The Trouble with Ownership: Literary Property and Authorial Liability in England, 1660–1730*, in *The American Historical Review*, Volume 111, Issue 3, June 2006, 902, Philadelphia: University of Pennsylvania Press. 2005, 272., accessibile presso «https://academic.oup.com/ahr/article-abstract/111/3/902/16311?redirectedFrom=fulltext» (Ultimo accesso: 10 maggio 2022).

[67] Il riferimento è alla celebre "bookseller battle" di cui ampia ricostruzione viene offerta in U. IZZO, *Alle origini del copyright e del diritto d'autore. Tecnologia, interessi e cambiamento giuridico,* cit. L'epilogo famoso di questa battaglia verrà offerto dal caso *Donaldson v. Becket*.

Commonwealth, in alcuni di tali paesi continuò a essere richiesta la registrazione presso la Stationers' Hall.

Tralasciando ulteriori digressioni storiche, quello che ora preme è tornare alla disamina dell'aneddoto relativo agli spartiti musicali. Anche in questa occasione la modifica viene nuovamente da una innovazione tecnologica connessa ad un cambiamento di percezione culturale. La messa a punto della litografia permise ai pirati di realizzare delle copie perfettamente identiche all'originale. La litografia venne infatti scoperta, quasi per caso, nel 1796 dall'austriaco Alois Senefelder utilizzando una pietra proveniente dalle cave di Solnhofen. Il funzionamento tecnico si basa sull'utilizzo di un particolare tipo di pietra, opportunamente levigata e quindi disegnata con una matita grassa, la quale ha la peculiarità di respingere l'acqua che invece viene trattenuta dalle parti non tracciate. In questo modo, ove debitamente inchiostrata, le parti non tracciate riceveranno inchiostro mentre quelle tracciate lo repelleranno. Passata al torchio consente una riproduzione su carta pressoché identica all'originale[68].

Questa capacità concessa dalla litografia permise di ottenere copie pirata di qualità identica all'originale a costi di produzione molto bassi. Al contempo sul piano sociale si verificò una congiuntura economica tale per cui sempre più parte della popolazione poteva disporre di denaro da destinare allo svago con conseguente maggior fruizione della musica e maggior domanda di spartiti musicali a basso costo.

La diffusione delle copie pirata fu cospicua. Contro la pirateria gli editori reagirono con iniziative su vari fronti sia individuali che collettive. Infatti, le maggiori case editrici dell'epoca quali la Chappell & Co. e la Francis, Day & Hunter si allearono costituendo la Music Publishers' Association (MPA[69]) già nel 1881[70]. L'associazione, diversamente dagli Stationer del XVII secolo, non dovette preoccuparsi di un riconoscimento legale dei propri diritti di riproduzione, in quanto la legge esistente già riconosceva loro tali prerogative, la difficoltà fu invece *nell'enforcement* di quel diritto.

3.1. Un corpo di polizia privata antipirateria: il "commando"

Adrian Johns[71] ricorda le azioni antipirateria di David Day della casa editrice Francis, Day & Hunter. Egli, con l'aiuto di un'agenzia investigativa privata, fece irruzione in un deposito nel 1902 sequestrando svariate copie di spartiti musicali. Di certo l'iniziativa non venne compiuta nella piena legalità, tuttavia i pirati non opposero resistenza. Confortato dalla riuscita della spedizione, Day procedette ad ulteriori azioni di questo genere. Il successo di queste azioni comportò uno svilupparsi di molti altri gruppi di polizia privata antipirateria, esortati retoricamente anche da Day stesso alla costituzione di un "*commando*". Le maggiori case editrici di spartiti musicali si mossero ben presto nella stessa direzione di David Day e persino si unirono in questa lotta anti-pirata formando la Musical Copyright Association (MCA) il cui segretario divenne John Abbott. Quest'ultimo venne incaricato dall'associazione

[68] Per ulteriori riferimenti alla storia della litografia ed alle tecniche di stampa si rimanda a C. J. HULLMANDEL, *The art of drawing on stone, giving a full explanation of the various styles, of the different methods to be employed to ensure success, and of the modes of correcting, as well as of the several causes of failure*, Londra, 1824.
[69] Per maggiori informazioni: «https://www.mpa.org» (Ultimo accesso: 10 maggio 2022).
[70] B. ATKINSON, B. FITZGERALD, *Copyright Law: Volume II: Application to Creative Industries in the 20th Century*, Londra, 2017.
[71] A. JOHNS, *Pirateria: storia della proprietà intellettuale da Gutenberg a Google,* cit., 442- 448.

a condurre nuove offensive e campagne di irruzione nei depositi e di sequestri privati cercando di colpire i punti nevralgici della città di Londra ove i pirati si credeva si riunissero.

Abbott reclutò un gran numero di ex agenti di polizia e di lottatori per condurre le operazioni ed il numero di copie sequestrate raggiunse presto centinaia di migliaia. Non sempre i pirati non opposero resistenza dinnanzi a procedure sicuramente irrituali e persino illegali. Adrian Johns[72] ricorda, esemplificando, che un pirata venne affrontato sulla sua soglia di casa dagli uomini dell'MCA i quali si fecero strada minacciando l'uso della forza ove vi fosse stata opposta resistenza. L'episodio venne sottoposto al vaglio del magistrato locale, qualificando la fattispecie concreta come una "aggressione". Il tutto si concluse con un rimprovero; tuttavia, dal magistrato venne affermato che la politica dell'MCA si riduceva ad una forma di "teppismo organizzato". Tale affermazione entrò ben presto nell'armamentario retorico di coloro che si opponevano alle tattiche ferree dell'MCA[73]. L'MCA nel procedere individualmente ad azioni mirate di polizia privata ed offensive antipirateria intendeva rendere la questione oggetto di interesse per la politica nazionale.

L'obiettivo dell'MCA ebbe realizzazione nell'ottobre del 1902 ove una nuova normativa sul *copyright* musicale venne emanata[74]. Questa legge andava a trasformare le azioni private antipirateria in azioni pubbliche, consentendo alla polizia di procedere a sequestro del materiale pirata. Il numero dei sequestri impennò radicalmente tanto che nei soli tre mesi seguenti le stazioni di polizia furono invase da settecentocinquantamila copie di spartiti musicali in attesa di distruzione[75]. Apparve subito chiaro che il flusso delle copie pirata non si sarebbe arrestato. Nel febbraio del 1903, quattro mesi dopo l'entrata in vigore della nuova legge, la polizia ne sospese l'applicazione. Era chiaro che la strategia doveva essere differente. L'MCA aveva perso la lotta.

Con l'MCA uscita ufficiosamente di scena divenne il momento per l'MPA di assumersi il testimone. Il rappresentante per la lotta antipirateria dell'MPA era William Arthur Preston. Egli mise in moto una strategia standard con cui affrontare i suoi avversari. Avvertito della presenza di pirati in un certo luogo, Preston vi si recava personalmente accompagnato dalle certificazioni attestanti i diritti autorali presentate alla Stationers' Hall di Londra. Queste certificazioni costituivano la base legale per poter ottenere legittimamente un ordine di perquisizione dal magistrato locale. Procedeva dunque con l'aiuto delle autorità di polizia ad ispezioni e sequestri ed intentava causa contro i pirati. Le iniziative più significative divennero quelle che miravano a colpire i centri di distribuzione del materiale contraffatto il quale sarebbe stato poi commerciato da venditori ambulanti. Il più famigerato dei centri di smistamento era forse quello del pub Rose & Crown nell'East End londinese. Vi teneva banco un gestore appellato Tum Tum che si riforniva da un deposito poco lontano in Compton Passage. La preda più grossa era tuttavia il pirata in persona, il clone illegale

---

[72] A. JOHNS, *ibidem,* 442-448.

[73] Per una più completa ricostruzione si veda: J. COOVER, *Music Publishing, Copyright, and Piracy in Victorian England: A Twenty-five Year Chronicle, 1881-1906, from the Pages of the Musical Opinion & Music Trade Review and Other English Music Journals of the Period*, Mansell, 1985.

[74] Musical (Summary Proceedings) Copyright Act 1902 (2 Edw. VII c. 15) e Musical Copyright Act 1902. In vigore formalmente fino al 1956, Esso prevedeva che il titolare del diritto d'autore su un'opera musicale potesse rivolgersi ad una *court of summary jurisdiction* con la prova che copie senza licenza dell'opera venivano "*hawked, carried about, sold or offered for sale*". Conseguentemente il tribunale poteva ordinare ad un agente di polizia di sequestrare queste copie senza mandato e portarle dinanzi al tribunale. Ove dimostrato che le copie non erano autorizzate, il tribunale avrebbe potuto ordinarne la distruzione o la consegna al titolare del *copyright*.

[75] Tutti i riferimenti storici della vicenda possono essere rinvenuti con dovizia di particolari in A. JOHNS, *Pirateria: storia della proprietà intellettuale da Gutenberg a Google,* cit., 429-463

dell'editore, quello che Adrian Johns chiama il "capitalista criminale". E venne catturato: era la Vigilia di Natale del 1903.

3.2. L'offensiva del 24 dicembre 1903

Le linee ferroviarie di Londra si intersecano nella grande stazione vittoriana della Città, gli archi che sottostanno ai viadotti cittadini sono stati spesso convertiti in magazzini ed officine di vario genere. Abbott immaginava che fra questi archi si nascondesse un pirata. Il 24 dicembre fu pronto a lanciare la sua offensiva: munitosi di un mandato emesso dalla Corte di Giustizia di Hackney procedette ad una irruzione nelle arcate. L'oggetto del sequestro fu enorme, quasi settantacinquemila spartiti contraffatti in procinto di essere smistati nella rete di distribuzione pirata attraverso le rotaie. Il nome del pirata era James Frederick Willetts[76], colui che riforniva Tum Tum del Rose & Crown.

L'offensiva del 24 dicembre fu solo la prima di una lunga serie di attacchi che si protrasse per tutto l'anno seguente con emersione di un sistema illegale di produzione e smercio di portata nazionale gestito proprio da Willetts. Il numero di offensive e la portata dei bottini in termini di copie pirata costrinsero nuovamente nel 1904 il Parlamento ad intervenire con una Commissione per le audizioni che avrebbe dovuto tentare di risolvere il problema. Abbott e Preston vennero ascoltati ma quello che ha dell'inaudito fu che anche Willetts, autoproclamatosi "Re dei Pirati" venne ascoltato[77]. La sua deposizione si concentrò in una difesa straordinaria della pirateria, condannando i prezzi proibitivi per le classi operaie degli spartiti musicali, rivolgendo la sua imprenditorialità a classi sociali trascurate dalle case editrici. Chiedeva che venissero operati dei cambiamenti significativi, il cartello degli editori non poteva più ostacolare la formazione musicale della Nazione. Willetts sosteneva che la pirateria rivestiva una fondamentale funzione sociale, non solo come già visto forniva accesso alla musica ad un prezzo economicamente vantaggioso per coloro che non se la sarebbero potuta permettere, ma altresì dava lavoro a migliaia di persone in un momento in cui il lavoro era cosa ambita da molti.

Per quanto astrattamente le idee di Willetts potessero quasi apparire lodevoli, la Commissione parlamentare non avvalorò nessuna delle tesi del "Re dei Pirati" ed anzi concluse i suoi lavori con una legge antipirateria ancora più restrittiva. Eppure, le tesi di Willetts fecero breccia nella stampa di settore ed anche in Parlamento, tanto che i pirati poterono contare sull'appoggio in Parlamento di James Caldwell un radicale originario di Glasgow.

3.3. Il crimine di cospirazione

Insieme alla tesi di Willetts, caldeggiata da Caldwell, la Commissione parlamentare sulla pirateria musicale si confrontò altresì con una ulteriore proposta per contrastare il fenomeno. A patrocinio di tal tesi vi era l'avvocato Sir Harry Poland. Egli osservava che era difficile o concretamente infattibile perseguire i pirati per violazione del *copyright*. Sosteneva infatti che i pirati commettevano in realtà un vero e proprio crimine nell'organizzarsi e far fronte

[76] Riferimenti alla figura possono essere rinvenuti sia in A. JOHNS, *Pop music pirate hunters,* Cambridge MA, 2002, disponibile presso: «https://www.amacad.org/publication/pop-music-pirate-hunters» (Ultimo accesso: 10 maggio 2022), che in A. JOHNS, *Pirateria: storia della proprietà intellettuale da Gutenberg a Google*, cit., 428 e ss.

[77] I riferimenti possono essere rinvenuti in J. COOVER, *Music Publishing, Copyright, and Piracy in Victorian England: A Twenty-five Year Chronicle, 1881-1906, from the Pages of the Musical Opinion & Music Trade Review and Other English Music Journals of the Period*, cit.

comune per perpetrare le loro gesta: il crimine di cospirazione. La tesi non venne presa seriamente in considerazione dalla Commissione parlamentare, ma fece breccia presso William Boosey, cacciatore di pirati per la Chappel & Co., che iniziò a pensare alla possibilità di perseguire l'atto di organizzazione in sé considerato.

Nel 1905 ne scaturì un processo che vedeva come imputati molti soggetti le cui attività di pirateria erano risultate legate da un vincolo organizzativo con Willetts. Essi furono incriminati di cospirazione per essersi organizzati al fine di produrre, pubblicare e distribuire il materiale contraffatto. Willetts venne condannato a nove mesi prigione, ogni difesa si dimostrò inutile[78].

Gli editori musicali avevano vinto, la pirateria non venne definitivamente debellata come è facile immaginare; tuttavia, divenne un fenomeno più marginale e meno preoccupante in questo ambito. Gli editori ebbero la meglio quando impararono a comprendere che la pirateria non consisteva meramente in una immoralità ma era un fenomeno complesso di radicate reti sociali comprendenti canali propri di comunicazione ed una ideologia a sorreggerne l'operato. L'accusa di cospirazione funzionò per aver identificato il problema non già nel materiale contraffatto di per sé considerato ma per aver riconosciuto la fondamentale dimensione reticolare della pirateria.

L'importanza storica dell'aneddoto sopra proposto riposa, in primo luogo, nel valore dell'operato di Preston ed Abbott. Essi diedero vita alla prima forza di polizia privata di larghe dimensioni impiegata per il contrasto della pirateria, sfruttando le pieghe dell'ordinamento a loro vantaggio. Non a caso queste vicende possono essere interpretate come un anello di congiunzione fra esperienze più e meno attuali. In *incipit* di questo capitolo si è avuto modo di evidenziare come esperienze similari fossero già presenti, *in nuce,* nell'operato degli ispettori della Stationers' Company, sebbene con intensità differente dal "*commando*" addestrato da Preston ed Abbott. L'iniziativa di quest'ultimi si inserisce storicamente in un contesto molto fecondo in quanto sia nel Regno Unito che negli Stati Uniti si stavano formando le prime agenzie di investigatori privati come la Pinkerton[79], dimostrando il loro valore uguale se non maggiore di quello delle forze di polizia ordinamentali. Ancora oggi il settore dei corpi privati antipirateria, seppur con specializzazioni digitalizzate, è un settore in espansione.

Una seconda notazione riguarda il fatto che si scopre che la pirateria non è solo frutto di macchinazioni truffaldine di artigiani e stampatori mossi dal dio denaro ed intenti a sottrarre fette di mercato ai concorrenti per mezzo di prezzi ribassati dovuti a risparmi illeciti nella produzione. La figura di James Frederick Willetts appare connotata da un'aura politica, ideologica. Anche questa visione della pirateria costituisce una non scontata linea direttrice del pensiero odierno su queste tematiche, ammantando spesso proposizioni di abbattimento

---

[78] Riferimenti al dibattimento processuale possono essere rinvenuti presso J. COOVER, *Music Publishing, Copyright, and Piracy in Victorian England: A Twenty-five Year Chronicle, 1881-1906, cit.*; A. JOHNS, *Pirateria: storia della proprietà intellettuale da Gutenberg a Google*, cit., 428 ss. Ulteriori riferimenti rinvenibili sul sito «https://www.oldbaileyonline.org/browse.jsp?foo=bar&path=sessionsPapers/19060108.xml&div=t19060108-188» (Ultimo accesso: 10 maggio 2022), il quale riporta integrali trascrizioni delle deposizioni degli imputati.

[79] La Pinkerton National Detective è un'agenzia di investigazione privata fondata nel 1850 negli Stati Uniti da Allan Pinkerton. Il suo successo, e motivo per cui è divenuta famosa nella cultura popolare, è dovuto alla vicenda storica della scoperta del complotto per l'assassinio di Abraham Lincoln. L'agenzia, ancora operante, offre numerosi prodotti e servizi, visionabili presso «http://www.pinkertons.com» (Ultimo accesso: 10 maggio 2022), fra cui anche forme di Corporate Investigations, compresi servizi antipirateria e contraffazione («https://pinkerton.com/investigations/corporate-investigations» (Ultimo accesso: 10 maggio 2022)).

dei sistemi del *copyright* con retoriche di libertà e controllo, di mass media e free software ed in fin dei conti di *privacy*[80].

Una terza notazione riguarda quello che ha segnato la storia della pirateria e dell'antipirateria da allora in avanti, ossia, come segnala Adrian Johns, l'alleanza destinata a durare fra il mondo degli affari, i servizi dell'informazione, le operazioni di polizia e la proprietà intellettuale. Alleanze che ancora oggi sono chiaramente ed evidentemente riprese anche nel panorama normativo europeo e nazionale. A dimostrazione di quanto affermato basti un breve cenno all'art. 17 della nuova Direttiva UE 2019/790 il quale, sebbene non esplicitamente, prende atto del fatto che la tecnologia di riconoscimento dei contenuti è oggi comunemente utilizzata per gestire l'uso dei contenuti protetti dal diritto d'autore e velatamente, ma non troppo, consiglia l'adozione di tecnologie di riconoscimento basate sul *fingerprinting* per la gestione in rete delle possibili violazioni del *copyright*.

4. La grande guerra dell'oscillazione

Ancora una volta fu il cambiamento tecnologico a portare ad una nuova forma di pirateria. Avvicinando questo episodio ai nostri tempi ed alla nostra sensibilità, si può notare come l'invenzione della tecnologia radiofonica abbia mutato il modo di intendere la pirateria. Se con gli Stationer e con Willetts i pirati erano stampatori, produttori e commercianti, adesso i pirati diventano i cittadini comuni, gli ascoltatori ed in definitiva diventiamo noi.

Negli anni venti del novecento, la radiodiffusione costituì una vera e propria rivoluzione consentendo di trasmettere istantaneamente un messaggio ad un numero indefinito di ascoltatori contemporaneamente. Le questioni che riguardano l'attuale pirateria digitale iniziano a presentarsi, seppur ancora agli albori, proprio in questo momento.

La storia relativa alla pirateria radiofonica solitamente ha due direttrici, una prima è abbastanza nota, ossia la pirateria data dalla illecita trasmissione su frequenze radio, fenomeno che ha investito per primi gli Stati Uniti per poi tornare prepotentemente negli anni sessanta e settanta. Essa è una ulteriore manifestazione di quella pirateria che già si è avuto modo di analizzare in altri contesti storici, una pratica di diffusione e riproduzione, seppur con sue peculiarità.

La seconda direttrice riguarda invece una storia forse meno nota ma non meno essenziale per la comprensione dell'odierno panorama digitale. È la pirateria che ha caratterizzato il Regno Unito e che ha messo in ginocchio l'industria radiofonica: la pirateria degli ascoltatori pirata. Come efficacemente nota Adrian Johns[81], essa è un inedito nella storia del *copyright*, una lesione legata alla ricezione e non invece alla produzione.

La radio nei primi anni '20 divenne parte integrante della vita quotidiana. In Inghilterra il controllo generalizzato sui segnali radiofonici era di competenza del Ministero delle Poste in virtù di una equiparazione con l'autorità in materia di telegrafo. Il ministero, assuntosi la responsabilità della gestione di tale nuovo sistema di comunicazione, limitò sin dal principio la concessione di licenze radio sulla base della dimostrazione di una utilità scientifica. Eppure, molti appassionati e curiosi della nuova tecnologia iniziarono in privato a compiere

[80] Si veda ad esempio il manifesto politico del Partito Pirata, accessibile presso: «https://www.partito-pirata.it/chi-siamo/manifesto/» (Ultimo accesso: 10 maggio 2022), partito che prese le mosse come controffensiva all'offensiva legale mossa dalla Svezia nel 2006 al sito The Pirate Bay. Interessi economici ed ideologie si fondono in un manifesto politico ed economico.

[81] A. JOHNS, *Pirateria: storia della proprietà intellettuale da Gutenberg a Google,* cit., 467-471.

sperimentazioni con macchine fai-da-te di ricezione e trasmissione e molte società cominciarono a richiedere licenze per la trasmissione via etere.

4.1. I pirati sono gli ascoltatori

Fra le principali società impiegate nel campo della sperimentazione via radiodiffusione vi era la Marconi che aveva una proposta rivoluzionaria di gestione dell'etere. Il progetto che la Marconi presentò nel 1922 al Ministero delle Poste prevedeva che la programmazione radio venisse supervisionata dal Governo e che tenesse un registro di acquirenti di apparecchi radio-riceventi. La società avrebbe, secondo il progetto, trasmesso programmi gratuiti per tutti i destinatari dotati di una licenza radiofonica ed offerto alcuni servizi a pagamento per alcuni utenti muniti di speciali apparecchi con apposite sintonizzazioni. Gamme di frequenze differenti sarebbero state dunque messe a disposizione e riservate per i programmi gratuiti, per quelli a pagamento e per gli sperimentatori dilettanti. Gli apparecchi radio sarebbero quindi stati venduti ai consumatori sigillati e già sintonizzati sulle specifiche frequenze a seconda dell'opzione.

Ulteriori società aderirono all'idea della Marconi e con una fitta serie di negoziati si diede origine alla British Broadcasting Company (poi British Broadcasting Corporation, meglio nota come BBC). Essa procedette già nel 1922 ad emettere le prime licenze. Tuttavia, non ebbe il successo sperato, molti cittadini britannici non intenzionati ad acquistare le ancora costose licenze BBC avevano due possibili soluzioni: decidere di fare a meno di una licenza e dunque darsi alla sintonizzazione clandestina oppure chiedere una licenza sperimentale. Questa licenza altro non era che una nuova edizione del permesso rilasciato dal Ministero delle Poste quando ancora la BBC non esisteva. Essa, pur avendo lo stesso prezzo della licenza di abbonamento (dieci sterline), era tuttavia esente dal pagamento del dispositivo; dunque, gli ascoltatori sperimentali potevano liberamente scegliere il dispositivo da acquistare, probabilmente optando per prodotti di importazione a prezzi inferiori e qualità maggiori. Tale agevolazione era chiaramente intesa a fini scientifici e di ricerca, tuttavia, permetteva di ascoltare la BBC a costo decisamente più basso. Adrian Johns nota come, appena vennero emesse queste licenze, molti cittadini britannici si scoprirono "sperimentatori" con grave danno alle casse della BBC.

Il numero dei richiedenti la licenza da sperimentatore fu ingente, superando di gran lunga quelli della licenza ordinaria da ascoltatore. Non si era in grado, tuttavia, di distinguere un vero sperimentatore da un pirata. Il Ministero delle Poste allora propose di ritenere un vero sperimentatore colui che costruiva un ricevitore. Il presupposto alla base del criterio era che un cittadino britannico abbastanza competente da riuscire a creare un ricevitore sarebbe stato ritenuto anche capace di compiervi sperimentazioni. Non sorprende dunque che non si dovette attendere molto per la comparsa delle prime istruzioni per la costruzione di una radio fai-da-te[82]. Sia gli ascoltatori clandestini che gli sperimentatori erano costretti per natura ad aprire gli apparecchi radio per apportarvi delle modificazioni cercando di incrementare la ricezione per il tramite di una tecnica di risonanza detta "reazione" che tuttavia come effetto collaterale provocava un suono distorto e straziante. Il fastidioso effetto era noto come "oscillazione". Essenzialmente accadeva che l'antenna procedeva ad irradiare onde in uscita

[82] In via esemplificativa si faccia riferimento a quanto apparso nel *The Radio Times*, in particolare al volume 2 numero 15 del 4 gennaio 1924, pagina 12, in cui si fa riferimento alla costruzione di un apparecchio radio ed alla pubblicizzazione di un manuale intitolato "*Building with RADIOBRIX*": «https://genome.ch.bbc.co.uk/page/dd4daf21915044e5b1f838eee6823b89?page=12» (Ultimo accesso: 10 maggio 2022).

dall'altoparlante causando interferenze per gli ascoltatori della zona circostante, un ululato che rendeva inascoltabile la programmazione radiofonica[83].

La standardizzazione degli apparecchi come originariamente pensata dalla BBC era intesa anche a ridurre tale effetto ma chiaramente gli ascoltatori pirata non fruivano di questa standardizzazione e gli sperimentatori ne erano per legge e per licenza esenti. Il problema dell'oscillazione era concreto, rendeva essenzialmente inascoltabili i programmi radio ed era frutto di continue lamentele alla BBC. Contro questo fenomeno, per arginare il disturbo, vennero proposte almeno tre strategie risolutive[84].

La prima ipotesi consisteva nel rivolgersi alla polizia, al ministero ed alla forza pubblica per scoprire chiunque si rendesse responsabile di tali oscillazioni. Ove il presunto pirata avesse a disposizione una licenza BBC sarebbe stato più semplice in quanto la licenza prevedeva che i funzionari potessero ispezionare l'apparecchio radio del titolare. Il presupposto però rimaneva che le oscillazioni più gravi erano quelle degli ascoltatori pirata tout-court ed ispezionare le loro case sarebbe stato una violazione delle libertà costituzionali. Se si fosse contestata una violazione di domicilio l'azione sarebbe stata più dannosa che utile e la stampa era pronta ad attaccare la BBC per questo.

Una seconda strategia puntava sulla forza dell'informazione[85]. Dato che l'oscillazione dipendeva da apparecchi mal sintonizzati sarebbe stato astrattamente possibile informare gli utenti ed istruirli nel sintonizzarsi meglio. La BBC procedette quindi alla diffusione di molte brochure informative con anche vignette che rendevano esplicito il messaggio. La strategia dell'educazione parve in un primo momento avere effetti benefici, nel 1925 le oscillazioni diminuirono ma non sparirono del tutto.

L'ultima strategia era quella che ai nostri fini dimostra la maggior rilevanza. Far fronte ad un problema tecnologico con la tecnologia come vedremo avvenire con sempre maggior vigore anche ai giorni odierni.

4.2. Il rilevatore di oscillazioni

La strada da percorrere allora sembrava quella di costruire un congegno meccanico capace di localizzare le oscillazioni e, per estensione, i responsabili del fenomeno. La soluzione era quella di sfruttare un radiogoniometro per triangolare la posizione dell'oscillatore. Il radiogoniometro consiste di un ricevitore radio mirato al rilevamento della direzione di provenienza delle trasmissioni che riceve, per mezzo dell'utilizzo di antenne radio direzionali. L'uso era originariamente destinato alla navigazione militare per poter dare direzioni e posizioni anche in condizioni di scarsa visibilità. Il primo radiogoniometro è stato

---

[83] Si può fare riferimento ai molti articoli apparsi nel *The Radio Times*, in particolare al volume 2 numero 15 del 4 gennaio 1924 accessibile presso: «https://genome.ch.bbc.co.uk/page/dd4daf21915044e5b1f838eee6823b89?page=1» (Ultimo accesso: 10 maggio 2022) in cui in prima pagina si tratta del problema dell'oscillazione.

[84] Approfondito resoconto sulla questione dell'oscillazione e dell'implementazione delle strategie di contrasto adottate dalla BBC è rinvenibile in A. JOHNS, *Pirateria: storia della proprietà intellettuale da Gutenberg a Google*, cit., 478 e ss.

[85] Si può fare riferimento ai molti articoli apparsi nel *The Radio Times*, accessibili in versione integrale presso: «https://genome.ch.bbc.co.uk/page/dd4daf21915044e5b1f838eee6823b89?page=1» (Ultimo accesso: 10 maggio 2022) in cui in prima pagina si tratta esattamente del problema dell'oscillazione. Altri numeri degli anni '20 sono accessibili presso «https://genome.ch.bbc.co.uk/years/1924» (Ultimo accesso: 10 maggio 2022). In particolare, nell' "*Issue 15, Friday, 4th January 1924, National edition, volume 2*" si legge in prima pagina "*OSCILLATION: A WARNING*" in cui si dà conto della vastità del problema e delle misure informative oggetto della pianificazione della BBC.

progettato nei primi anni del XX secolo dall'ingegnere italiano Ettore Bellini e dal capitano della Regia Marina Alessandro Tosi, ma ben presto l'uso si diffuse in ambito anche civile.

L'utilizzo di questo strumento avrebbe potenzialmente permesso di risolvere il problema degli ascoltatori clandestini. Inoltre, sciolta la British Broadcasting Company nel 1926 e creata la British Broadcasting Corporation, conservata fino ad oggi, si modificò anche il regime delle licenze. L'emittenza britannica si sarebbe basata su una licenza uniforme imposta a tutti gli utenti di una radioricevente. Da questo momento in poi la distinzione fra gli ascoltatori legittimi ed i pirati sarebbe stata netta con l'eliminazione della categoria dubbia degli sperimentatori. Il radiogoniometro, dunque, avrebbe dedotto dall'equazione gli sperimentatori e stanato tutti gli ascoltatori pirata.

Il piano che venne proposto fu quello di creare dei veicoli adibiti al trasporto di antenne. Ove il veicolo avesse puntato la casa di un oscillatore grazie alla triangolazione sarebbe riuscito a rinvenire il pirata.

Nel 1926 due veicoli di prova vennero posti all'opera, presentavano sul tettuccio un'antenna di grandi dimensioni a gabbia circolare che poteva essere ruotata per mezzo di un manico che scorreva nel furgone dove un operatore procedeva a puntarla ed a ridirezionarla. Adrian Johns così ne descrive il funzionamento: "*La procedura prevedeva di parcheggiare il furgone in qualche punto all'interno del raggio dell'interferenza, sintonizzare l'antenna così da rilevare il caratteristico ululato e ruotare l'antenna circolare fino a che il segnale non raggiungeva un minimo. A quel punto l'operatore poteva tracciare una linea su una mappa della località, orientandola in direzione della fonte. Quindi, tramite una bussola di bordo (recuperata da un sottomarino residuato di guerra), il navigatore guidava il conducente fino ad un secondo punto, dal quale veniva presa una seconda lettura; e poi verso un terzo. Insieme, queste tre indicazioni identificavano una zona triangolare di circa 180 metri per lato, che gli addetti ai lavori ribattezzarono presto il "tricorno". A questo punto il furgone percorreva il bordo del triangolo "pettinandolo", ovvero ripetendo la procedura di triangolazione fino ad isolare un tratto di strada, l'operatore poteva perfino identificare la casa da cui proveniva l'oscillazione. I due agenti potevano allora bussare alla porta dell'abitazione incriminata e notificare al trasgressore il suo comportamento antisociale*[86]".

Fortunatamente l'operazione non divenne mai così efficace da risultare sinistra, da degenerare in una sorveglianza di ascendenza orwelliana. Un esempio utile nel mondo del P2P e delle nuove forme di sorveglianza a dimostrazione che le strategie odierne di *enforcement* del *copyright*, per quanto sicuramente innovative, affondano le proprie radici in pregresse esperienze, perfezionando metodi e strumenti già presenti.

L'importanza di questo aneddoto è evidente, costituendo una tappa obbligata nella definizione della pirateria come oggi la intendiamo. Nel momento storico così affrontato si rinvengono già operazioni strategiche che poi verranno ad emersione più compiutamente, come vedremo, sul finire del secolo. Anche in questo caso, almeno tre possono essere le considerazioni sull'utilità dell'esempio.

Una prima notazione riguarda il cambio di paradigma nell'intendere la nozione di pirata. Negli esempi già sviluppati in precedenza, i pirati erano gli stampatori, i commercianti, persino i farmacisti, ma in ogni caso erano soggetti che, violando un altrui preteso monopolio, si industriavano in attività commerciali con danno all'altrui mercato. Non era quindi il cittadino comune ad essere tacciato di questa immoralità, ma il produttore disonesto che nella propaganda del tempo agiva nei vicoli cittadini, nel buio dei quartieri malfamati. Con la radio il pirata, pur in parte rimanendo sicuramente anche quello commerciale, diventa un altro soggetto: l'ascoltatore. L'indicazione, dunque, dimostra che sin dai primi del '900 e

[86] A. JOHNS, *Pirateria: storia della proprietà intellettuale da Gutenberg a Google,* cit. 467-522.

fino ai giorni nostri l'attività che inizia a preoccupare è quella della massa di fruitori di prodotti intellettuali, la stessa massa che sarà oggetto delle azioni e dei dibattiti sul finire degli anni sessanta e settanta per il nastro magnetico e poi per le tecnologie *peer-to-peer*.

Una seconda considerazione riguarda la dimensione tecnologica. Fra le strategie di contrasto che sono state succintamente elencate in precedenza, l'unica ad essere stata attuata con un qualche successo fu quella tecnologica. Si inizia a pensare al fatto che gli strumenti consueti di *enforcement* del diritto d'autore non siano idonei a stanare i pirati ed a colpire un così gran numero di soggetti. La risposta della BBC sembra sinistramente familiare, ricorda quello che sul finire del secolo divenne la tecnologia anticopia per le videocassette. Di *Digital Rights Management* e sistemi tecnologici di *enforcement* dei diritti ancora si sente la costante presenza.

Una terza notazione, connessa strettamente alle precedenti due riguarda la dimensione invasiva della tecnologia di sorveglianza, sembrando quasi una profetica annunciazione di strumenti futuri. Non potendo fisicamente entrare nelle case degli utenti con i mezzi legalmente conosciuti della perquisizione o dell'ispezione, si decise di farlo con la tecnologia. È forse questo meno invasivo della sfera di privata? Ed è su queste basi che, come vedremo, il diritto alla privacy ed alla riservatezza troverà lo spazio per fortificarsi. È una prima indicazione, per quanto iniziale, di una linea di tendenza dei moderni sistemi di *enforcement* che al giorno d'oggi investe in particolare l'utente della rete e costantemente chiede di trovare corretti bilanciamenti fra contrapposti interessi.

5. Pirateria Domestica: il nastro magnetico dall'audio al video

La pirateria come descritta in precedenza ha messo spesso in gioco la rilevanza della "casa" ed il suo status politico e sociale. Dal XVII secolo ad oggi gran parte delle dispute sulle azioni antipirateria e sui meccanismi di *enforcement* del diritto d'autore dipesero dalla percezione della sacralità della casa e di quanto accadeva dietro le private mura e quanto invece sarebbe dovuto accadere. Indubbio quindi che si sia resa sempre necessaria una considerazione sul modo in cui la "vigilanza", per non dire sorveglianza, dovesse avvenire all'interno della casa e della proprietà privata in genere in democrazie che si professano garantiste e liberali.

Fu la duplicazione domestica su nastro che sconvolse l'industria musicale sul finire del XX secolo, forse con conseguenze economiche persino più significative di quanto non fosse avvenuto con altre forme di pirateria nelle epoche precedenti.

Ed ancora una volta per quest'ultimo esempio di questa introduzione storica, il punto di partenza è costituito da una invenzione tecnologica: il nastro magnetico[87]. Dalla disfatta della Germania nazista, in seguito alla Seconda Guerra Mondiale, l'America raccolse non solo un'epoca di potenza economica e politica inaudita, ma anche la tecnologia che avrebbe rivoluzionato il modo di ascoltare musica. Quando la dimensione del fenomeno di duplicazione dei nastri divenne al contempo universale e domestica, la proprietà intellettuale dovette fare i conti con la sacralità della casa.

Dagli aneddoti previamente riportati non stupisce che la pirateria che si estrinseca nella duplicazione di prodotti intellettuali possa avvenire fra le mura domestiche. Gli stessi

[87] F. ENGEL, P. HAMMAR, *A Selected History of Magnetic Recording*, ed. *Richard L. Hess*, 2006, liberamente accessibile presso: «https://www.richardhess.com/tape/history/Engel_Hammar--Magnetic_Tape_History.pdf» (Ultimo accesso: 10 maggio 2022).

Stationer londinesi operavano nelle loro officine situate in casa propria. Ma la pirateria come era stata sempre intesa aveva un qualcosa di commerciale a caratterizzarla, era certo il prestigio della categoria e la fedeltà dei testi a muovere gli Stationer, ma più realisticamente erano gli interessi economici monopolistici ed il furto di una fetta di mercato a destare timore. Dal momento che la pirateria era sempre stata considerata commerciale, la duplicazione domestica per uso personale e senza scopo di smercio non appariva in linea con i connotati tipici di questa categoria.

La registrazione domestica di programmi radio prima, la duplicazione dei dischi e poi delle videocassette anche se compiuta per scopi non commerciali iniziò ad essere anch'essa etichettata come pirateria e l'industria musicale sul finire degli anni '70 la trattò come la più grande minaccia che avesse mai dovuto affrontare, tale da poter minare l'esistenza stessa della musica.

Adrian Johns[88] ricorda che la storia della pirateria e della casa sono intrinsecamente connesse. Il significato stesso di casa riguarda concezioni di ordine morale e politico. Nel diventare, sin da epoca rinascimentale, luogo adibito ai mestieri artigianali e professionali aveva acquisito un crisma di decoro morale ed integrità non indifferente. La soglia domestica doveva segnare un'inviolabile linea di demarcazione fra la casa e la strada, fra il privato ed il pubblico. Dagli anni '50 assistiamo tuttavia ad un cambiamento anche della visione della casa, sempre più spesso individuata come un ambito femminile e come spazio aperto alle nuove tecnologie ed agli elettrodomestici tipici del boom economico. In questo contesto la casa smise di essere intesa come luogo del lavoro creativo e divenne spazio dedito al tempo libero senza però perdere per questo l'aura di moralità che circondava gli ambienti casalinghi.

Ed è in questo contesto culturale e storico che l'industria musicale decise di agire con potenza contro i pirati domestici. Da questa unitaria categoria possono distinguersi due generi con implicazioni differenti. Un primo tipo di pirata comprende gli intenditori di musica che, mossi da spinte ideologiche di conservazione di alcuni tipi di musica, scalzati dalla moda dell'epoca, temevano che alcune raccolte andassero perdute. Il secondo invece sarà di maggior interesse per i nostri fini.

5.1. Gli intenditori: la lirica ed il jazz

Adrian Johns definisce questo primo genere di pirateria come "morale". Due generi musicali furono investiti da questa forma di duplicazione massiccia: il jazz e la lirica. La peculiarità del caso è data dal fatto che i pirati erano degli intenditori, dei cultori del genere e quasi dei collezionisti oltre che semplici ascoltatori. Essi coltivavano ancora quel sogno tipicamente illuministico di una raccolta che potesse comprendere l'interezza della produzione musicale. L'accusa mossa da questi pirati, di ordine ideologico, è che le grosse case discografiche avevano trascurato i classici a tal punto che un intero patrimonio musicale era sull'orlo dell'estinzione, legittimando in questo modo la loro azione di riproduzione sotto un'aura di intensa moralità.

Per quanto riguarda la storia del Jazz, un cavillo nella legge statunitense sul *copyright* in vigore dal 1909 agli anni '70 giocava a favore dei pirati[89]. Infatti, mentre il testo di una

[88] A. JOHNS, *Pirateria: storia della proprietà intellettuale da Gutenberg a Google*, cit., 564-604.
[89] Maggiori riferimenti alle origini di questo problema sono rinvenibili in L. GITELMAN, *Scripts, Grooves, and Writing Machines, Representing Technology in the Edison Era,* in *Stanford University Press*, Stanford, 1999, rinvenibile presso «https://nyuscholars.nyu.edu/en/publications/scripts-grooves-and-writing-machines-representing-technology-in-t» (Ultimo accesso: 10 maggio 2022).

canzone, il suo spartito e la melodia rientravano sicuramente entro l'ambito oggettivo di protezione, una registrazione di una canzone aveva un diverso destino. Una canzone registrata poteva essere riprodotta e venduta previo pagamento di una royalty obbligatoria. Tuttavia, le case discografiche interessate a questo tipo di commercio prestavano poca attenzione al *copyright* e l'ASCAP, l'associazione americana dei compositori, autori ed editori, non mostrava interesse negli artisti afroamericani.

Adrian Johns[90] ricorda come il musicista Charles Smith attribuisse le origini della pirateria discografica ad un costume sorto già negli anni venti di collezionare i dischi di jazz. Afferma infatti che al fine di assicurarsi un classico che mancava alla collezione bisognava rimediare con acetati ricavati dalla copia di un amico. Questi esemplari venivano definiti *dubs* e la pratica *dubbing*. Ben presto però la pratica da domestica si trasformò in commerciale[91]. Forse la più conosciuta ed ambiziosa casa discografica "pirata" era la Jolly Roger di Dante Bolletino.

Il vertiginoso aumento di case discografiche indipendenti già negli anni quaranta pose un problema non di scarso conto per le c.d. "*majors*". Ben presto diedero vita a sistemi di ampia distribuzione portando la musica, prima jazz e poi blues, a tutta la nazione. Queste etichette indipendenti iniziarono a comparire nelle classifiche di "Billboard" per poi scalarne la vetta intorno agli anni '50. Inizialmente le *majors* confidavano in un rapido declino del fenomeno, così però non avvenne ed iniziarono campagne massicce di offensiva.

Le case discografiche iniziarono dunque a procedere in modo più aggressivo nei confronti dei pirati e primo fra questi era Dante Bolletino a capo della Jolly Rogers prima e di un gruppo di società dominato dalla Paradox Industries[92] poi. In particolare, l'American Federation of Musicians decise di mettere al libro nero le società di Bolletino per non aver pagato le royalties sui brani riprodotti. Il boicottaggio della AFM consolidò l'identità di pirata di Bolletino e ben presto la cultura della pirateria del jazz collassò.

In via similare, seppur con alcune peculiarità, lo stesso avvenne anche nel mondo della lirica. Rispetto al fenomeno del jazz, nel campo della musica classica le incisioni non derivavano da dischi già realizzati in America, quanto invece da imprecise fonti europee o più spesso da trasmissioni radiofoniche. Quello che le connaturava però era che le opere piratate camuffavano la loro vera origine dietro attribuzione a qualche sconosciuto artista europeo. Come nel jazz, anche nella lirica il mercato di case discografiche minori e pirata era costituito da intenditori che solevano apprezzare le diverse sfumature nelle esecuzioni delle varie arie.

Tutta l'opera di queste etichette pirata si fondava su un'ideologia che abbiamo già avuto modo di apprezzare con James Frederick Willetts, il re dei pirati. Accusando le major discografiche di una servitù al capitale, si ponevano a difesa ed a servizio dell'Arte. Dopo il 1952 l'industria discografica mutò la propria linea di condotta rispetto alla pirateria, riuscendo a compattarsi nella nuova *Recording Industry Association of America* (RIAA) che sarà protagonista anche nel successivo capitolo. La RIAA iniziò ad esercitare numerose pressioni politiche per il *copyright* sulle incisioni ed intervenne con modalità assimilabili a quelle già incontrate con

---

[90] A. JOHNS, *Pirateria: storia della proprietà intellettuale da Gutenberg a Google*, cit, 586 e ss.

[91] Per maggiori informazioni, A. S. CUMMING, *Democracy of Sound: Music Piracy and the Remaking of American Copyright in the Twentieth Century*, in *New York: Oxford University Press,* 2013.

[92] Per maggiori dettagli sulla storia di Dante Bolletino si veda la voce "Paradox" in *The New Grove Dictionary of Jazz,* II edizione, ed. Barry Kernfeld, accessibile presso «https://archive.org/details/grovesdictionar02maigoog/page/35/mode/thumb?view=theater» (Ultimo accesso: 10 maggio 2022).

Abbott e Preston per combattere i fenomeni di pirateria. L'associazione infatti assoldò agenti privati, una sorta di corpo di polizia interno, operante al di fuori di ogni controllo pubblico e ricorse, come vedremo, a tutti gli strumenti giuridici in suo possesso. Sul finire degli anni '60, la RIAA pensava di poter dichiarare vinta la battaglia contro la pirateria commerciale, in declino, ma al suo posto intervenne una nuova ed altra forma di pirateria: quella domestica.

5.2. La sacralità domestica e la pirateria dei nastri su cassetta

Il posto lasciato vacante dalla pirateria commerciale della lirica e del jazz venne presto assunto dalla pirateria domestica, ora resa possibile dalla straordinaria diffusione su larga scala del nastro magnetico. Non solo un mangianastri era presente in tutte le case, ma anche nelle auto ed entro la fine degli anni settanta con il celebre Walkman Sony divenne onnipresente. Con l'avvento delle cassette fu proprio la copia non commerciale a mettere in crisi epocale il settore musicale. Le cassette resero possibile un mondo dinamico di registrazioni domestiche, di scambio di materiale e di diffusione musicale su larga scala.

Il cambiamento non è di poco conto: nel momento in cui la copia era di scarsa qualità e l'attività di contraffazione poteva essere efficacemente contrastata con l'armamentario giuridico a disposizione, il sistema del diritto d'autore ha saputo reggere i colpi della pirateria. Ma il sistema ha iniziato a mostrare le sue falle quando sono comparse tecnologie e strumenti capaci di riprodurre con estrema facilità le opere dell'ingegno [93]. Basti pensare alle fotocopiatrici ed alle videocassette per mezzo delle quali si è potuto, nell'intimità dell'ambiente casalingo e domestico, compiere riproduzioni sempre più fedeli all'originale e della medesima qualità. Il mutato scenario tecnologico ha posto dunque seri problemi di *enforcement* per l'industria musicale.

Questo problema ci interessa più da vicino e alla fine dei conti non dista molto da quanto già incontrato con riferimento agli ascoltatori radiofonici pirata degli anni venti. Anche in questo caso come in quello allora enunciato, non si trattava di un fenomeno facilmente arginabile se non con mastodontiche azioni di polizia della cui legittimità si potrebbe almeno dubitare.

Cedendo alle preoccupazioni della RIAA, negli anni sessanta il Congresso statunitense avviò un dibattito sulla duplicazione domestica e nel giro di pochi anni, nel 1971, promulgò una nuova legislazione in merito[94]. Ma questa nuova legge non corrispose alle aspettative. Essa, infatti, comprese le incisioni audio sotto l'ala protettiva del *copyright* ma si rifiutò di limitare la duplicazione domestica in quanto la copia per fini non commerciali non doveva considerarsi una trasgressione. La misura legislativa, dunque, tracciò una demarcazione fra il commerciale e la duplicazione casalinga. Così facendo il congresso lasciò largo spazio alla dimensione privatistica, la quale assunse l'iniziativa di contrastare quest'ultima forma di pirateria per mezzo della c.d. tecnologia anticopia cui siamo familiari ancora oggi[95]. I giudici si comportarono di conseguenza, pensando che una dispensa per la duplicazione domestica

[93] Per ulteriori indicazioni si faccia riferimento a R. CASO, *Il diritto d'autore dell'era digitale,* in G. PASCUZZI (a cura di*), Il diritto dell'era digitale. Tecnologie informatiche e regole privatistiche,* II ed., Bologna, 2006, 145 e ss.

[94] Pub. L. 92-140, 85 Stat. 391: "*An Act to amend title 17 of the United States Code to provide for the creation of a limited copyright in sound recordings for the purpose of protecting against unauthorized duplication and piracy of sound recording, and for other purposes*" accessibile presso: «https://www.govinfo.gov/content/pkg/STATUTE-85/pdf/STATUTE-85-Pg391.pdf#page=1» (Ultimo accesso: 10 maggio 2022).

[95] Per maggiori notazioni in merito si faccia riferimento a T. GILLESPIE, *Wired Shut. Copyright and the shape of Digital Culture, MIT Press*, Cambridge (Mass.) 2007, 167-193.

esistesse davvero ed il principio della sacralità domestica prevalse su quello dell'*enforcement* del diritto d'autore.

5.3. Dall'audio al video: Il caso Betamax

La crisi connessa al fenomeno della duplicazione domestica rimase confinata entro ambiti circoscritti finché ad essere coinvolte furono solo le tracce audio. La situazione prese velocemente a mutare nel momento in cui fu il turno del video. Non a caso, infatti, l'industria cinematografica hollywoodiana era molto più potente delle etichette musicali e la sua azione era globale. La nuova tecnologia che muove i fili di questa vicenda è la videocassetta[96]. Lo strumento era stato sviluppato dalla Ampex, società californiana, già negli anni cinquanta come strumento per gli studi televisivi; tuttavia, fu la Sony ad inaugurarne una diffusione di massa prima con *l'U-matic* e poi con il *Betamax*.

Poco dopo l'arrivo del Betamax sul mercato, la Universal Studios e la Walt Disney Company decisero di combatterlo. L'Universal inizialmente cercò di affrontare il problema procurandosi un elenco di acquirenti del dispositivo a Los Angeles e mise sulle loro tracce degli agenti investigativi privati. Prontamente, tuttavia, la magistratura statunitense intervenne per impedire tale tracciamento. Sia la Universal che la Disney allora cercarono di compiere indagini circa il modo di utilizzo dei videoregistratori e scoprirono che due potevano essere gli impieghi: il "*time-shifting*" ed il "*librarying*". Mentre il primo consisteva nel registrare un programma per guardarlo in seguito, il secondo era meno innocuo in quanto non comportava solo la mera riprogrammazione ma anche la conservazione del programma. Alla luce delle risultanze, le due società intentarono dunque una causa giudiziaria nei confronti dell'impresa produttrice di videocassette per violazione del *copyright*[97].

I colossi di Hollywood, in particolare, chiesero un risarcimento per i danni subiti ed un'ingiunzione che impedisse la vendita e l'uso di tale tecnologia. La causa venne portata dinnanzi al Nono Circuito californiano. Sostenevano gli attori che i membri del pubblico utilizzavano i videoregistratori venduti dalla Sony per registrare alcune delle loro trasmissioni protette dal diritto d'autore. La domanda presentata all'attenzione della Corte consisteva nel chiedere se la vendita delle apparecchiature di duplicazione al pubblico potesse violare i diritti protetti dalla legge sul diritto d'autore[98].

La Corte Distrettuale aveva inizialmente negato tutti i provvedimenti richiesti dai ricorrenti. Aveva infatti ritenuto che la registrazione di programmi televisivi per uso domestico e non commerciale potesse essere considerata come un "fair use", non costituendo dunque alcuna violazione del *copyright*, ritenendo persino coerente con la politica del Primo Emendamento di fornire il più completo accesso possibile alle informazioni televisivamente trasmesse[99].

---

[96] Per una attenta disamina della storia della videocassetta e del nastro magnetico si faccia riferimento a C. D. MEE, E. D. DANIEL., M. H. CLARK, *Magnetic recording: the first 100 years*, edited by Eric D. Daniel, C. Denis Mee, Mark H. Clark, *IEEE Press New York*, 1999, 124-219.

[97] Sony Corp. of America v. Universal City Studios, Inc., 464 U.S. 417 (1984), liberamente accessibile presso: «https://www.law.cornell.edu/supremecourt/text/464/417» (Ultimo accesso: 10 maggio 2022).

[98] Nel testo originario della sentenza *Sony Corp. of America v. Universal City Studios, Inc., 464 U.S. 417 (1984)* si legge: "*whether the sale of petitioners' copying equipment to the general public violates any of the rights conferred upon respondents by the Copyright Act*".

[99] Nel testo originario della sentenza Sony Corp. of America v. Universal City Studios, Inc., 464 U.S. 417 (1984) si legge "*The District Court concluded that noncommercial home use recording of material broadcast over the public airwaves was a fair use of copyrighted works and did not constitute copyright infringement. It emphasized the fact that the material was broadcast*

In sede di gravame avverso la pronuncia distrettuale, la Corte d'Appello del Nono Circuito degli Stati Uniti, ritenne invece i convenuti responsabili per c.d. "*contributory infringement*", una forma di responsabilità secondaria da violazione del *copyright* che consente di andare a colpire un soggetto per una condotta materialmente svolta da altri, responsabili invece in via diretta. In tal senso allora, colui che consapevolmente induce, causa o contribuisce materialmente alla violazione del diritto d'autore, da parte di un altro, ma che non ha commesso o partecipato agli atti di violazione, può essere ritenuto responsabile per *contributory infringement* se aveva conoscenza, o aveva motivo di conoscere, dell'infrazione commessa dal responsabile in via principale[100].

Avverso la pronuncia d'appello, Sony propose ricorso alla Corte Suprema, la quale riformò integralmente il giudizio di secondo grado procedendo ad escludere qualunque "*copyright infringement*" sulla base della dottrina del "fair use" di cui alla Section 17 US Code, §107.

Brevemente ripercorrendo il ragionamento della Corte, il punto focale era stabilire se, in questo caso, potesse essere imposta a Sony una responsabilità indiretta, una c.d. *"vicarious liability*" ai sensi del Copyright Act. Tale responsabilità sarebbe derivata dall'aver commercializzato un prodotto che, al dire dei resistenti, consentiva principalmente di compiere operazioni di riproduzione di materiale protetto da *copyright*, in violazione dei diritti di esclusiva sui programmi così registrati. Tale responsabilità si sarebbe dovuta basare sul fatto che la Sony aveva venduto apparecchiature con una "consapevolezza rafforzata", definibile in termini di "*constructive knowledge*", del fatto che i suoi clienti potessero utilizzare tali apparecchiature per effettuare tali copie pirata.

La Suprema Corte ricorda come Sony avesse altresì, in vista della vicenda, condotto sondaggi sulle modalità di utilizzo dei suoi apparecchi, sondaggi che avevano dimostrato che l'uso principale della macchina era il c.d. "spostamento temporale", definito dalla Corte come "*time-shifting*"[101]. Come previamente accennato, la pratica consisteva nel registrare un programma televisivo con l'intenzione di vederlo successivamente, per una sola volta, e quindi cancellarlo.

L'analisi della pratica in termini di "fair use" richiedeva, sostanzialmente, di andare a verificare se il Betamax fosse idoneo ad essere utilizzato per fini non illeciti (*substantial noninfringing uses*)[102]. La Corte concluse nel senso che il *time-shifting,* non avendo certamente

---

free to the public at large, the noncommercial character of the use, and the private character of the activity conducted entirely within the home. Moreover, the court found that the purpose of this use served the public interest in increasing access to television programming, an interest that "is consistent with the First Amendment policy of providing the fullest possible access to information through the public airwaves"

[100] Si veda in merito la voce "*Contributory Infringement*" in *Legal Information Institute*, liberamente consultabile presso: «https://www.law.cornell.edu/wex/contributory_infringement» (Ultimo accesso: 10 maggio 2022), con anche riferimenti alle sentenze della Corte Suprema Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913 (2005); Sony Corp. v. Universal City Studios, Inc., 464 U.S. 417 (1984).

[101] Per la definizione di "time shifting", elemento cruciale nella decisione della Corte, si veda il testo della sentenza in versione originale il quale recita: "*Although there were some differences in the surveys, they both showed that the primary use of the machine for most owners was "time-shifting,"—the practice of recording a program to view it once at a later time, and thereafter erasing it. Time-shifting enables viewers to see programs they otherwise would miss because they are not at home, are occupied with other tasks, or are viewing a program on another station at the time of a broadcast that they desire to watch*".

[102] Nel testo originario della sentenza Sony Corp. of America v. Universal City Studios, Inc., 464 U.S. 417 (1984) si legge "*Accordingly, the sale of copying equipment, like the sale of other articles of commerce, does not constitute contributory infringement if the product is widely used for legitimate, unobjectionable purposes. Indeed, it need merely be capable of substantial noninfringing uses*"; "*The question is thus whether the Betamax is capable of commercially significant noninfringing uses. In order to resolve that question, we need not explore all the different potential uses of the machine and determine whether or not they would constitute infringement. Rather, we need only consider whether on the basis of the facts as found by the district court a significant*

finalità di lucro né costituendo una peculiare violazione ai diritti autorali dei resistenti, poteva essere considerato come un fair use.

Tralasciando ulteriori considerazioni prettamente giuridiche della vicenda, se da una parte la decisione della Corte Suprema può sorprendere per aver difeso la dimensione domestica della pirateria, dall'altra invece si comprende la pronuncia se si pone l'attenzione al contesto in cui la decisione venne assunta. In quegli anni, infatti, proliferavano sulla stampa vignette satiriche in cui si ammoniva la popolazione di una imminente istituzione di una forza di video-polizia, in cui si richiamava alla mente la figura del tipico ispettore in soprabito grigio che avrebbe fatto irruzione nelle case degli americani, in cui si ritraevano aeri AWACS che avrebbero sorvolato le aree urbane cancellando le registrazioni con campi elettromagnetici. La prospettiva di una simile invasione dell'ambito domestico sicuramente vogliamo pensare che abbia avuto un effetto nella pronuncia della Corte[103].

La questione del ritenere "fair" o meno il "*time-shifting*" in realtà si risolveva nella considerazione della sacralità domestica e nella minaccia alla privacy insita in qualsiasi condotta mirante a controllare la vita dei consociati all'interno delle loro abitazioni. Il risultato ottenuto in sede giudiziaria allora ripristinò la supremazia della soglia domestica e della privacy dei cittadini, segnando una vittoria, fugace, sulle esigenze di *enforcement* del diritto d'autore. Pareva chiaro: non esisteva, allo stato dell'arte, alcuna base legale per spingere il *copyright* fin dentro le abitazioni private. Queste implicazioni, come vedremo, sarebbero state sfruttate nel passaggio al digitale dalle reti *peer-to-peer*, prima fra tutte Napster[104], poi Grokster[105] e Pirate Bay[106].

La pirateria domestica ebbe uno sviluppo ed una crescita tale da potersi ritenere davvero un fenomeno universale. Le cassette erano sufficientemente economiche da diffondersi anche nei paesi in via di sviluppo e ciò comportò che una duplicazione casereccia spiazzò la pirateria commerciale. Ed i primi patiti degli elaboratori elettronici ripresero e tennero a mente i principi della duplicazione domestica e li applicarono, nella generazione successiva, ai dati digitali.

6. Considerazioni conclusive

In incipit di questo primo capitolo, volutamente dedicato ad un'analisi storica *dell'enforcement* del diritto d'autore si è voluto concordare con Cicerone quand'egli declamava che "*historia vero testis temporum, lux veritatis, vita memoriae, magistra vitae, nuntia vetustatis"*. Dalla selezione aneddotica di alcune vicende storiche, infatti, si vuol trarre un insegnamento:

---

number of them would be non-infringing. Moreover, in order to resolve this case we need not give precise content to the question of how much use is commercially significant. For one potential use of the Betamax plainly satisfies this standard, however it is understood: private, noncommercial time-shifting in the home. It does so both (A) because respondents have no right to prevent other copyright holders from authorizing it for their programs, and (B) because the District Court's factual findings reveal that even the unauthorized home time-shifting of respondents' programs is legitimate fair use"

[103] Per una più compiuta analisi si veda A. JOHNS, *Pirateria: storia della proprietà intellettuale da Gutenberg a Google,* cit., 586-607.

[104] A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (2001), liberamente accessibile presso: «https://casetext.com/case/a-m-records-inc-v-napster-inc-3» (Ultimo accesso: 10 maggio 2022).

[105] MGM Studios, Inc. v. Grokster, Ltd., 545 U.S. 913 (2005), liberamente accessibile presso: «https://casetext.com/case/metro-goldwyn-mayer-studios-inc-v-grokster-ltd-3» (Ultimo accesso: 10 maggio 2022).

[106] CGUE 14 giugno 2017, C-610/15, *Stichting Brein*, liberamente accessibile presso: «https://curia.europa.eu/juris/document/document.jsf?docid=191707&doclang=EN&mode=req&occ=first » (Ultimo accesso: 10 maggio 2022).

segnalare alcune linee di tendenza nell'attuazione del diritto d'autore che si pongono in delicato bilanciamento, se non in conflitto con altri diritti, quali quelli alla libertà individuale, alla privacy ed alla sicurezza nella propria casa.

Sicuramente degno di essere notato è il riferimento costante che si è voluto compiere al cambiamento tecnologico, probabilmente vero motore, assieme agli interessi economici, del mutamento di paradigma giuridico. La vera rivoluzione è stata data dall'invenzione della stampa a caratteri mobili, da cui la visuale di questo elaborato è voluta partire, segnatamente per aver posto fine al problema della irriproducibilità tecnica in serie del testo e dunque aver favorito la nascita delle corporazioni di stampatori, vero nucleo di strategie per l'*enforcement* del diritto d'autore. Soprassedendo tuttavia in questa sede da ulteriori ricostruzioni in campo di *law and technology*, è bene, riassumendo, segnalare quali linee di tendenza, in definitiva, possono essere tratte dalla ricostruzione storica così come affrontata.

Una prima linea direttrice è sicuramente quella riguardante l'autotutela. Essa, pur con diverse caratterizzazioni, è onnipresente nel panorama esaminato. Non si dimentichino infatti i poteri attribuiti agli Stationer dalla Charter del 1557, a mente della quale la gilda "*shall very lawfull as well search, as often as they please, any place, shop, house, chamber or building of any stamper, printer, binder or feller of any manner of books within kingdom of England*" con anche le connesse misure sanzionatorie consistenti nel "*seizing, taking, or burning the foresaid books or things, or any of them printed or to be printed contrary to the form of any statute, act, or proclamation*" [...]"[107]. Parimenti si veda il "*commando*" di polizia addestrato da Preston ed Abbott.

Nell'*enforcement* di matrice privata, nel ricorso all'autotutela si deve segnalare, collateralmente, anche una ulteriore linea di tendenza: l'alleanza con il mondo degli affari. Sono infatti i privati, gli Stationer, i farmacisti, la MCA e la MPA, la BBC, la RIAA i veri protagonisti di questa storia. Sono i privati che cercano forme sempre nuove, mutate nei tempi, di strategie costanti di tutela dei propri interessi economici.

Non da sottovalutare ancore altre direttrici, quali la rilevanza delle norme sociali, degli usi e delle consuetudini in questo campo, ma anche la forte connotazione ideologica che inizia ad ammantare l'operato dei pirati. Due notazioni ancora di estrema importanza. Innanzitutto, si è avuto modo di constatare che la nozione di pirata è mutata nella narrazione dei predetti aneddoti. In un primo momento il pirata era lo stampatore abusivo, in un secondo invece gli utilizzatori finali, gli utenti, gli ascoltatori delle radio e i duplicatori di registrazioni su nastro magnetico. Questo mutamento di percezione costituisce una linea di tendenza fondamentale per i fini di questo elaborato: come si avrà meglio modo di vedere nel capitolo seguente, fra le strategie di *enforcement* più invasive della privacy si annoverano proprio quelle volte a colpire gli utenti finali, gli internauti delle reti *peer-to-peer*. La seconda notazione ancora riguarda l'emergere di forme di protezione tecnologica, *rectius*, l'affidarsi alla tecnologia per l'*enforcement* del diritto d'autore. Questa tendenza è oggi in rapida espansione, dai furgoncini della BBC degli anni '20, quasi un secolo dopo ancora ci si affida alla tecnologia anticopia, ai *Digital Rights Management* in generale ed a sempre nuovi modi di gestione dei contenuti in rete.

---

[107] Sezioni così riprese da E. ARBER, *A Transcript of the Registers of the Company of Stationers of London, 1554-1640 A.D.,* Stationer's Company, London,1875-77. Sui poteri della Company si faccia riferimento anche a H.S. BENNETT, *English Books & Readers 1558 to 1603, Cambridge University Press*, Cambridge 1989; traducendo liberamente il testo citato: "*ordinanze, disposizioni e statuti per il governo dell'arte o del mistero degli stampatori*"; "*sarà ritenuto lecito anche perquisire, con la frequenza che si vuole, ogni luogo, negozio, casa, camera o edificio di qualsiasi stampatore, rilegatore o venditore di qualsiasi tipo di libri all'interno del regno d'Inghilterra"; "sequestrare, prendere o bruciare i predetti libri o cose, o alcuno di essi stampati o da stampare contrari alla forma di qualsiasi statuto, atto o proclama*".

Infine, l'ultima linea direttrice che ci limitiamo a segnalare è quella su cui l'attenzione ricadrà in via privilegiata, seppur non esclusiva, nei capitoli successivi. Essa è quella legata allo scontro, spesso frontale, di queste strategie di *enforcement* con alcuni altri diritti, variamente inquadrabili nei secoli. Dalle perquisizioni degli Stationer ai tentativi di controllo della duplicazione domestica su nastro, si è assistito sempre ad una stessa retorica: l'invocazione della libertà individuale, della sacralità stessa dell'ambiente domestico ed in fin dei conti una delle sfaccettature del complesso diritto alla privacy. Questo è il vero fulcro dell'attenzione che andrà a svilupparsi nei seguenti capitoli.

CAPITOLO SECONDO
DALL'ANALOGICO AL DIGITALE: UN DELICATO BILANCIAMENTO

1. Considerazioni preliminari

Come affermato in chiusura del capitolo precedente, dalla storia si possono trarre numerose linee direttrici utili nell'analizzare il precario bilanciamento fra *l'enforcement* del diritto d'autore e la tutela della riservatezza. Queste tendenze, così come tratteggiate, guidano l'elaborazione anche di questo secondo contributo in cui l'attenzione si dirigerà sulle strategie di tutela dei diritti d'autore nel passaggio al mondo digitale.

In particolare, come si avrà modo di vedere, la legislazione dei Paesi presi in considerazione appare quasi incentivare una vasta attività di sorveglianza e di investigazione privata da parte dei titolari dei diritti d'autore, prospettiva che si ripercuote anche sulla giurisprudenza, chiamata ad attuare un bilanciamento fra diritti costituzionalmente garantiti che pare quasi impossibile.

La motivazione alla base della sorveglianza della pirateria su Internet risiede nella protezione delle opere tutelate da *copyright*, un obiettivo quindi apparentemente lodevole. Tuttavia, *l'enforcement* online del diritto d'autore comporta, come risultato finale, un sacrificio, sotto molti aspetti eccessivo, della privacy degli utenti.

Delle possibili strategie di *enforcement* del diritto d'autore, nel contesto digitale del *peer-to-peer*, ci si concentrerà, in questo capitolo, sulle possibili azioni giudiziarie esperibili dai *copyright holders* per frenare il dilagare del *file-sharing* attraverso la rete. Segnatamente, dopo un breve riferimento alle azioni giudiziarie, di prima generazione, volte ad inibire servizi informativi per il *file-sharing* o la produzione del software che genera le reti *P2P*, l'attenzione ricadrà privilegiatamente sulle azioni giudiziarie e stragiudiziarie volte a colpire gli utenti delle reti *P2P*, in cui la frizione fra contrapposte pretese degli utenti e dei titolari di diritti autorali si sente con maggior vigore. Nel capitolo successivo invece l'analisi andrà a vertere su una terza strategia altrettanto essenziale, ossia la produzione di sistemi di *Digital Rights Management* (DRM) che abilitano la gestione ed il commercio di file associati a misure tecnologiche di protezione che, tra l'altro, possono impedire la copia e la distribuzione non autorizzate[108].

Con questo capitolo, in sintesi, si vuole analizzare come i differenti Stati propongano le proprie soluzioni a questo bilanciamento, passando da una considerazione della legislazione, prima costituzionale e poi ordinaria, per giungere alle pronunce giurisprudenziali ed al diritto vivente.

2. La rete non gerarchica

Al pari di come si è scelto di procedere nel primo capitolo del presente elaborato, anche in principio di questo secondo capitolo l'analisi prende le mosse dai medesimi presupposti: il cambiamento di tecnologia. Il passaggio dall'analogico al digitale rappresenta forse la più grande delle rivoluzioni cui abbiamo assistito come giuristi. Abbiamo infatti dovuto adattare

[108] Le strategie, così come enucleate, sono riprese dall'analisi compiuta da R. CASO, *Il conflitto tra copyright e privacy nelle reti Peer to Peer: il caso Peppermint – Profili di diritto comparato,* 2007, 3 e ss, liberamente accessibile presso: «http://eprints.biblio.unitn.it/1334/» (Ultimo accesso: 10 maggio 2022).

diritti e ragionamenti nati per il mondo della carta stampata al mondo dei *bit*[109]. Le sfide del nuovo millennio e del Web 2.0 stanno portando rapidamente all'emersione novità di assoluto rilievo che pongono il concreto rischio non solo di mettere in crisi le definizioni del diritto, ma anche di infrangere, come l'ultima goccia che fa traboccare il vaso, ogni concezione che di sistematica giuridica sia rimasta.

L'evoluzione che tocca da vicino i temi di questo elaborato riguarda l'emersione delle reti *peer-to-peer* per lo scambio di materiale e di conoscenza per il tramite del sistema conosciuto come *file-sharing*. I sistemi di condivisione di file, introdotti da Napster e poi dominati da Kazaa, sono diventati subito popolari nella comunità online ed una primaria fonte di preoccupazione per le case discografiche che svilupparono ben presto l'obiettivo del perseguimento legale di questi fenomeni.

In prospettiva informatica, il *file-sharing* può essere inteso come quell'attività di condivisone di file all'interno di una rete di elaboratori. Il sistema si può a sua volta suddividere sulla base dell'architettura utilizzata per la gestione dello scambio, potendo alternativamente compendiarsi in forme "*client-server*" ovvero "*peer-to-peer*". Queste reti consentono di rinvenire un file particolare per mezzo di un URI (*Universal Resource Identifier*) e, di conseguenza, una volta identificato, scaricarlo sul proprio supporto.

L'architettura *client-server* consiste in una struttura nella quale genericamente un computer *client* o terminale si connette ad un *server* per la fruizione di un certo servizio. Maggiormente interessante, quantomeno ai fini del presente contributo, è l'architettura *peer-to-peer* in quanto sarà quest'ultima a portare i maggiori problemi in termini di violazione del diritto d'autore e di invasione nella privacy degli utenti della rete, oggetto della più parte delle pronunce giurisprudenziali che in seguito procederemo ad analizzare.

In una *rete peer-to-peer* (P2P) tutti gli utenti hanno le medesime possibilità di scambiarsi file, motivo per cui sono definite "*peer*" ossia "pari". In queste architetture tutti i computer connessi alla rete si comportano simultaneamente come *client* e come *server*.

Infatti, una struttura *peer-to-peer* cancella essenzialmente la divisione gerarchica tra *client* e *server*, ribaltando così l'idea di una rete di *governance* di Internet. Un modello *peer-to-peer* crea una modalità di comunicazione che tratta ogni macchina come entità separata e uguale nella condivisione delle informazioni. Questo modello permette ai singoli computer di interagire tra loro consentendo a un terminale di "chiedere" direttamente ad altri elaboratori un tipo specifico di file. Ciascun computer, quindi, inoltra la richiesta a un secondo livello di macchine, che a loro volta inoltrano la richiesta ad un terzo livello, e così via. Quando il file richiesto viene individuato, viene automaticamente trasmesso all'utente originario. In questo modo, si trasforma ogni nodo della rete sia in *client* che in *server*, consentendo di eseguire un trasferimento (o *download*) di file tramite una connessione diretta[110]. Il modello *peer-to-peer*,

[109] Per una compiuta ricostruzione del diritto nell'era digitale e di come la tecnologia cambi la prospettiva giuridica si faccia riferimento al contributo di G. PASCUZZI (a cura di*), Il diritto dell'era digitale. Tecnologie informatiche e regole privatistiche*, II ed., Bologna, 2006.

[110] S. KATYAL, *Privacy vs. Piracy*, 7 *Yale Journal of Law & Technology* 222, 272-273 (2004), disponibile anche su *SSRN* all'URL: «http://ssrn.com/abstract=722441» (Ultimo accesso: 10 maggio 2022); K. BOWREY, M. RIMMER, *Rip, Mix, Burn: The Politics of Peer to Peer and Copyright Law*, 7 *FIRST MONDAY* 8, (2002), liberamente consultabile presso: «http://www.firstmonday.dk/issues/issue7_8/bowrey/index.html» (Ultimo accesso: 10 maggio 2022).

tuttavia, può presentarsi secondo tre forme: centralizzata, decentralizzata ed infine distribuita[111].

Un esempio, meglio analizzato inseguito, è quello del funzionamento di Napster[112] che può essere preso a paradigma dei c.d. "sistemi centralizzati". Napster consisteva in un sito Web ed un software che insieme consentivano agli appassionati di musica di scambiarsi copie di registrazioni audio. Il sito web di Napster conteneva una *directory* che elencava tutte le registrazioni che potevano essere trovate sui dischi rigidi di tutti i computer dei suoi membri ed un indice di tali registrazioni. Un appassionato di musica che desiderava entrare a far parte della comunità e ottenere l'accesso a tali registrazioni, doveva prima accedere al sito Web e scaricare da esso un software gratuito noto come *MusicShare*. Dopo aver installato il software sul proprio computer, l'utente si iscriveva selezionando un nome utente univoco, in genere fittizio, ed una password. Avrebbe quindi creato sul suo computer una "libreria utente" in cui avrebbe copiato tutte le registrazioni, in genere sotto forma di file MP3, che voleva condividere con altri utenti. Il software da quel momento sarebbe stato posto in correlazione con i server di Napster. Cercando dunque nella *directory* di Napster il nome del file musicale da scaricare, il software avrebbe identificato in quale delle librerie degli utenti connessi al sistema poteva trovarsi una traccia audio corrispondente. A questo punto sarebbe stato possibile scaricare una copia del file direttamente dal computer di un utente e salvarla sul disco rigido dell'altro. Il fatto che i computer dei due utenti fossero in contatto diretto spiega il nome "*peer-to-peer*".

Ora, se solo pochi utenti si fossero impegnati in questa pratica, i proprietari dei diritti d'autore, delle composizioni e delle registrazioni molto probabilmente l'avrebbero tollerata, proprio come avevano tollerato, od erano stati costretti a tollerare, la pratica della pirateria domestica analizzata nel precedente capitolo in merito alle cassette musicali. Infatti, il sorgere dei sistemi di *file-sharing* è connesso a filo doppio al caso Betamax in quanto sulle giustificazioni, o su quanto la società civile aveva dedotto da tali giustificazioni, si basava questa attività.

I sistemi di *file-sharing* possono essere strutturati anche in modo decentralizzato: l'esempio che meglio verrà in rilievo nel proseguo del capitolo è quello di Grokster[113].

---

111 Per maggiori informazioni sui sistemi P2P si faccia riferimento a: A. W.S. LOO, *Peer-to-peer computing: Building Supercomputers with web Technologies*, Springer Verlag, 2007; R. STEINMETZ, K. WEHRLE, *Peer-to-peer Systems and Applications*, Springer Verlag, 2005

112 Per maggiori informazioni sul caso Napster si veda: G. PASCUZZI, *Opere musicali su Internet: il formato MP3* in *Foro it*., 2001, IV, 101-111.; P. AUTIERI, *Il Caso Napster alla luce del diritto comunitario*", in *Luigi Carlo Ubertazzi (ed.), TV, Internet e "new trends" di diritti d'autore e connessi*, 2003; Case Study: *A&M Records, Inc. v. Napster, Inc.*, in *Washington University In Saint Louis, School of Law*, 2013, liberamente accessibile presso: «https://onlinelaw.wustl.edu/blog/case-study-am-records-inc-v-napster-inc/» (Ultimo accesso: 10 maggio 2022); *A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004* (9th Cir. 2001), U.S. Copyright Office Fair Use Index, liberamente accessibile presso: «https://www.*copyright*.gov/fair-use/summaries/a&mrecords-napster-9thcir2001.pdf» (Ultimo accesso: 10 maggio 2022).

113 MGM Studios, Inc v. Grokster, Ltd, 259 F. Supp. 2d 1029 (C.D. Cal. 2003) liberamente consultabile presso: «https://law.justia.com/cases/federal/district-courts/FSupp2/259/1029/2362925/» (Ultimo accesso: 10 maggio 2022); MGM Studios, Inc v. Grokster, Ltd 380 F.3d 1154 (9th Circuit, 2004), liberamente accessibile presso: «https://casetext.com/case/metro-goldwyn-mayer-v-grokster-ltd» (Ultimo accesso: 10 maggio 2022); MGM Studios, Inc v. Grokster, Ltd 545 U.S. 913 (2005), liberamente accessibile presso: «https://supreme.justia.com/cases/federal/us/545/913/» (Ultimo accesso: 10 maggio 2022); per una approfondita analisi del caso si rimanda a F. GIOVANELLA *Copyright and Information Privacy. Conflicting Rights in Balance*, Cheltenham, 2017; D. R LEVIN., *The Future of Copyright Infringement: Metro-Goldwyn-Mayer Studios, Inc. v. Grokster Ltd*, in *John's Journal Legal Comment* 271, 2006; R. AXBERG, *File-Sharing Tools and Copyright Law: A Study of In re Aimster Copyright Litigation and MGM Studios, Inc. v. Grokster, Ltd.*, Volume 35 Issue 1 Fall 2003, *Loyola*

Differiva dai suoi predecessori, in qualche modo, nella struttura. In particolare, era la tecnologia *FastTrack* ad essere decentralizzata. In sintesi, un utente *FastTrack* interessato allo scambio di file avrebbe localizzato, con l'ausilio di un *server* centrale, uno dei set di computer connessi a Internet che fungevano da c.d. "supernodi", coordinando le richieste di ricerca tra *cluster* di utenti. Una volta inserito nel sistema, l'utente avrebbe potuto inviare una richiesta per una particolare registrazione. Se una copia della registrazione richiesta si fosse trovata su uno dei computer degli utenti collegati, sarebbe stata inoltrata alla parte richiedente senza ulteriore coinvolgimento da parte di Grokster.

Il sistema distribuito non si discosta molto da questo quanto a presupposti, con l'unica differenza che vengono meno persino questi supernodi e tutte le strutture si presentano come assolutamente eguali e distribuite uniformemente tanto da essere stato definito anche come sistema "P2P puro"[114].

La necessaria notazione tecnologica così compiuta si dimostra essenziale proprio per comprendere le potenzialità lesive dei diritti d'autore ma anche per comprendere la difficoltà *dell'enforcement* di tali diritti sul mare del web. Infatti, come vedremo, i titolari dei diritti d'autore hanno risposto alla condivisione di file su reti *peer-to-peer* con un'intensa azione di monitoraggio degli utenti. Lo hanno fatto tentando di espandere la legge per controllare la dinamica dell'architettura del *file-sharing*, la privacy delle informazioni e l'anonimato e consentendo ai proprietari dei diritti d'autore di difendere i loro prodotti da usi non autorizzati[115].

Per queste ragioni il riferimento deve passare, come anticipato introduttivamente, a quali strategie di contrasto possano essere adottate dai *copyright holders* per arginare il pericolo posto dalle reti *peer-to-peer* ai rispettivi monopoli.

2.1. Le strategie di contrasto

Non sarebbe possibile nascondere il fatto che le tecnologie di *file-sharing* accennate abbiano sempre avuto un potenziale utilizzo illecito. Per il loro tramite, infatti, è astrattamente possibile scambiarsi sulla rete contenuti protetti dal diritto d'autore commettendo una violazione dello stesso, ed in particolare dei diritti economici di sfruttamento dell'opera ovvero di distribuzione e riproduzione.

Il problema, tuttavia, posto da una tecnologia non gerarchica è che richiede ai titolari dei diritti d'autore di rinvenire delle strategie di contrasto innovative a questa nuova forma di pirateria. In una struttura gerarchica, infatti, *l'enforcement* del diritto d'autore punterebbe naturalmente a cercare di colpire il *server* centrale che pone direttamente in essere la violazione. Le azioni avverso le reti non gerarchiche, invece, hanno dinnanzi a sé un numero potenzialmente infinito di connessioni fra computer legati privatamente l'uno all'altro.

University Chicago Law Journal, 2003, liberamente accessibile presso: «https://lawecommons.luc.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1280&context=luclj» (Ultimo accesso: 10 maggio 2022).

[114] Per maggiori informazioni sui sistemi P2P si faccia riferimento a: A. W.S. LOO, *Peer-to-peer computing: Building Supercomputers with web Technologies*, cit.; R. STEINMETZ, K. WEHRLE, *Peer-to-peer Systems and Applications*, cit.

[115] S. KATYAL, *Privacy vs. Piracy*, 7 *Yale Journal of Law & Technology* 222, 272-273 (2004), disponibile anche su *SSRN* all'URL: «http://ssrn.com/abstract=722441» (Ultimo accesso: 10 maggio 2022).

Come ricorda Roberto Caso[116], le strategie concretamente adottabili possono essere raggruppate in quattro categorie di azioni: *"(a) Aggressive campagne pubblicitarie che mirano a persuadere il pubblico del carattere illecito del file sharing di contenuti protetti dal copyright (tali campagne si basano anche su semplificazioni fuorvianti come quella che punta ad identificare il file sharing non autorizzato con il reato di furto)[117]; (b) Produzione di sistemi di Digital Rights Management (DRM) che abilitano la gestione ed il commercio di file associati a misure tecnologiche di protezione che, tra l'altro, possono impedire la copia e la distribuzione non autorizzate[118];(c) Azioni giudiziarie, di prima generazione, volte ad inibire servizi informativi per il file sharing, e azioni giudiziarie, di seconda generazione, volte ad inibire la produzione del software che genera le reti P2P;(d) Azioni giudiziarie e stragiudiziarie volte a colpire gli utenti delle reti P2P*".

Le strategie che questo contributo si propone di portare si condensano principalmente sulla dimensione giudiziaria che coinvolge l'utente e sui sistemi di gestione digitale dei diritti. In entrambe queste dimensioni, come si avrà modo di dimostrare, *l'enforcement* del diritto d'autore ha capacità invasiva di grande rilievo e comporta una compressione dei diritti alla privacy ed alla protezione dei dati personali, capaci di annullare la riservatezza dei soggetti coinvolti in questi scambi. Come vedremo infatti, riprendendo importanti osservazioni dottrinali[119], la scelta del legislatore si è concentrata, in questa materia, in una privatizzazione *dell'enforcement* del diritto d'autore, incentivando, nei fatti, un largo uso dell'autotutela con connessa compressione della privacy. Infatti, i recenti sviluppi della legge sul diritto d'autore, in particolare il DMCA, hanno invitato i titolari dei diritti d'autore a creare sistemi extragiudiziali di monitoraggio che rilevano, scoraggiano e controllano gli atti di violazione dei consumatori[120].

Inoltre, si avrà modo anche di dimostrare come il bilanciamento fra queste due contrapposte esigenze sia mutevole ed altalenante ed in questo la prospettiva comparata che permea questo elaborato si dimostrerà particolarmente importante.

3. Copyright e Privacy: copertura costituzionale in comparazione

3.1. Dimensione costituzionale del copyright

Prima di procedere all'analisi della legislazione settoriale in tema di *enforcement* del diritto d'autore e di come questa debba essere bilanciata con i diritti alla riservatezza, alla privacy ed alla libertà di espressione, è bene partire da una premessa: sia il diritto d'autore che il diritto alla riservatezza sono diritti fondamentali, internazionalmente e costituzionalmente garantiti. Questa affermazione consente di pensare ad un bilanciamento fra esigenze che si pongano almeno sullo stesso piano, mostrando che una preferenza per l'uno o per l'altro è di difficile realizzazione. Per fugare censure di apoditticità, è bene procedere argomentando una simile affermazione che avrà riverbero, come vedremo, nell'analisi giurisprudenziale.

---

116 R. CASO, *Il conflitto tra copyright e privacy nelle reti Peer to Peer: il caso Peppermint – Profili di diritto comparato,* cit. 3 e ss.

117 In merito, il riferimento compiuto dall'autore riguarda la nota campagna pubblicitaria che si era soliti vedere nei primi minuti di un DVD noleggiato in videoteca, che recitava "*You wouldn't steal this, you wouldn't steal that. You wouldn't steal a movie, right? Movie piracy is stealing. Stealing is against the law. Piracy is a crime*".

118 Per maggiori informazioni si segnala il capitolo successivo al presente, nonché il contributo dottrinale di R. CASO, *Digital rights management: il commercio delle informazioni digitali tra contratto e diritto d'autore*, Padova, 2004, liberamente accessibile presso: «http://eprints.biblio.unitn.it/4375/» (Ultimo accesso: 10 maggio 2022).

119 S. KATYAL, *Privacy vs. Piracy*, cit. 1 e ss.; R. CASO, *Il conflitto tra copyright e privacy nelle reti Peer to Peer: il caso Peppermint – Profili di diritto comparato*, cit. 3 e ss.

120 Per maggiori informazioni si veda S. KATYAL, *Privacy vs. Piracy*, cit. 1 e ss.

In prospettiva comparata, si può notare come già a livello internazionale, sia l'Italia che gli Stati Uniti siano parte di uno dei più importanti trattati internazionali in materia di diritto d'autore: la Convenzione di Berna per la protezione delle opere letterarie e artistiche, conosciuta anche come Convenzione Universale sul Diritto d'Autore[121]. La prima adozione si deve al 1886 e nasceva con l'intento di porre un argine al principio di territorialità del diritto d'autore[122] volendo proteggere egualmente gli autori di tutti i paesi aderenti la Convenzione. Mentre l'Italia fu uno dei paesi firmatari sin dal 1886[123], gli Stati Uniti aderirono alla Convenzione solo nel 1988[124].

Sia l'Italia che gli Stati Uniti sono altresì parte dei trattati WIPO, segnatamente il "WIPO Copyright Treaty (WCT)[125]" ed il "WIPO Performances and Phonograms Treaty (WPPT)[126]" adottati nel 1996. Questi hanno una peculiare rilevanza in quanto concernono principalmente l'impatto delle tecnologie digitali sul diritto d'autore e sui diritti connessi. Gli Stati Uniti ratificarono questi trattati già nel 1998 con il DMCA (Digital Millennium Copyright Act) mentre l'implementazione in ambito italiano è una conseguenza della adozione a livello europeo della Direttiva 2001/29 CE (c.d. Direttiva INFOSOC, legata all'armonizzazione di alcuni aspetti del *copyright* e dei diritti connessi nella società dell'informazione), trasposta nazionalmente con il Decreto Legislativo 9 aprile 2003 n. 68.

Sul piano nazionale invece possiamo notare come in entrambi gli Stati presi in considerazione si possa ritenere che il *copyright* assurga a protezione costituzionale.

Per quanto riguarda gli Stati Uniti, il riferimento obbligato è alla c.d. "IP Clause" o "Copyright Clause"[127] (US Constitution Clause 8, Section 8, Article 1) che recita che il

---

121 Il testo della convenzione è liberamente consultabile presso: «http://www.interlex.it/testi/convberna.htm» (Ultimo accesso: 10 maggio 2022). Per maggiori riferimenti in merito si segnala M. SCIALDONE, *I profili internazionali del Diritto d'Autore*, pubblicato su *Altalex.com*, 2008, liberamente accessibile presso: «https://www.altalex.com/documents/news/2010/03/24/i-profili-internazionali-del-diritto-d-autore» (Ultimo accesso: 10 maggio 2022).

122 Per principio di territorialità si intende il riferimento alla circostanza per cui le normative in materia di diritto d'autore determinano la loro sfera di efficacia spaziale in maniera coincidente con il territorio dello Stato che lo disciplina. Ciò significa non solo che ogni Paese è competente in via esclusiva a regolare le questioni relative all'esistenza, alla titolarità, al contenuto, all'estinzione e alla tutela di una specifica creazione intellettuale nel proprio territorio, ma anche che la tutela così fornita è indipendente da quella eventualmente fornita da altri Paesi. Maggiori informazioni rinvenibili presso: M. FABIANI, *Autore (diritto di),* in *Diritto internazionale privato e processuale,* in *Enc. Giur.*, IV, 1988, 1; N. BOSCHIERO, *Beni immateriali* (dir. internaz. priv. e proc.), in *Enc. Dir.*, Annali, II, 2, 2008, 121 ss.; e FOÀ, *Territorialità degli IP e riparto delle competenze amministrative*, in *Annali it. dir. aut. cult. spett.* (2007), Milano, 2013, 198 ss.; G. MORGESE, *La Normativa Internazionale ed Europea sul Diritto D'autore*, In *La Comunità Internazionale,* Fasc. 4/2014, 569-594 Editoriale Scientifica Srl, liberamente accessibile presso: «https://www.uniba.it/docenti/morgese-giuseppe/pubblicazioni/Articolodirittoautore.pdf» (Ultimo accesso: 10 maggio 2022).

123 Ratifica ed esecuzione della Convenzione in Italia avvenuta con legge 20 giugno 1978 n. 399

124 Il titolo §17 USC venne emendato con il "Berne Convention Implementation Act" nel 1988

125 Il testo del Trattato è liberamente accessibile presso: «https://wipolex.wipo.int/es/text/295166» (Ultimo accesso: 10 maggio 2022).

126 Il testo del Trattato è liberamente accessibile presso: «https://wipolex.wipo.int/en/text/295578» (Ultimo accesso: 10 maggio 2022).

127 Per riferimenti bibliografici sulla "*Copyright Clause*" si faccia riferimento a F. GIOVANELLA *Copyright and Information Privacy. Conflicting Rights in Balance*, Cheltenham, 2017 e la bibliografia citata; in particolare: K. FENNING, *The Origin of the Patent and Copyright Clause of the Constitution* [1929], *Georgetown Law Journal* 1.09; R. OMAN, *The Copyright Muse: A Charter For A Living People* 1987, *University of Baltimore Law Review* 99; E. C. WALTERSCHEID, *To promote the progress of Science and Useful Arts: The Background and Origin of the Intellectual Clause of the United States Constitution* [1994], *Journal of Intellectual Property Law* 1, liberamente accessibile presso: «https://digitalcommons.law.uga.edu/cgi/viewcontent.cgi?article=1070&context=jipl» (Ultimo accesso: 10 maggio 2022); L. RAY PATTERSON, *Understanding the Copyright Clause* [2000], *Journal of the Copyright Society of USA*

Congresso ha il potere di promuovere il progresso della scienza e delle arti utili, assicurando per tempi limitati ad autori e inventori il diritto esclusivo ai rispettivi scritti ed alle rispettive scoperte[128]. Questa disposizione è il fondamento normativo su cui poggiano le disposizioni statunitensi sui brevetti e sul diritto d'autore, sebbene la clausola non utilizzi nessuno di questi termini.

Senza dilungarsi eccessivamente sul significato della clausola e le sue ripercussioni giurisprudenziali, ai fini del presente elaborato basti notare che, elevando il *copyright* a diritto costituzionalmente garantito, procede al tempo stesso ad imprimergli una connotazione utilitaria tentando di bilanciare le esigenze autorali e gli incentivi alla creazione di opere dell'ingegno con la necessità di promuovere il progresso e dunque la libera circolazione della conoscenza[129].

La Repubblica Italiana, nella propria Costituzione, non prevede un articolo assimilabile a quello statunitense; tuttavia, questo non sembra ostacolare una considerazione in termini costituzionali del diritto d'autore. Unico riferimento diretto e non meramente semantico alla proprietà intellettuale si rinviene all'articolo 117 Cost. il quale, fra le materie di competenza esclusiva statale, come risultanti dalla riforma del Titolo V, annovera alla lettera r): "*pesi, misure e determinazione del tempo; coordinamento informativo statistico e informatico dei dati dell'amministrazione statale, regionale e locale; opere dell'ingegno*". La norma è stata interpretata dalla giurisprudenza costituzionale[130] come comprendente tutti i diritti di proprietà intellettuale che quindi confluiscono pienamente nella competenza centrale dello Stato italiano. Nonostante questo richiamo non abbia la forza di fornire al diritto d'autore un'autonoma copertura costituzionale, vi sono altre norme che pur non facendo alcun riferimento diretto al diritto d'autore, indirettamente lo ricomprendono all'interno del loro ambito applicativo. In particolare, l'art. 9 Cost. che promuove lo sviluppo della cultura e la ricerca scientifica e tecnica, l'art. 33 che protegge la libertà delle arti e delle scienze, l'art. 21 e la libertà di espressione ed infine chiaramente l'art. 3 Cost. che nel proteggere l'uguaglianza, formale e sostanziale, fra i cittadini, impone altresì indirettamente la possibilità di creare e pubblicare opere dell'ingegno che sono espressione della dignità umana e costituiscono il pieno sviluppo della persona[131].

365; CRAIG JOYCE, *Introduction* - L. RAY PATTERSON: *Copyright (and Its Master) in Historical Perspective,* 10 J. *Intell. Prop. L.* 239 (2003), liberamente accessibile presso: «https://digitalcommons.law.uga.edu/jipl/vol10/iss2/2» (Ultimo accesso: 10 maggio 2022) o «https://digitalcommons.law.uga.edu/cgi/viewcontent.cgi?article=1256&context=jipl» (Ultimo accesso: 10 maggio 2022).

128 "*To promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries".*

129 Si veda in merito W. FISHER, *Theories of Intellectual Property* in Stephen Munzer, ed., *New Essays in the Legal and Political Theory of Property* (Cambridge University Press, 2001), liberamente accessibile presso: «https://cyber.harvard.edu/people/tfisher/iptheory.pdf» (Ultimo accesso: 10 maggio 2022).

130 Si faccia riferimento, ad esempio, alla sentenza C.Cost. 14 novembre 2008 n. 386 in cui la Corte Costituzionale ha dichiarato incostituzionale la legge della Regione Friuli-Venezia Giulia 2 ottobre 2007, n. 24, cosiddetta "Salva Tocai". Con tale legge, la Regione intendeva consentire ai produttori vitivinicoli regionali l'utilizzo per il vino commercializzato sul territorio italiano della denominazione "Tocai friulano", quale segno identificativo del vino bianco prodotto dall'omonimo vitigno. In particolare, in tale contesto la Corte decise di lasciare da parte la questione relativa alla violazione sostanziale degli obblighi comunitari, questione di cui era stata investita, per affrontare preliminarmente il profilo del riparto interno di competenze tra Stato e Regioni in materia di denominazione geografiche.

131 In questo senso si esprime altresì F. GIOVANELLA, *Copyright and Information Privacy. Conflicting Rights in Balance*, Cheltenham, 2017, 51 ss.

Se questo non fosse sufficiente a dimostrare una copertura costituzionale del diritto, si può altresì fare riferimento alla Carta di Nizza, la quale è oggi vincolante per il tramite dell'attuazione del Trattato di Lisbona[132]. L'art. 17 di detta Carta stabilisce al primo comma che "*ogni persona ha il diritto di godere della proprietà dei beni che ha acquisito legalmente, di usarli, di disporne e di lasciarli in eredità. Nessuna persona può essere privata della proprietà se non per causa di pubblico interesse, nei casi e nei modi previsti dalla legge e contro il pagamento in tempo utile di una giusta indennità per la perdita della stessa. L'uso dei beni può essere regolato dalla legge nei limiti imposti dall'interesse generale*". Icasticamente, il secondo comma proclama: "*la proprietà intellettuale è protetta*". La disposizione è stata interpretata come riconoscimento normativo della proprietà intellettuale e come impegno alla protezione da parte delle Istituzioni europee[133].

Il rapido riferimento alla dimensione costituzionale della protezione del *copyright* serve, ai fini di questo elaborato, per comprendere gli esiti del bilanciamento con l'altro diritto preso a riferimento, ossia la riservatezza. In merito a quest'ultimo, il contesto normativo sembra meno univoco e solo recentemente si è giunti ad una piena considerazione della valenza costituzionale dello stesso. Ed è quindi procedendo di seguito con l'analisi del diritto alla privacy che si vuole tentare di porre le fondamenta su cui basare il successivo bilanciamento e saggiare i differenti esiti in panorama comparato. Infatti, come affermato, il bilanciamento, spesso mutevole, fra questi due diritti avviene fra istanze almeno di pari rango.

È infatti da notare che a livello normativo internazionale, in un mondo caratterizzato da un'intensa globalizzazione e da un abbattimento dei confini nazionali, a causa ed in virtù di Internet e delle tecnologie digitali, una protezione universale per il diritto alla riservatezza od alla protezione dei dati personali non sia ancora esistente. Solamente due testi hanno una rilevanza su questo livello: la Dichiarazione Universale dei Diritti Umani (1948) e le Guidelines della OECD (Organisation for Economic Co-operation and Developement)[134].

In particolare, l'art. 12 della Dichiarazione Universale afferma che "*nessun individuo potrà essere sottoposto ad interferenze arbitrarie nella sua vita privata, nella sua famiglia, nella sua casa, nella sua corrispondenza, né a lesione del suo onore e della sua reputazione. Ogni individuo ha diritto ad essere tutelato dalla legge contro tali interferenze o lesioni*".

---

132 Riferimenti rinvenibili in B. NASCIMBENE, *Carta dei diritti fondamentali, applicabilità e rapporti fra giudici: la necessità di una tutela integrata*, in *European Papers*, Vol. 6, 2021, No 1, 81-99, liberamente accessibile presso: «https://www.europeanpapers.eu/en/system/files/pdf_version/EP_EF_2021_I_009_Bruno_Nascimbene_00453.pdf» (Ultimo accesso: 10 maggio 2022).

133 C. GEIGER, *Intellectual Property shall be protected!? – Article 17 (2) of the Charter od Fundamental Rights of the European Union: a Mysterious provision with an Unclear Scope*, in *European Intellectual Property Review 113*, 2009, liberamente accessibile presso: «https://www.researchgate.net/profile/Christophe-Geiger/publication/43234343_Intellectual_Property_shall_be_protected_Article_17_2_of_the_Charter_of_Fundamental_Rights_of_the_European_Union_a_Mysterious_Provision_with_an_Unclear_Scope/links/56b30e8f08ae795dd5c7dbb0/Intellectual-Property-shall-be-protected-Article-17-2-of-the-Charter-of-Fundamental-Rights-of-the-European-Union-a-Mysterious-Provision-with-an-Unclear-Scope.pdf» (Ultimo accesso: 10 maggio 2022).

134 Dichiarazione Universale dei Diritti Umani, liberamente consultabile presso:«https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/itn.pdf»(Ultimo accesso: 10 maggio 2022); OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data sia nel testo originale: «https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm» (Ultimo accesso: 10 maggio 2022) che in quello rivisto nel 2013: «https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf» (Ultimo accesso: 10 maggio 2022).

Inoltre, nel 1990 le Nazioni Unite hanno adottato delle "Guidelines for the Regulation of Computerized Personal Data Files" [135] e, nonostante non costituiscano un corpo normativo vincolante, sono intese a fornire delle direttrici per l'implementazione nazionale di normative in materia. A livello europeo invece sia la Convenzione Europea dei Diritti dell'Uomo[136] che la Carta di Nizza[137] proteggono la dimensione della privacy.

Per comprendere la sfera applicativa di questo diritto e la forza che lo stesso può giocare se bilanciato con i diritti di proprietà intellettuale, si deve compiere una partita analisi dei sistemi sia statunitense che euro-italiano. Anticipando le conclusioni, possiamo affermare che la differenza nell'approccio avrà riverbero nel differente esito dei bilanciamenti.

3.2. Protezione statunitense del diritto alla riservatezza

L'evoluzione del diritto alla privacy statunitense ha condotto ad una affermazione costituzionale dello stesso da parte della giurisprudenza. Tuttavia, ogni notazione circa il diritto alla riservatezza negli Stati Uniti deve necessariamente fare i conti con i capostipiti della materia: Warren e Brandeis[138]. L'approccio di *law and technology* anche in questa occasione mostra la sua affidabilità, in quanto il *casus belli* da cui prese origine la loro opera riguardava l'introduzione di una nuova tecnologia: la fotocamera portatile e lo "*yellow journalism*". La vicenda ha del personale in quanto oggetto della stampa scandalistica era la moglie di Warren, un avvocato di Boston, figlia a sua volta di un facoltoso politico. Indipendentemente dalle supposte cause della stesura del testo, i suoi autori definirono questo diritto come il "*right to be let alone*". A dimostrazione della sempre e costante interrelazione fra il diritto d'autore e il diritto alla privacy si segnala anche che proprio a giustificazione del loro rinvenimento di questo diritto nel *common law* statunitense tracciarono un parallelismo significativo con il diritto d'autore e con la protezione delle opere dell'ingegno, rinvenendo uno spunto per la loro elaborazione nel diritto d'inedito[139].

In particolare, nel loro articolo si legge che la stampa stava oltrepassando in ogni direzione gli ovvi limiti del decoro e della decenza. "*Il pettegolezzo non è più la risorsa degli oziosi e dei viziosi, ma è diventato un mestiere, che viene perseguito con l'industria oltre che con sfrontatezza. Per soddisfare un gusto lascivo i dettagli dei rapporti sessuali sono diffusi nelle colonne dei quotidiani. Per occupare*

---

[135] Guidelines for the Regulation of Computerized Personal Data Files adottate dalla Assemblea Generale con resolution 45/95 del 14 dicembre 1990, liberamente accessibili presso: «https://www.refworld.org/pdfid/3ddcafaac.pdf» (Ultimo accesso: 10 maggio 2022).

[136] Il riferimento è all'art. 8 CEDU, rubricato come "Diritto al rispetto della vita privata e familiare" il quale dispone: "*1. Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza.2. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui".*

[137] Riferimento agli articoli 7 ed 8 della Carta dei Diritti Fondamentali dell'Unione Europea che dispongono: Articolo 7: Rispetto della vita privata e della vita familiare "*Ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni";* Articolo 8, Protezione dei dati di carattere personale "*1. Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano. 2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica.*"

[138] S. D. WARREN, L. D. BRANDEIS, *The Right to Privacy,* in *Harvard Law Review*, Vol. 4, No. 5. (Dec. 15, 1890), pp. 193-220 disponibile sul sito: «https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf» (Ultimo accesso: 10 maggio 2022).

[139] Per maggiori informazioni si consulti D.J. SOLOVE, M. ROTENBERG, *Information privacy Law,* Aspen Publishers, 2003; D.J. SOLOVE, P.M. SCHWARTZ, *Privacy information and technology,* Aspen Publishers, 2009; F.S. LANE, *American Privacy, the 400-Year history of Our Most Contested Right,* Beacon Press, 2010

l'indolente, colonna su colonna è riempita di pettegolezzi oziosi, che possono essere procurati solo dall'intrusione nella cerchia domestica. L'intensità e la complessità della vita, in attesa dell'avanzare della civiltà, hanno reso necessario un certo ritiro dal mondo, e l'uomo, sotto l'influenza raffinata della cultura, è diventato più sensibile alla pubblicità, così che la solitudine e la privacy sono diventate più essenziali per l'individuo; ma l'impresa e l'invenzione moderne hanno, attraverso invasioni sulla sua privacy, sottoposto l'uomo a dolore mentale e angoscia, molto più grande di quanto potrebbe essere inflitto da un semplice danno fisico." [140]

I suggerimenti di Warren e Brandeis vennero accolti dalla giurisprudenza sul principiare del XX secolo, con prime introduzioni e riconoscimenti che condussero presto ad attirare l'attenzione del legislatore. Solowe e Schwatz[141] richiamano l'attenzione ad uno dei primi casi, ossia Pavesich v. New England Life Insurance[142]. La vicenda riguardava un quotidiano della Georgia che diffuse la pubblicità di una compagnia di assicurazioni, pubblicità ritraente il signor Pavesich senza consenso. La statuizione della Corte ha avuto un significato non indifferente nell'evoluzione della tutela del diritto alla privacy statunitense, potendosi infatti considerare la Georgia come il primo fra gli Stati americani ad aver riconosciuto in via di *common law* una tutela alle istanze di riservatezza. La Corte, infatti, afferma che chi desidera vivere una vita di parziale reclusione ha diritto di scegliere i tempi, i luoghi e le modalità con cui e nelle quali sottoporsi allo sguardo del pubblico. Se ne trae la conseguenza che una violazione del diritto alla privacy costituisce un'invasione diretta di un diritto dell'individuo andando a qualificarsi come illecito[143].

Il diritto alla privacy stava dunque lentamente emergendo nelle pieghe dell'ordinamento e ben presto venne ad assumere una notazione ed una protezione costituzionale. I riferimenti normativi più consoni, infatti, sono il primo ed il quarto emendamento. Il primo emendamento in particolare si riferisce al diritto alla privacy intendendolo come un diritto all'autodeterminazione, mentre il quarto dispone che il diritto del popolo ad essere al sicuro nelle proprie persone, case, carte ed effetti, contro perquisizioni e sequestri irragionevoli, non sarà violato, e nessun mandato sarà emesso, se non per causa probabile[144]. L'utilizzo del quarto emendamento da parte della giurisprudenza statunitense non si fece attendere. Era il 1928 e il giudice era Brandeis.

Nel caso Olmstead v. United States[145] la Corte affermò che per esservi una violazione del quarto emendamento dovesse servire un "*trespass*" ritenendo dunque tale diritto

---

[140] Il testo originario così recita: "*The press is overstepping in every direction the obvious bounds of propriety and of decency. Gossip is no longer the resource of the idle and of the vicious, but has become a trade, which is pursued with industry as well as effrontery. To satisfy a prurient taste the details of sexual relations are spread broadcast in the columns of the daily papers. To occupy the indolent, column upon column is filled with idle gossip, which can only be procured by intrusion upon the domestic circle. The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual; but modem enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury.*"

[141] D.J. SOLOVE, P.M. SCHWARTZ, *Privacy information and technology cit. 1 e ss.*; per una analisi approfondita dei casi che verranno in seguito citati si veda anche F. GIOVANELLA, *Copyright and Information Privacy. Conflicting Rights in Balance*, cit., 135 e ss.

[142] Pavesich v. New England Life Insurance Co., 50 S.E 68 (Ga. 1905), liberamente accessibile presso: «https://casetext.com/case/pavesich-v-new-england-life-ins-co» (Ultimo accesso: 10 maggio 2022).

[143] Riportando il testo originario: "*One who desires to live a life of partial seclusion has a right to choose the times, places, and manner in which and at which he will submit himself to the public gaze […] It therefore follows from what has been said that a violation of the right of privacy is a direct invasion of a legal right of the individual. It is a tort […]"*

[144] Nel testo del quarto emendamento: "*the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized"*

[145] Olmstead v. United States, 277 U.S. 438 (1928), 478, liberamente consultabile presso: «https://supreme.justia.com/cases/federal/us/277/438/» (Ultimo accesso: 10 maggio 2022).

applicabile alla sola proprietà fisicamente intesa. Del caso invece resta la celebre *dissenting opinion* di Brandeis in cui richiede la applicazione del quarto emendamento anche ad altri casi con un argomento curioso: egli afferma che il quarto emendamento fosse da applicare in quanto era posto a presidio della felicità delle persone, dato che i padri costituenti volevano proteggere anche le emozioni ed i pensieri dei cittadini americani introducendo nella costituzione un *right to be let alone*. Ogni intrusione governativa doveva allora considerarsi come una violazione del quarto emendamento. Ma ancor più significativo è il monito che il Justice Brandeis pone nella sua opinion: "*è improbabile che il progresso della scienza nel fornire al governo mezzi di spionaggio si esaurisca con le intercettazioni. Si potranno un giorno elaborare modalità mediante le quali il governo, senza togliere carte da cassetti segreti, le possa riprodurre in tribunale, e mediante le quali sarà messo in grado di esporre a una giuria le vicende più intime della casa. I progressi nelle scienze psichiche e correlate potranno portare mezzi per esplorare credenze, pensieri ed emozioni inespresse*".[146]

Molte altre furono le sentenze[147] che si susseguirono e che andarono a definire un diritto alla privacy come noi oggi lo conosciamo. In particolare, l'opinione di Brandeis venne definitivamente recepita dalla Corte Suprema nel caso Katz v. United States[148] il quale, procedendo ad un *overruling* del precedente Olmstead, arrivò alla conclusione per cui il quarto emendamento "*protegge le persone piuttosto che i luoghi*"[149].

In questa rapida rassegna giurisprudenziale un ultimo caso risulta di interesse, ossia la pronuncia Whalen v. Roe[150] in cui si delinea un concetto di privacy più vicino a quello della sensibilità attuale, andando a toccare il trattamento dei dati personali.

---

[146] Nella parole del Justice Brandeis: "*The progress of science in furnishing the Government with means of espionage is not likely to stop with wire- tapping. Ways may someday be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home. Advances in the psychic and related sciences may bring means of exploring unexpressed beliefs, thoughts and emotions"*

[147] Si vedano ad esempio: Griswold v. Connecticut, 381 U.S. 479 (1965), liberamente accessibile presso:«https://supreme.justia.com/cases/federal/us/381/479/» (Ultimo accesso: 10 maggio 2022); Whalen v. Roe, 429 U.S- 589 (1977) 599, liberamente accessibile presso: «https://supreme.justia.com/cases/federal/us/429/589/» (Ultimo accesso: 10 maggio 2022); Katz v. United States, 389 U.S. 347 (1967), liberamente accessibile presso: «https://supreme.justia.com/cases/federal/us/389/347/»(Ultimo accesso: 10 maggio 2022); Roe v. Wade, 410 U.S. 113 (1973), liberamente accessibile presso: «https://supreme.justia.com/cases/federal/us/410/113/» (Ultimo accesso: 10 maggio 2022); U.S. v. Jones, 132 S. Ct. 945 (2012), liberamente accessibile presso: «https://www.law.cornell.edu/supremecourt/text/10-1259» (Ultimo accesso: 10 maggio 2022); Riley v. California, 136 S. Ct. 506 (2015), liberamente accessibile presso: «https://www.law.cornell.edu/supremecourt/text/13-132» (Ultimo accesso: 10 maggio 2022). Per una completa analisi e riferimenti bibliografici in merito si veda F. GIOVANELLA, *Copyright and Information Privacy. Conflicting Rights in Balance*, cit., 139 e ss.

[148] Katz v. United States, 389 U.S. 347 (1967), liberamente accessibile presso: «https://supreme.justia.com/cases/federal/us/389/347/» (Ultimo accesso: 10 maggio 2022).

[149] Nelle parole della Corte questo è espresso affermando "*people, rather than places*". Il caso è anche importante perché nella *concurring opinion* del Justice Harlan viene delineato un test definito come della "*reasonable expectation of privacy*", in cui afferma "*My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, - first that a person have exhibited an actual (subjective) expectation of privacy and, - second, that the expectation be one that society is prepared to recognize as "reasonable".*

[150] Rispondendo alla preoccupazione che i medicinali venissero deviati in canali illeciti, il legislatore dello Stato del New York, nel 1972, aveva adottato uno schema legale per correggere i difetti della legge precedente che si basava sulla predisposizione e la collezione di moduli dei pazienti. Il modulo in questione richiedeva l'identificazione del medico che effettuava la prescrizione, della farmacia che dispensava il farmaco, del farmaco e del dosaggio, e il nome, l'indirizzo e l'età del paziente, ed il tutto doveva essere archiviato presso il Dipartimento della Sanità dello Stato, dove i dati pertinenti venivano registrati su nastri per l'elaborazione informatica. Tutti i moduli così redatti venivano poi conservati per un periodo di cinque anni e successivamente distrutti. I ricorrenti, dunque, ritenevano che il rapporto medico-paziente fosse una delle "*zone*" di tutela costituzionale della privacy e che le disposizioni di identificazione del paziente della legge avessero invaso

In questa sentenza, nonostante il rigetto delle pretese dei ricorrenti, la Corte Suprema estese il "*right to privacy*" fino a comprendere un "*right to informational privacy"* ossia riconoscendo un diritto dei consociati ad evitare il disvelamento di questioni personali. Il ragionamento si basò sulla considerazione di due interessi: (a) evitare la diffusione di informazioni personali; (b) garantire indipendenza decisionale per particolari questioni importanti.

Nel ragionamento della Corte ha certamente influito anche il pensiero del Professor Kurland[151] il quale afferma che esistono almeno tre sfaccettature del diritto costituzionale alla privacy. La prima forma è costituita dal diritto dell'individuo di essere libero nei suoi affari privati dalla sorveglianza e dall'intrusione del Governo. La seconda è il diritto di un individuo a non vedere i suoi affari privati resi pubblici. La terza è il diritto di un individuo di essere libero nell'azione, nel pensiero, nell'esperienza e nel credo. Mentre il primo diritto è quanto direttamente protetto dal quarto emendamento, gli altri due corrispondono ai due interessi presi in considerazione dalla Corte per delineare una sfera di "*informational privacy*" proteggibile astrattamente grazie al quarto emendamento.

I casi così succintamente delineati dimostrano quindi come, nel panorama statunitense, vi sia stata una evoluzione che dalla dottrina di Warren e Brandeis ha portato l'originario "*right to be let alone*" ad espandere la sua influenza ed il suo ambito oggettivo, garantendo alla privacy una copertura costituzionale. La digressione in termini costituzionali non è peregrina ai fini di questo elaborato, in quanto lo scopo è dimostrare come due diritti, entrambi tutelati costituzionalmente, possano confliggere. E nello scontro fra *l'enforcement* del diritto d'autore e del diritto alla riservatezza gli esiti non sono scontati. Vedremo infatti come i bilanciamenti compiuti siano mutevoli e, in funzione comparatistica, si giunga a diverse soluzioni per i medesimi problemi.

Un'ultima notazione si rende necessaria per definire il *right to privacy* statunitense, ossia il far riferimento alla disciplina civilistica di sua applicazione così come delineata e confluita nel *Restatement of Torts*. L'attenzione ancora una volta si volge alla dottrina ed in particolare all'articolo "*Privacy*" di Prosser[152]. Egli analizza numerosi casi[153] successivi all'articolo di

---

quella zona. La Corte, pur rigettando le pretese dei ricorrenti nota che i casi a volte caratterizzati come tutela della "privacy" hanno coinvolto almeno due diverse tipologie di interessi. Uno è l'interesse individuale ad evitare la divulgazione di questioni personali, ed un altro è l'interesse all'indipendenza nel prendere certi tipi di decisioni importanti. Gli appellati sostengono che entrambi questi interessi sono stati lesi dalla legislazione di New York. La semplice esistenza in forma prontamente disponibile delle informazioni sull'uso da parte dei pazienti dei farmaci crea una genuina preoccupazione che le informazioni diventino pubbliche e che influiscano negativamente sulla loro reputazione. Questa preoccupazione rende alcuni pazienti riluttanti ad usare taluni farmaci e alcuni medici riluttanti a prescriverli anche quando il loro uso è indicato dal punto di vista medico. Pertanto, lo statuto minacciava di compromettere sia il loro interesse alla non divulgazione di informazioni private sia il loro interesse a prendere decisioni importanti in modo indipendente.

[151] La Corte nel caso Whalen v. Roe, 429 U.S. 589 (1977) cita infatti P. B. KURLAND, *The private I*, in *The University of Chicago Magazine* 7, 8 (autunno 1976). Nella versione in lingua originale il testo dispone: "*The concept of a constitutional right of privacy still remains largely undefined. There are at least three facets that have been partially revealed, but their form and shape remain to be fully ascertained. The first is the right of the individual to be free in his private affairs from governmental surveillance and intrusion. The second is the right of an individual not to have his private affairs made public by the government. The third is the right of an individual to be free in action, thought, experience, and belief from governmental compulsion*"

[152] W. L. PROSSER, *Privacy, California Law Review* 383, 1960 liberamente accessibile presso: «https://lawcat.berkeley.edu/record/1109651» (Ultimo accesso: 10 maggio 2022).

[153] Fra gli innumerevoli casi analizzati da Prosser si può certamente ricordare: Roberson v. Rochester Folding Box Co. 171 N.Y. 538, 64 N.E. 442 (1902), liberamente accessibile presso: «https://casetext.com/case/roberson-v-rochester-folding-box-co-1» (Ultimo accesso: 10 maggio 2022), in cui il convenuto si era servito dell'immagine di una giovane senza il suo consenso per pubblicizzare della farina, insieme allo slogan "*La farina di famiglia*". La Corte in questo caso ha respinto la tesi di Warren e Brandeis e ha

Warren e Brandeis e da questi ricava quattro fattispecie di *tort* azionabili giudizialmente. Nelle parole dello stesso autore si legge "*Ciò che è emerso dalle decisioni non è cosa semplice. Non è un illecito, ma un complesso di quattro. La legge sulla privacy comprende quattro distinti tipi di invasione di quattro diversi interessi dell'attore, che sono legati tra loro da un nome comune*[154]".

Queste quattro fattispecie sono: (a) *Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs;* (b) *Public disclosure of embarrassing private facts about the plaintiff;* (c) *Publicity which places the plaintiff in a false light in the public eye;* (d) *Appropriation, for the defendant's advantage, of the plaintiff's name or likeness*[155].

3.3. Protezione euro-italiana del diritto alla riservatezza

Nella storia del riconoscimento di copertura costituzionale del diritto alla riservatezza nel panorama italiano un ruolo di prim'ordine è stato giocato dalla Corte di Cassazione che ha interpretativamente derivato da principi costituzionali una regolamentazione compiuta di questo diritto[156]. I *"leading cases"* in questa materia sono principalmente tre che per la loro fama è sufficiente accennare[157].

---

dichiarato che il diritto alla privacy non esisteva e che l'attore non aveva diritto a nessuna protezione contro tale condotta. Le ragioni addotte erano l'assenza di precedenti, il carattere puramente mentale della lesione, la "grande mole di contenziosi" che ci si poteva aspettare, la difficoltà di tracciare una linea di demarcazione tra personaggi pubblici e privati, e il timore di un'indebita restrizione della libertà di stampa. Il risultato immediato del caso Roberson è stata una tempesta di disapprovazione pubblica. Di conseguenza, la successiva legislatura di New York emanò uno statuto che rendeva sia un reato che un illecito civile l'uso del nome, del ritratto o dell'immagine di qualsiasi persona per "scopi pubblicitari o per scopi commerciali" senza il suo consenso scritto; si può altresì ricordare il già citato Pavesich v. New England Life Insurance Co 122 Ga. 190, 50 S.E. 68 (1905).

[154] Traduzione libera: il testo originale dispone "*What has emerged from the decisions is no simple matter. It is not one tort, but a complex of four. The law of privacy comprises four distinct kinds of invasion of four different interests of the plaintiff, which are tied together by the common name*".

[155] Riassumendo i risultati dell'analisi di Prosser possiamo affermare quanto segue. Per il primo fra i tort, (sub a) esso si sostanzia in una figura che non necessita che le informazioni siano rese pubbliche, basta una introduzione nella vita privata altrui carpendo informazioni private. L'intrusione nella vita privata altrui può anche non essere fisica, ma solamente visiva o uditiva. In ogni caso deve essere altamente offensiva per una "persona ragionevole". È il solo dei quattro tort che non necessita che le informazioni siano rese "pubbliche"; pertanto l'illecito si realizza già nel momento in cui le informazioni sono raccolte. Il secondo (sub b) riguarda ipotesi in cui un individuo rende pubbliche informazioni vere di un altro individuo senza il consenso dello stesso. È composto di quattro elementi: (1) disseminazione di informazioni veritiere (2) offensive per una persona ragionevole, (3) che non siano di interesse pubblico e (4) siano così intime da confliggere con il senso comune di decoro. Il terzo (sub c) mira ad evitare che un soggetto possa avere un ritorno economico derivante dall'utilizzo della immagine o del nome della persona senza il suo consenso, così prevenendo l'ingiusto arricchimento. Si caratterizza chiaramente per lo scopo "commerciale" che il soggetto mira a conseguire con l'utilizzo dell'immagine altrui. L'ultimo dei tort (sub d) è rivolto alla situazione in cui si vada a mettere una persona in cattiva luce pubblicando informazioni che sono false sull'individuo o, per il modo in cui sono esposte, che creano una falsa rappresentazione del soggetto. Deve trattarsi di una condotta altamente offensiva per una "persona ragionevole" e perché vi sia responsabilità, chi pubblica la notizia deve farlo nella consapevolezza della falsità.

[156] In merito alla "costituzionalizzazione" del diritto alla riservatezza in ambito euro-italiano si veda altresì G. ALPA, G. RESTA, *Le Persone e la Famiglia 1, Le persone fisiche e i diritti della personalità*, in Trattato di Diritto Civile (a cura di R. SACCO), Milano, 2019, 463 e ss.

[157] Per maggiori informazioni in merito si faccia riferimento a G. PASCUZZI, F. GIOVANELLA, *Dal diritto alla riservatezza alla computer privacy* in G. PASCUZZI (a cura di) *Il diritto dell'era digitale,* cit., 43 e ss.; G. GIARDINI, *Le regole dell'informazione. Principi giuridici, strumenti, casi,* Milano, 2009.

La prima sentenza in questa materia è stata resa nel 1956, generalmente ricordata come "Caso Caruso"[158]. La questione riguardava la rappresentazione della vita privata del tenore Enrico Caruso nel film "Leggenda di una voce" del 1951 diretto da Giacomo Gentilomo con Ermanno Randi e Gina Lollobrigida. Gli eredi del tenore citarono in giudizio la casa produttrice (Tirrena Asso Film) affermando che il film andasse a ledere l'onore, la memoria e la riservatezza del *de cuius*.

Gli attori sostenevano che un limite all'attività del narratore o del biografo fosse dato dal divieto di riferire quei fatti che, attenendo unicamente alla vita intima, familiare ed affettiva della persona celebre, non presentassero alcun interesse per la ricostruzione della personalità di questa, e la cui narrazione fosse destinata unicamente a soddisfare la indiscreta e malsana curiosità dei lettori e spettatori. Su questa base la Corte si chiedeva se dovesse "*ricevere protezione un generale diritto alla riservatezza o privatezza qualificato dalla giurisprudenza anglosassone right to privacy, che si vorrebbe introdotto nel nostro ordinamento giuridico*". La risposta che giunse fu tuttavia negativa. La Corte sostenne infatti che "*nessuna disposizione di legge autorizza a ritenere che sia stato sancito, come principio generale, il rispetto assoluto all'intimità della vita privata e tanto meno come limite alla libertà dell'arte. Sono soltanto riconosciuti e tutelati, in modi diversi, singoli diritti soggettivi della persona. Gli artt. 96 e 97 della legge di autore riguardano esclusivamente il ritratto della persona e la riproduzione dell'immagine nella persona ritrattata, ma non offrono argomento per ravvisare in essi l'applicazione di un principio generale a tutela dei diritti della personalità e tanto meno di un preteso diritto all'intimità*", "[…] *fuori dei limiti fissati, l'aspirazione alla privatezza non riceve protezione, salvo che l'operato dell'agente, offendendo l'onore o il decoro o la reputazione della persona, ricada nello schema generale del fatto illecito. Quando la conoscenza delle vicende della vita altrui non sia stata ottenuta con mezzi di per sé illeciti o che impongano l'obbligo del segreto, non è vietato comunicare i fatti, sia privatamente ad una o più persone, sia pubblicamente a mezzo della stampa, di opere teatrali, o cinematografiche o di discorsi*". "*Il semplice desiderio di riserbo non è stato ritenuto dal legislatore un interesse tutelabile; chi non ha saputo o voluto tener celati i fatti della propria vita non può pretendere che il segreto sia mantenuto dalla discrezione altrui; la curiosità ed anche un innocuo pettegolezzo, se pur costituiscono una manifestazione non elevata dell'animo, non danno luogo di per sé ad un illecito giuridico*".

Il secondo caso è ricordato come "Caso Petacci v. Palazzi"[159]. La fattispecie concreta riguardava la pubblicazione di un libro biografico in cui l'autore narrava avvenimenti afferenti alla vita privata di Claretta Petacci, amante di Mussolini. Gli eredi della defunta intentarono causa contro l'autore e l'editore sostenendo che l'opera violava la riservatezza della Petacci recando offesa alla sua memoria e reputazione. Dunque, un caso molto simile a quello previamente richiamato di Caruso. Eppure, in quegli anni era intervenuto un mutamento importante per l'ordinamento giuridico italiano in quanto solo nel 1956 la Corte Costituzionale italiana iniziò attivamente ad operare andando ad affermare un principio inedito: riconobbe la natura vincolante delle norme costituzionali anche nei confronti delle leggi anteriori, investendo le norme costituzionali di una natura precettiva e non solo programmatica[160].

---

158 Cass. Civ., 22.12.1956, no. 4487 in *Foro.it,* 1957, I, 423. Prima di raggiungere la sede romana, il caso era stato deciso in senso differente da Pretore di Roma, 19 novembre 1951 e Tribunale di Roma, 14 settembre 1953.

159 Cass. Civ., 20.4.1963, n. 990, in *Giust. Civ.*, 1963, I, 1280 ed in *Foro.it.*, 1963, I, 129

160 La vicenda dell'attuazione della costituzione è stata una vicenda sofferta, non solo per l'inerzia del legislatore nel farsi carico dei principi fondamentali, ma anche per la lentezza nell'istituire la Corte Costituzionale. In questo contesto, merita di essere segnalato che la cultura giuridica in cui la Costituzione si incardina è quella che esprimeva scetticismo rispetto ad una applicazione diretta della Costituzione. Da un lato vi erano autori come Calamandrei, Esposito e Mortati che ritenevano che le norme costituzionali non dovessero essere applicate direttamente dai giudici, esaurendo i propri effetti giuridici all'interno del giudizio di costituzionalità. A questi autori si contrapponeva Crisafulli che affermava invece che le norme costituzionali oltre ad indicare

In questa pronuncia, mentre la Corte d'appello di Milano aveva riconosciuto l'esistenza di un non meglio precisato "diritto alla riservatezza", la Cassazione giunse, tortuosamente, ad affermare che un tale diritto non fosse rinvenibile nel nostro ordinamento, ma che l'autore avesse comunque violato un indefinito "diritto assoluto di personalità". La Corte, infatti, affermava che si dovesse riconoscere che "*la personalità è il presupposto di diritti ma anche che essa […] postula un diritto di concretizzazione, cioè un diritto di libertà di autodeterminazione nei limiti consentiti dall'ordinamento, il quale come diritto assoluto, astratto si distingue dal potere di autonomia inerente ai singoli concreti diritti*". Interessante il richiamo alla Costituzione italiana in quanto conferma che "*Il fondamento in diritto positivo di un diritto assoluto nel senso indicato può ravvisarsi nell'art. 2 della Costituzione, il quale […] ammette un diritto di libera autodeterminazione nello svolgimento della personalità*". Tuttavia, secondo la Corte "*non può, in mancanza di esplicita previsione, affermarsi né […] si può ritenere per analogia sulla base di singoli diritti di personalità […] un autonomo diritto soggettivo ad una non precisata riservatezza […] Ma deve ammettersi la tutela nel caso di violazione del diritto assoluto di personalità inteso quale diritto erga omnes alla libertà di autodeterminazione nello svolgimento della personalità dell'uomo come singolo*".

Nonostante la Corte di Cassazione avesse proceduto a negare l'esistenza di un diritto alla riservatezza, le Corti inferiori continuarono a ritenerlo sussistente [161] e nel 1975 finalmente un ufficiale riconoscimento giunse dalla Suprema Corte. Il riferimento è al c.d. "Caso Soraya"[162]. Il contesto della fattispecie concreta, pur divergendo dalle precedenti due pronunce, è invece molto simile a quanto emergeva in Warren e Brandeis: Soraya Esfandiari, principessa persiana in esilio in Italia, era stata ritratta all'interno delle mura di casa sua da un paparazzo finché si intratteneva intimamente con un uomo. Fra le *causae petendi* della sua azione giudiziaria nei confronti dell'editoriale "Gente", in cui apparvero gli scatti, rientrava l'affermata violazione del suo diritto alla riservatezza. Il procedimento condusse nel 1975 in Cassazione, la quale giunse alla compiuta affermazione dell'esistenza nel nostro ordinamento giuridico di un diritto alla riservatezza sulla base non solo dell'analisi delle norme civilistiche quali quelle sul nome (art. 10 cod. civ.) e sull'immagine (artt. 96 e 97 l. 633/1941) ma anche sulla base dei principi costituzionali di cui (fra i molti citati) si ricordano gli articoli 2, 3, 13, 14, 29 e 41 co.2[163]. La Corte dunque giunge ad affermare che "*pur non essendo opportuno dare*

obiettivi programmatici dovessero essere intese come norme immediatamente precettive e quindi applicabili dai giudici ordinari, valorizzando la portata pervasiva di tali norme. Azzariti sosteneva invece che le norme costituzionali fossero alcune precettive ed altre programmatiche e che quindi potessero essere applicate direttamente solo quelle precettive, posizione avallata anche della Corte di Cassazione nella sentenza Scalogna del 1951 (Sezioni Unite del 20 gennaio 1951 ric. Scalogna, *Giust. Pen*, 1951, II, 211).

[161] Il riferimento è ad una copiosa giurisprudenza di merito in senso conforme a quanto indicato, ad esempio si faccia riferimento a: Pret. Roma, 19 novembre 1951, in *Foro it.,* 1952; Trib. Roma, 14 settembre 1953, in *Giut it.,* 1954, I, 2, c. 532; App. Milano, 21 gennaio 1955, in *Foro it.,* 1955, I, c. 386; App. Napoli, 20 agosto 1958, in *Giust. civ*., 1959, p. 1811; App. Milano, 26 agosto 1960, in *Foro it.,* 1955, I, c. 386; App. Milano, 19 gennaio 1971, in *Foro it.,* 1971, II, c. 24; Pret. Milano, sentenza 12 maggio 1972, in *Foro it.,* 1972, I, c. 2706.

[162] Soraya Esfandiari v. Rusconi Editore – Cass. 27.5.1975, n. 2129 in *Foro.it*., 1976, I, 2895.

[163] La sommaria indicazione nel testo delle norme costituzionali merita un breve approfondimento. Per quanto riguarda il richiamo preminente all'art. 2 Cost la Corte afferma: "*Questa Corte aveva ravvisato nell'art. 2 Cost. l'unico fondamento del diritto assoluto di personalità, che risulta violato dalla divulgazione di notizie della vita privata. Alla critica, secondo cui l'art. 2 enuncia solo in via generale la tutelabilità di diritti inviolabili, che trovano il loro riconoscimento effettivo in altre specifiche norme, deve precisarsi che questa Corte - deducendo dal citato articolo il « diritto erga omnes alla libertà di autodeterminazione » - intendeva porre l'accento - più che sul riferimento ai diritti inviolabili - sull'espressione della norma che riconosce all'uomo il rispetto della sua personalità, come singolo e nelle formazioni sociali ove tale personalità si svolge*"; per quanto riguarda il riferimento all'art. 3 la Corte nota che "*Un duplice spunto di convalida al diritto di riservatezza si trae anche dall'art. 3 Cost. sia perché, riconoscendosi la dignità sociale del cittadino, si rende necessaria una sfera di autonomia che garantisca tale dignità, sia in quanto rientrano nei limiti di fatto della libertà ed eguaglianza dei cittadini anche quelle menomazioni cagionate dalle indebite ingerenze altrui nella sfera di autonomia di ogni persona*", il che sarebbe confermato anche dall'art. 13 Cost. inteso in senso più ampio rispetto alla libertà meramente fisica. Gli artt. 14 e 29 Cost. vengono ritenuti una

del diritto alla riservatezza rigide descrizioni analitiche di impaccio alla necessaria duttilità del suo preciso contenuto e alle esigenze degli ambienti, delle zone e dei tempi - può affermarsi che tale diritto consiste nella tutela di quelle situazioni e vicende strettamente personali e familiari, le quali, anche se verificatesi fuori del domicilio domestico, non hanno per i terzi un interesse socialmente apprezzabile, contro le ingerenze che, sia pure compiute con mezzi leciti, per scopi non esclusivamente speculativi e senza offesa per l'onore, la reputazione e il decoro, non siano giustificate da interessi pubblici preminenti".

Quindi per quanto sin qui considerato possiamo affermare che in Italia, il maggior contributo all'elaborazione costituzionale di un diritto alla privacy venne dalla giurisprudenza che, inizialmente negando nel Caso Caruso l'esistenza di un diritto alla riservatezza, per mezzo della rilettura costituzionalmente orientata dei diritti, presente già nel Caso Petacci, permette alla Cassazione di giungere nel 1975, con il Caso Soraya, alla consacrazione definitiva del diritto alla riservatezza.

Molte furono le evoluzioni giurisprudenziali[164]che seguirono tale consacrazione, anche alla luce dell'armonizzazione europea per il tramite della Direttiva 95/46 CE prima e del Regolamento 2016/679 poi. In questo rafforzando la protezione grazie all'intervento della Corte di Giustizia europea[165] ed alla Corte Europea dei Diritti dell'Uomo che costantemente sono investite di tematiche relative alla riservatezza ed alla protezione dei dati personali. Non pare necessario in questo frangente indagare oltre la dimensione di protezione del diritto alla riservatezza stante l'obiettivo di dimostrarne la portata costituzionale anche in ambito italiano ed europeo.

Come si è tentato di dimostrare allora, sia il diritto d'autore che il diritto alla riservatezza, per il tramite o di riferimenti normativi diretti o per interpretazioni giurisprudenziali, godono di una copertura costituzionale; quindi, il bilanciamento fra gli stessi si pone almeno sullo stesso piano e fra forze di egual vigore.

È però ora il caso di lasciare da parte le considerazioni evolutive del diritto e concentrarsi sul momento prescelto in cui lo scontro fra *l'enforcement* del diritto d'autore ed il

---

estrinsecazione dell'art. 2 in quanto posti a tutela dei diritti inviolabili dell'uomo tra cui si ritrova anche la tutela del domicilio e dello spazio familiare. Una notazione infine sull'art. 41 che parrebbe distonico rispetto alle altre indicazioni, ma che nel ragionamento della Corte assume un rinnovato rilievo. Essa, infatti, afferma che dal secondo comma dell'art. 41 Cost. si trae un importante spunto laddove l'iniziativa economica trova un limite nel rispetto della libertà e della dignità umana.

164 Fra le molteplici pronunce giurisprudenziali si possono ricordare: Cass. 22 giugno 1985, n. 3769, in *Foro it.,* 1985, I, 2211 (Caso Veronesi), in cui la Corte afferma che "*ciascun soggetto ha interesse, ritenuto generalmente meritevole di tutela giuridica, di essere rappresentato, nella vita di relazione, con la sua vera identità, così come questa nella realtà sociale, generale o particolare, è conosciuta o poteva essere conosciuta con la applicazione dei criteri della normale diligenza e della buona fede soggettiva; ha, cioè, interesse a non vedersi all'esterno alterato, travisato, offuscato, contestato il proprio patrimonio intellettuale, politico, sociale, religioso, ideologico, professionale, ecc. quale si era estrinsecato od appariva, in base a circostanze concrete ed univoche, destinato ad estrinsecarsi nell'ambiente sociale.");* Trib. Milano, 3.9.2012, n.9749, in *Danno e responsabilità*, 2013, 51-61 con nota di R. FOFFA (c.d. "Caso Vieri") in cui Christian Vieri apprendeva dai mezzi di informazione che le sue utenze telefoniche fisse e mobili erano state illecitamente intercettate e controllate, in cui la Corte giunge ad affermare che il danno "[*r]isulta provato perché è fatto notorio che una simile situazione possa provocare inquietudine, ansia, disagio, anche se non sufficienti ad integrare danno biologico, soprattutto quando la violazione della privacy si è protratta per molto tempo (4 anni) e anche in considerazione del risalto mediatico data alla vicenda*"; Sentenza Cass. 9 aprile 1998, n. 3679 (c.d. "Caso Rendo") in cui si inizia a parlare di "diritto all'oblio".

165 Si ricordi ad esempio l'impulso della CGUE nel caso c.d "Google Spain" (Causa C-131/12, Google Spain SL, Google Inc. c. Agencia Española de Protección de Datos (AEPD), Mario Costeja González, 13 maggio 2014, Grande Sezione), ove si è giunti ad affermare che "*Il gestore di un motore di ricerca è obbligato a sopprimere, dall'elenco di risultati che appare a seguito di una ricerca effettuata a partire dal nome di una persona, dei link verso pagine web pubblicate da terzi e contenenti informazioni relative a questa persona, anche nel caso in cui tale nome o tali informazioni non vengano previamente o simultaneamente cancellati dalle pagine web di cui trattasi, e ciò eventualmente anche quando la loro pubblicazione su tali pagine web sia di per sé lecita*".

diritto alla privacy si è fatto più sentire. Il riferimento è infatti, come accennato, a quei sistemi extragiudiziali di monitoraggio e applicazione del diritto d'autore che, sorvegliando l'utente delle reti online, compiono un'ingerenza nella sfera di riservatezza degli stessi.

4. Privacy sulla rete e dati personali: gli indirizzi IP

Il punto su cui si concentra questo capitolo riguarda, come affermato introduttivamente, uno scontro noto dell'era digitale: il *file-sharing*. In questa materia lo scontro fra *l'enforcement* del diritto d'autore ed il trattamento dei dati personali si è particolarmente sentito ed espresso in termini molto vicini alla nostra sensibilità, riproducendo tuttavia, secondo altre forme, metodi che abbiamo già incontrato nella storia: gli stessi metodi degli *Stationer* e del *commando* addestrato di Preston ed Abbott, dei cacciatori di ascoltatori pirata e del Betamax.

Nel contesto digitale, infatti, per tutelare il diritto d'autore, i *copyright holders* realizzano un'estesa attività di sorveglianza degli utenti del web, compiendo un trattamento dei dati personali senza il consenso degli utenti. Come si avrà ora modo di dimostrare, gli indirizzi IP costituiscono dati personali e la loro raccolta un trattamento. Tuttavia, come apparirà chiaro dall'analisi giurisprudenziale, questa notazione non avrà sempre la luce che merita e sarà un elemento spesso ignorato dalle Corti.

Abbiamo visto come la pirateria abbia una storia secolare, tuttavia solo più recentemente è divenuto un fenomeno globale, grazie alla diffusione di Internet, capace davvero di modificare i modelli di business e di mettere in ginocchio intere industrie di produzione di contenuti. La storia che accompagna questo elaborato si era interrotta con le cassette musicali prima e le videocassette poi, ma la medesima dinamica si è ripetuta anche per i CD ed i DVD.

L'avvento di Internet e dei file mp3 e mp4 ha reso la riproduzione e la distribuzione di canzoni e video molto più veloce e semplice, nonché economica, con una diffusione per mezzo del web potenzialmente globale. Una decina di anni dopo il caso Betamax, la RIAA (*Recording Industry Association of America*) iniziò un gran numero di procedimenti legali nei confronti degli utenti al fine di combattere la pirateria online. Per garantire *l'enforcement* del diritto d'autore nei confronti degli utenti, che, come si ricorderà, è una delle quattro strategie previamente delineate usabili in questi contesti, i titolari dei diritti d'autore necessitavano di scoprire quali fossero le reali identità degli utenti finali che si celavano al di là di uno schermo da computer.

Infatti, nel contesto digitale, gli utenti sono identificabili per il tramite del loro pseudonimo o del loro indirizzo di *Internet Protocol* (c.d. *IP Address*). La strategia dei titolari dei diritti d'autore allora consisteva, in larga misura, nel fare affidamento a delle *service companies* che si dimostravano in grado di collezionare dati di utilizzo nel traffico delle reti P2P, individuando gli indirizzi IP degli utenti che si intrattenevano in attività in violazione del diritto d'autore[166]. Le compagnie, quindi, comunicavano i risultati della loro ricerca ai titolari del diritto d'autore i quali tuttavia non avevano modo di risalire alle identità reali che risiedevano dietro l'indirizzo IP.

[166] Tali attività, sfruttando agenti software o bot come i Web crawler, sono diffusamente esplicitate in S. KATYAL, *Privacy vs. Piracy*, 7 *Yale Journal of Law & Technology* 222, 272-273 (2004), disponibile anche su SSRN all'URL: «http://ssrn.com/abstract=722441» (Ultimo accesso: 10 maggio 2022), 225 ss

Per compiere una completa "*disclosure*" delle identità degli utenti è necessaria la collaborazione degli *Internet Service Providers* (ISP, e nella specie di quelli definibili come "*access providers*") che, conferendo agli utenti la connessione Internet ed affidando loro un indirizzo IP, sono a conoscenza delle identità cui quegli indirizzi sono associati[167].

Prima di analizzare questo momento in cui gli ISP ed i titolari del diritto d'autore possono collaborare o meno, è meglio partire dal definire cosa sono gli indirizzi IP e perché hanno una così grande rilevanza.

Essenzialmente un *Internet Protocol Address* o indirizzo IP è un codice numerico usato da tutti i dispositivi connessi alla rete che costituisce il fondamento necessario per una trasmissione corretta delle informazioni dal mittente al destinatario. Tale numero funge in particolare da "*locating adress*" quindi, il possesso di un IP consente di rinvenire ove si trovi il *device* con tale numero essendo connesso ad uno specifico nodo della rete.

L'utente della rete, dunque, ottiene un IP per il tramite di una assegnazione da parte dell'*access provider* con cui stipula il contratto di connessione alla rete, *provider* il quale può assegnare alternativamente un IP c.d. "statico" ovvero uno "dinamico". Quello dinamico costituisce la modalità più comune ed utilizzata per la navigazione sulla rete, significando che ogni volta che l'utente si connette ad Internet, l'ISP di riferimento attribuisce un numero differente. Questo avviene principalmente perché ogni ISP ha una quantità predefinita di numeri assegnabili, al che quando l'utente si disconnette dalla rete, l'ISP può riassegnare il numero ad un altro utente. Si può ragionevolmente affermare che comunque la assegnazione di un indirizzo IP casuale, che cambia dopo ogni sessione o a intervalli, garantisce una maggiore protezione della privacy degli utenti consentendo una navigazione più anonima. L'IP statico invece costituisce un numero assegnato in via esclusiva che quindi rimane invariato nel tempo e oggi impiegato principalmente nelle LAN (reti private) per comunicare con altro *device* connesso alla rete locale quale, ad esempio, una stampante.

Ove si procedesse al tracciamento di un indirizzo IP, le informazioni principali che si potrebbero ottenere consistono nella localizzazione del *device* con un raggio più o meno ampio di certezza, il momento in cui quel *device* ha compiuto una attività e quale attività è stata compiuta. Sono informazioni che potrebbero non risultare particolarmente sensibili, tuttavia costituiscono informazioni che pertengono all'utente ed in quanto tali classificabili come dati personali[168].

Ed ecco dunque che la questione mostra la sua portata. Gli indirizzi IP sono stati considerati dati personali dalle Corti e dalle Autorità di *data protection*; tuttavia, la loro dimensione giuridica dipende dalla normativa ad essi applicabile.

Nel contesto normativo europeo si può richiamare l'opinione espressa dal Gruppo di lavoro Art. 29[169] secondo il quale gli Indirizzi IP attribuiti agli utenti di Internet sono dati

---

[167] Per una descrizione del funzionamento di questa strategia di *enforcement* vedere F. GIOVANELLA, *Copyright and Information Privacy. Conflicting Rights in Balance*, cit., 219 e ss.

[168] Per maggiori notazioni si veda F. GIOVANELLA, *Copyright and Information Privacy. Conflicting Rights in Balance*, cit., 219 e ss. ; F. GIOVANELLA, *Enforcement del diritto d'autore nell'ambito di Internet vs. protezione dei dati personali: bilanciamento tra diritti fondamentali e contesto culturale*, in *Trento Law and Technology Research Group*, Research Paper n.20, 2014, liberamente accessibile presso: «http://eprints.biblio.unitn.it/4273/» (Ultimo accesso: 10 maggio 2022).

[169] Gruppo di Lavoro Articolo 29, (Article 29 – WP), Opinion 2/2002 *On the use of unique identifiers in telecommunication terminal equipment: the example of IPv6*, adottata il 30 maggio 2002, disponibile presso: «http://www.eu.ipv6tf.org/PublicDocuments/wp58_en.pdf» (Ultimo accesso: 10 maggio 2022); Gruppo di Lavoro Articolo 29, (Article 29 – WP), Opinion 4/2007 *On the concept of personal data,* adottata il 20 giugno 2007

personali e protetti dalle Direttive europee 95/46 e 97/46. Ma anche alla luce dell'odierna regolamentazione, la conclusione deve essere la stessa, proprio per il fatto che nel contesto europeo la definizione di dato personale è "*qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale*" (GDPR, art. 4 n.1).

Sebbene l'indirizzo IP di per sé solo non identifichi direttamente una persona fisica, essendo meramente un numero di cui solo l'ISP conosce l'ascrivibilità contrattuale, costituisce un dato riguardante una persona *identificabile*. Il Considerando 26 GDPR recita, infatti, che per stabilire l'identificabilità di una persona è opportuno considerare tutti i mezzi di cui il titolare del trattamento o un terzo può ragionevolmente avvalersi per identificare detta persona fisica direttamente o indirettamente. La conferma deriva poi dallo stesso Considerando 30 in cui si ammette che "*le persone fisiche possono essere associate a identificativi online prodotti dai dispositivi, dalle applicazioni, dagli strumenti e dai protocolli utilizzati, quali gli indirizzi IP, marcatori temporanei (cookies) o identificativi di altro tipo, quali i tag di identificazione a radiofrequenza. Tali identificativi possono lasciare tracce che, in particolare se combinate con identificativi univoci e altre informazioni ricevute dai server, possono essere utilizzate per creare profili delle persone fisiche e identificarle*".

Conferma di questa impostazione deriva anche dalla giurisprudenza comunitaria in cui la Corte di Giustizia è giunta a ritenere che "*un indirizzo di protocollo Internet dinamico registrato da un fornitore di servizi di media online in occasione della consultazione, da parte di una persona, di un sito Internet che tale fornitore rende accessibile al pubblico costituisce, nei confronti di tale fornitore, un dato personale, qualora detto fornitore disponga di mezzi giuridici che gli consentano di far identificare la persona interessata grazie alle informazioni aggiuntive di cui il fornitore di accesso a Internet di detta persona dispone*"[170].

I titolari dei diritti d'autore quindi, servendosi di società capaci di intercettare un gran numero di indirizzi IP apparentemente industriati nello scambio su reti *peer-to-peer*, compiono un'attività definibile in termini di sorveglianza o monitoraggio estensivo degli utenti, realizzando un trattamento dei dati personali in via di autotutela, privo*, prima facie*, di alcuna base legale ex art. 6 GDPR. Solo sporadicamente le Corti si interessano di questo trattamento, avente ad oggetto dati personali in quanto attenenti ad un utente "identificabile", concentrandosi invece sul problema della *disclosure* delle identità degli utenti.

Sulla base di queste premesse dunque il conflitto appare evidente: bilanciare *l'enforcement* del diritto d'autore ed il diritto alla privacy ed al trattamento dei dati personali. Infatti, ove

disponibile presso: «https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1496512» (Ultimo accesso: 10 maggio 2022).

[170] CGUE 19 ottobre 2016, C-582/14, *Patrick Breyer c. Bundesrepublik Deutschland*, (Seconda Sezione), liberamente accessibile presso: «https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:62014CJ0582&from=it» (Ultimo accesso: 10 maggio 2022), in cui la Corte statuisce che "*L'articolo 2, lettera a), della Direttiva 95/46 del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, dev'essere interpretato nel senso che un indirizzo di protocollo Internet dinamico registrato da un fornitore di servizi di media online in occasione della consultazione, da parte di una persona, di un sito Internet che tale fornitore rende accessibile al pubblico costituisce, nei confronti di tale fornitore, un dato personale ai sensi di detta disposizione, qualora detto fornitore disponga di mezzi giuridici che gli consentano di far identificare la persona interessata grazie alle informazioni aggiuntive di cui il fornitore di accesso a Internet di detta persona dispone.*"

prevalesse il diritto d'autore, l'identità degli utenti dovrebbe essere svelata, ove prevalesse il diritto alla privacy invece il diritto d'autore non avrebbe modo di essere tutelato.

La questione della privacy e della tutela dei dati personali si apre anche ad altre prospettive sulla rete e nel mondo del *peer-to-peer*. Come nota brillantemente Sonia Katyal[171], più le persone percepiscono la loro privacy e l'anonimato, più è probabile che si sentano libere di creare ed esprimere completamente la propria identità ed i propri punti di vista nel cyberspazio. La percezione dell'anonimato ha consentito un livello di partecipazione al discorso pubblico diverso da qualsiasi altro periodo storico prima d'ora, permettendo, ad esempio, alle persone con risorse finanziarie limitate di pubblicare informazioni e opinioni su questioni di interesse pubblico[172]. Come ha affermato la professoressa Sherry Turkle[173], *"when we step through the screen into virtual communities, we reconstruct our identities on the other side of the looking glass*[174]". Anche al di fuori dei forum strutturati, un utente può adottare una molteplicità di identità di genere, sessuale, razziale o di altro tipo, inventare storie personali e impegnarsi in un assortimento di atti che probabilmente non avrebbe compiuto nella vita reale. In altre parole, lo spazio virtuale consente agli individui di costruire identità che scelgono per se stessi, piuttosto che quelle con cui sono nati. Questa capacità di adottare identità transitorie e multiple è al centro delle possibilità illimitate del cyberspazio.

Secondo l'autrice infatti, oggi, la percezione della privacy informativa si estende, almeno nel cyberspazio, a qualcosa di completamente diverso: copre l'atto stesso di creare personalità e accedere alle informazioni, oltre alla possibilità di pubblicare informazioni in modo anonimo. Essa nota infatti come un utente potrebbe liberamente aprire un account e-mail sotto falso nome e con quell'identità navigare sul Web, effettuare acquisti e impegnarsi in conversazioni online. La sua identità online, le conversazioni e le attività sono tutte "pubbliche", nel senso che possono essere soggette a vari gradi di trasparenza nel cyberspazio. Tuttavia, la sua vera identità, o le sue informazioni personali - preferenze, abitudini di acquisto, ricerche sul web - sono tutte "private", nel senso che potrebbe preferire che siano nascoste alla conoscenza pubblica. La sua percezione dell'anonimato permea le sue espressioni e attività nel cyberspazio.

5. Istituti di "*discovery*"

Come anticipato, una volta che i titolari dei diritti d'autore ottengono gli indirizzi IP di coloro che hanno compiuto violazioni del *copyright* devono rivolgersi agli ISP per ottenere l'identificazione compiuta dell'utente. Non tutti i *Service Provider* però collaborano con i titolari del diritto d'autore costringendo in questo modo questi ultimi a rivolgersi al sistema normativo per ordinare agli ISP di comunicare l'identità dei pirati.

L'attenzione posta agli *Internet Service Provider* in questo capitolo è anche giustificata dal fatto che essi si sono trasformati in una forma di *governance* privata nel ciberspazio perché conservano una notevole quantità di informazioni sui consumatori relative alle attività online degli utenti e perché spesso controllano la trasmissione e la distribuzione delle

---

171 S. KATYAL, *Privacy vs. Piracy*, cit., 252 e ss.

172 In merito si faccia altresì riferimento a L. BARNETT LIDSKY, *Silencing John Doe: Defamation & Discourse in Cyberspace*, 49 *Duke Law Journal* 855-946 (2000), liberamente accessibile presso: «https://scholarship.law.duke.edu/dlj/vol49/iss4/1/» (Ultimo accesso: 10 maggio 2022).

173 S. TURKLE, Life *On The Screen: Identity In The Age Of The Internet 177* (1995), citata da KATYAL S., *Privacy vs. Piracy,* cit., 252 e ss.

174 Traducendo liberamente: "*Quando entriamo attraverso lo schermo nelle comunità virtuali, ricostruiamo le nostre identità dall'altra parte dello specchio"*

informazioni[175]. È quindi necessario, ai fini della presente dissertazione, procedere ad analizzare la legislazione ordinaria, sia statunitense che italiana, in tema di *enforcement* del diritto d'autore per considerare come queste offrano strumenti di *disclosure* delle identità degli utenti. Ove richiesti legalmente di svelare le identità degli utenti, i *provider* sollevarono preoccupazioni circa la privacy e la protezione dei loro dati personali, dimostrando come il bilanciamento fra il diritto d'autore e la riservatezza sia la chiave di volta di risoluzione della casistica concernente questo fenomeno giuridico.

5.1. US: §512 DMCA *Subpoena*

Il primo degli strumenti di *enforcement* presi in considerazione è sicuramente quello introdotto dalla §512 del Digital Millennium Copyright Act che, in congiunzione con l'applicazione delle c.d. "*Safe Harbor Provisions*" di cui *infra*, introduce lo strumento del *subpoena duces tecum*[176]. In via generale, un *subpoena* è uno strumento conosciuto alla procedura civile di *common law*, sostanziandosi in una citazione in giudizio per la produzione di prove. Esso, dunque, è un ordine ordinariamente emesso da una Corte e rivolto al destinatario di comparire davanti al tribunale e produrre documenti o altre prove tangibili da utilizzare in un'udienza o in un processo.

La Section 512 (h) fornisce un meccanismo per il titolare del copyright utile a citare in giudizio un ISP per ricercare l'identificazione di un presunto trasgressore del diritto d'autore. Secondo la storia legislativa della disposizione in commento, il Congresso intendeva limitare la portata della disposizione alle "informazioni in possesso del fornitore di servizi, piuttosto che obbligare il fornitore di servizi a condurre ricerche di informazioni disponibili in altri sistemi o reti". I *subpoena*, per questi fini, avrebbero dovuto essere emanati rapidamente ove le pratiche burocratiche necessarie per la loro emissione fossero state in regola con quanto previsto dalla norma, ed in particolare dalla §512(c)(3)(A).[177]

La Section 512 (h) (1) dunque contempla un *subpoena* specifico per l'ipotesi in cui il titolare dei diritti d'autore intenda richiedere ad un ISP di produrre delle informazioni in giudizio, e segnatamente l'identità di coloro che sono associati all'indirizzo IP. La norma dispone che "*a copyright owner or a person authorized to act on the owner's behalf may request the clerk of any United States district court to issue a subpoena to a Service Provider for identification of an alleged*

---

[175] S. KATYAL, *Privacy vs. Piracy*, cit. 252 e ss.; W. W. FISHER III & C. YANG, *Peer-to-Peer Copying, an Introduction*, in *Berkman Center for Internet & Society* (Nov. 18, 2001), liberamente accessibile presso: «http://cyber.law.harvard.edu/ilaw/P2P.html» (Ultimo accesso: 10 maggio 2022).

[176] Maggiori informazioni sullo strumento del Subpoena sono rinvenibili presso: F. GIOVANELLA *Copyright and Information Privacy. Conflicting Rights in Balance*, Edward Elgar Pub., Cheltenham, 2017; F. GIOVANELLA, *Enforcement del diritto d'autore nell'ambito di Internet vs. protezione dei dati personali: bilanciamento tra diritti fondamentali e contesto culturale,* in *Trento Law and Technology Research Group*, Research Paper n.20, 2014, liberamente accessibile presso: «http://eprints.biblio.unitn.it/4273/» (Ultimo accesso: 10 maggio 2022).

[177] Per maggiori riferimenti in merito alla section 512(h) si veda: United States Copyright Office, *Section 512 of Title 17, A Report Of The Register Of Copyrights*, 2020, 164 e ss, liberamente accessibile presso: «https://www.copyright.gov/policy/section512/section-512-full-report.pdf» (Ultimo accesso: 10 maggio 2022). Nello specifico, il report afferma che "*According to the legislative history, Congress intended to limit the scope of the subpoena to "information in the possession of the service provider, rather than obliging the service provider to conduct searches for information that is available from other systems or networks," and articulated the role of courts in issuing subpoenas as "a ministerial function performed quickly for this provision to have its intended effect". Subpoenas were to be "expeditiously issued" if the rightsholder's paperwork was in order, including a notification that complies with the elements required under section 512(c)(3)(A)*".

infringer in accordance with this subsection"[178]. Attraverso questa disposizione i titolari dei diritti d'autore possono chiedere al cancelliere (*clerk*), non dunque in un contesto giurisdizionale nel contraddittorio fra le parti, un *subpoena* nel rispetto della normativa delineata dall'articolo stesso. In particolare, in virtù del §512 (h)(2), la richiesta compiuta dal titolare del diritto d'autore deve essere accompagnata da (A) una copia di una notifica descritta nella sottosezione (c) (3) (A); (B) un mandato di comparizione; e (C) una dichiarazione giurata secondo cui lo scopo per il quale si richiede la citazione è di ottenere l'identità di un presunto trasgressore e che tali informazioni saranno utilizzate solo allo scopo di proteggere i diritti d'autore[179].

Lo strumento che si attaglierebbe perfettamente alle esigenze di *enforcement* del diritto d'autore, tuttavia, non ebbe successo in quanto le Corti diedero interpretazioni differenti della normativa in commento e si interrogarono sulla costituzionalità di una tale previsione sotto l'egida della "*overbreadth doctrine*" [180] . Il maggiore ostacolo, tuttavia, derivò dall'interpretazione della norma che escludeva dall'ambito soggettivo di applicazione della stessa i c.d. "*mere conduit provider"* ossia quegli intermediari online che si limitano a concedere all'utente una connessione ad Internet e consentono le comunicazioni fra utenti senza però agire sulle comunicazioni stesse.

Un recente contributo del Copyright Office statunitense mostra piena consapevolezza dell'insuccesso dell'istituto in commento, proprio affermando che, in pratica, i tribunali statunitensi hanno in gran parte escluso dalla copertura della presente disposizione gli ISP più rilevanti, per esempio quelli che sarebbero stati utili per scoprire l'identità di individui che utilizzavano strumenti quali BitTorrent e protocolli di condivisione di analoga natura per scambiare porzioni di opere illecite. In seguito al caso Verizon, come di seguito verrà analizzato, la sezione 512(h) si è rivelata uno strumento meno utile per i titolari dei diritti di quanto il Congresso avrebbe potuto prevedere. Questo è stato primariamente dovuto, come afferma il Copyright Office, al fatto che i tribunali hanno adottato vari test per bilanciare la necessità di tutela del titolare dei diritti d'autore e gli interessi degli utenti, principalmente in riferimento al primo emendamento e al diritto alla privacy[181].

Per queste ragioni, il Copyright Office si è anche espresso in senso favorevole ad una correzione legislativa per affrontare le ambiguità della sezione 512(h) e chiarire se gli ISP sono soggetti ai *subpoena* ai sensi della sezione 512(h) anche se allo stesso tempo concorda sul fatto che in realtà debba esservi una più ampia discussione sostanziale concernente le tattiche di contenzioso utilizzate da alcune società, che, come vedremo, possono comportare gravi ripercussioni sui diritti degli utenti ed in particolare sul loro diritto alla riservatezza[182].

---

178 Traducendo liberamente: "*un titolare del diritto d'autore o una persona autorizzata ad agire per conto del titolare può chiedere al cancelliere di qualsiasi tribunale distrettuale degli Stati Uniti di emettere una citazione a un fornitore di servizi per l'identificazione di un presunto trasgressore in conformità con questa sottosezione"*

179 Nel testo della legislazione statunitense si legge: "*(A) a copy of a notification described in subsection (c)(3)(A); (B) a proposed subpoena; and (C) a sworn declaration to the effect that the purpose for which the subpoena is sought is to obtain the identity of an alleged infringer and that such information will only be used for the purpose of protecting rights under this title".*

180 Per notazioni bibliografiche sull'overbreadth doctrine si faccia riferimento, fra i molti, a: D.S BOGEN, *Fist amendament ancillary doctines*, in *Maryland law review* 679*,* 1978; H.P. MONAGHAN, *Overbreadth*, in *Supreme Court Review*,1981. La dottrina è tipica dei casi in cui si verifica una c.d "facial challenge" di costituzionalità che mira ad ottenere una declaratoria di invalidità della legge soggetta al vaglio della Corte nella sua interezza, così distinguendosi dalla invalidità "as-applied" che mira alla declaratoria di invalidità di una specifica interpretazione di una norma. La overbreadth doctrine in particolare punta a censurare la legge sul profilo costituzionale per essere troppo comprensiva (too broad).

181 United States Copyright Office, *Section 512 of Title 17, A Report Of The Register Of Copyrights*, cit.,163 e ss

182 United States Copyright Office, *Section 512 of Title 17, A Report Of The Register Of Copyrights*, cit.,164 e ss

In ogni caso, stante per le ragioni che verranno in seguito esposte l'ineffettività della §512(h), dalle parole del legislatore statunitense emerge evidentemente come il Congresso, nel *subpoena* del DMCA, abbia scelto un approccio di regolazione che affidasse all'autotutela privata l'iniziativa di perseguire le violazioni dei diritti d'autore. Questo, come accennato, comporta che si incoraggino i titolari dei diritti d'autore a rivolgersi a società private per porre in essere una massiccia sorveglianza ed un trattamento di dati personali senza il consenso degli utenti.

5.2. US: *John Doe proceedings*

La larga inapplicabilità dello strumento del DMCA *subpoena* condusse i titolari dei diritti d'autore statunitensi ad orientarsi verso un diverso strumento che garantisse l'ostensione delle identità dei "pirati" delle *reti peer-to-peer*. Questo strumento consisteva nei c.d. "*John Doe Proceedings*"[183].

Le regole di procedura civile statunitensi consentono in ogni lite civile, ove sia necessario procedere in assenza di una parte, di esercitare un'azione contro "*John Doe*" consistente in una "*ex parte discovery*", ossia in una azione processuale che si connatura per il fatto che una delle parti non è né presente né rappresentata. Per mezzo di tale procedura una parte può ottenere una "*immediate discovery*" con la quale procedere a notificare un *subpoena* per la produzione di un materiale o di una informazione ad una terza parte. Applicato alle liti di cui il presente capitolo si vuole occupare, questo avrebbe consentito ai titolari dei diritti d'autore di procedere contro un fittizio e sconosciuto pirata, un anonimo "*John Doe*", conseguentemente ottenendo un *subpoena* che sarebbe stato notificato ad un *Internet Service Provider* ordinando una "*immediate discovery*" della identità dell'utente che si celava dietro l'indirizzo IP. Così dunque ottenuta l'informazione necessaria per l'identificazione del pirata, si sarebbe potuto emendare l'originaria azione contro ignoti *John Doe*, e procedere contro colui che si era rinvenuto essere il possibile "*copyright infringer*".

Come ricorda Federica Giovanella[184], dal momento che le regole di procedura civile sono poco chiare nello statuire circa i convenuti anonimi, le Corti statunitensi hanno rinvenuto differenti interpretazioni e decisioni sul problema dello smascheramento dell'identità degli utenti.

Tuttavia, prima di procedere all'analisi casistica, oggetto dei prossimi paragrafi, è bene ultimare il riferimento legislativo con alcune notazioni riguardanti alcuni standard applicabili a tutti i "*John Doe proceedings*", indipendentemente dall'attinenza o meno al *copyright infringement*.

Un primo elemento, come riconosciuto da Federica Giovanella, è la "*good faith*", la buonafede. In particolare, nel caso *In re Subpoena Duces Tecum to Am. Online, Inc., 52 Va. Cir*

---

[183] Per maggiori informazioni sui John Doe procedings si faccia riferimento a C. M. RICE, *Meet John Doe: It is Time for Federal Civil Procedure to Recognize John Doe Parties,* 57 *U. Pitt. L. Rev.* 883 (1995), liberamente accessibile presso: «https://scholarship.law.ua.edu/cgi/viewcontent.cgi?article=1035&context=fac_articles» (Ultimo accesso: 10 maggio 2022); R. G. LARSON, P. A. GODFREAD, *Bringing John Doe to Court: Procedural Issues in Unmasking Anonymous Internet Defendants,* in *William Mitchell Law Review* 328, Vol. 38: Iss. 1, Article 6., 2011, liberamente accessibile presso: «https://open.mitchellhamline.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1435&context=wmlr» (Ultimo accesso: 10 maggio 2022); F. GIOVANELLA, *Copyright and Information Privacy. Conflicting Rights in Balance*, cit., 227 e ss.

[184] F. GIOVANELLA, *Copyright and Information Privacy. Conflicting Rights in Balance*, cit., 227 e ss.

26[185]*,* la Corte della Virginia afferma che un giudice debba ordinare ad un fornitore di servizi Internet di svelare informazioni sull'identità di un abbonato (1) ove il tribunale possa considerarsi soddisfatto delle memorie o delle prove fornite; (2) la parte dimostri di possedere una base legittima per la richiesta e una buona fede nel sostenere di essere vittima di una condotta perseguibile nella giurisdizione in cui è stata intentata la causa; (3) le informazioni sull'identità citate in giudizio siano essenziali per avanzare tale richiesta[186].

Un secondo standard è invece rinvenibile nel caso *Columbia Ins. Co. v. Seescandy.com, 185 F.R.D. 573 (N.D. Cal. 1999)*[187] in cui venne introdotto un "*balancing test*" basato su quattro fattori che si atteggiano a limite per l'ostensione dell'identità degli utenti[188]. Secondo la Corte distrettuale della California del Nord, in primo luogo, l'attore dovrebbe identificare la parte sconosciuta con sufficiente specificità in modo tale che la Corte possa stabilire che il convenuto è una persona o entità reale che potrebbe essere citata in giudizio in un tribunale federale; in secondo luogo, la parte dovrebbe indicare tutti gli sforzi compiuti per cercare di localizzare il convenuto elusivo. Questo secondo elemento è infatti volto a garantire che gli attori compiano uno sforzo in buona fede per ottemperare ai requisiti di notifica del processo e a identificare specificamente gli imputati. In terzo luogo, l'attore dovrebbe dimostrare alla Corte che la causa contro il convenuto potrebbe resistere a un'istanza di rigetto. L'attore, infine, deve presentare istanza di accertamento al Tribunale volta all'individuazione di un numero limitato di persone o enti cui potrebbe essere notificato il procedimento di accertamento per il cui tramite identificare il convenuto anonimo.

A partire da questo primo "*balancing test*", Federica Giovanella ricorda che altri ne vennero sviluppati da altre Corti. In particolare, degna di nota risulta una ulteriore pronuncia in quanto basata principalmente sulla considerazione dell'interesse alla privacy dell'utente, ossia la sentenza Sony Music Entertainment, Inc. v. Does 1-40 326 F. Supp. 2d 556 (S.D.N.Y. 2004)[189]. I quattro fattori che la Corte individua sono: (1) una dimostrazione concreta di una pretesa *prima facie* di danno perseguibile, (2) specificità della richiesta di scoperta (3) l'assenza di mezzi alternativi per ottenere le informazioni richieste, (4) una necessità dimostrata delle informazioni per avanzare la richiesta (5) l'aspettativa di privacy della parte[190].

---

[185]In re Subpoena Duces Tecum to Am. Online, Inc., 52 Va. Cir 26, 2000, liberamente consultabile presso: «https://h2o.law.harvard.edu/cases/4393» (Ultimo accesso: 10 maggio 2022).

[186] Nel testo originale: "*a court should only order a non-party, Internet Service Provider to provide information concerning the identity of a subscriber (1) when the court is satisfied by the pleadings or evidence supplied to that court (2) that the party requesting the subpoena has a legitimate, good faith basis to contend that it may be the victim of conduct actionable in the jurisdiction where suit was filed and (3) the subpoenaed identity information is centrally needed to advance that claim*".

[187]Columbia Ins. Co. v. Seescandy.com, 185 F.R.D. 573 (N.D. Cal. 1999), liberamente consultabile presso: «https://cyber.harvard.edu/property00/domain/Sees.html» (Ultimo accesso: 10 maggio 2022).

[188] Nelle parole della Corte, ricostruendo i quattro passaggi fondamentali nel testo originario: "*First, the plaintiff should identify the missing party with sufficient specificity such that the Court can determine that defendant is a real person or entity who could be sued in federal court"; "Second, the party should identify all previous steps taken to locate the elusive defendant. This element is aimed at ensuring that plaintiffs make a good faith effort to comply with the requirements of service of process and specifically identifying defendants"; "Third, plaintiff should establish to the Court's satisfaction that plaintiff's suit against defendant could withstand a motion to dismiss." ; "Lastly, the plaintiff should file a request for discovery with the Court, along with a statement of reasons justifying the specific discovery requested as well as identification of a limited number of persons or entities on whom discovery process might be served and for which there is a reasonable likelihood that the discovery process will lead to identifying information about defendant that would make service of process possible*".

[189] Sony Music Entertainment, Inc. v. Does 1-40 326 F. Supp. 2d 556 (S.D.N.Y. 2004), liberamente accessibile presso: «https://www.casemine.com/judgement/us/5914b700add7b0493477c750» (Ultimo accesso: 10 maggio 2022).

[190] Nel testo della Corte: "*These factors include: (1) a concrete showing of a prima facie claim of actionable harm, see Seescandy.Com, 185 F.R.D. at 577, 579-81 (permitting plaintiff to request discovery, based on particular factors, to determine identities of defendants known only by Internet pseudonyms and domain name registration identities); America Online, 2000 WL*

La valutazione di ciascuno di questi fattori supporta la divulgazione delle identità dei supposti pirata, con implicazioni giurisprudenziali che verranno analizzate nel proseguo di questo elaborato.

Il sistema statunitense quindi si dimostra particolarmente attento ad assicurare strumenti di *enforcement* del diritto d'autore, largamente incentivando un'attività di sorveglianza da parte dei titolari dei diritti d'autore per combattere la pirateria online. Sembra infatti che il sistema americano compia la scelta di anteporre il *copyright* alla privacy, facendosi carico della evidente difficoltà dei titolari dei diritti d'autore di far rispettare i propri monopoli su Internet.

Avendo brevemente fornito indicazioni sulla dimensione degli istituti di *discovery* negli Stati Uniti, in prospettiva comparata si rinviene necessario passare al contesto euro-italiano, cercando di identificare quali istituiti potrebbero mostrarsi come l'equivalente di quelli d'oltreoceano.

5.3. L'art. 156-bis della legge 633/1941

Nella legislazione italiana gli strumenti di *enforcement* del diritto d'autore sono rappresentati dagli articoli 156 e 156-bis della legge sul diritto d'autore, 633/1941. Essi vennero introdotti tramite decreto legislativo 16 marzo 2006 n. 140 come conseguenza del necessario recepimento della Direttiva 2004/48/CE. La c.d. "*IPR Enforcement Directive*" imponeva a tutti gli Stati membri di applicare rimedi e sanzioni efficaci, dissuasive e proporzionate nei confronti di coloro che si occupano di contraffazione e pirateria.

L'articolo 156 offre uno strumento ai titolari dei diritti d'autore per *l'enforcement* dei loro diritti contro azioni di pirateria da parte degli utenti. Esso dispone che chi abbia ragione di temere la violazione di un diritto di utilizzazione economica a lui spettante od intenda impedire la continuazione o la ripetizione di una violazione già avvenuta, sia da parte dell'autore della violazione che di un intermediario i cui servizi sono utilizzati per tale violazione, può agire in giudizio per ottenere che il suo diritto sia accertato e sia vietato il proseguimento della violazione. Pronunciando l'inibitoria, il giudice può fissare una somma dovuta per ogni violazione o inosservanza successivamente constatata o per ogni ritardo nell'esecuzione del provvedimento.

L'art. 156-bis costituisce il vero punto principale di contatto con le disposizioni statunitensi e consente di considerare trasposto in Italia un istituto di "*discovery*" non dissimile da quelli del sistema americano, sebbene debba essere più correttamente considerato, nel nostro ordinamento, come una misura cautelare[191]. L'articolo in commento dispone che

*1210372, at *8, rev'd on other grounds, America Online, Inc. v. Anonymous Publicly Traded Co., 542 S.E.2d 377 (Va. 2001);Dendrite, 775 A.2d at 760; (2) specificity of the discovery request, Seescandy. Com, 185 F.R.D. at 578, 580;Dendrite, 775 A.2d at 760; (3) the absence of alternative means to obtain the subpoenaed information, see Seescandy.Com, 185 F.R.D. at 579; (4) a central need for the subpoenaed information to advance the claim, America Online, 2000 WL 1210372, at *8;Dendrite, 775 A.2d at 760-61; and (5) the party's expectation of privacy, Verizon, 257 F. Supp.2d at 260-61, 267-68, rev'd on other grounds, Recording Indus. Ass'n of America, Inc. v. Verizon Internet Servs., Inc., 351 F.3d 1229 (D.C. Cir. 2003). As set forth below, each of these factors supports disclosure of defendants' identities*".

191 Si veda ad esempio in merito la tesi sostenuta dal Professor C. CONSOLO, in *Spiegazioni di diritto processuale civile. Volume I, Le tutele (di merito, sommarie ed esecutive) e il rapporto giuridico processuale*, Torino, XII Edizione, 2019. Tale tesi è stata anche parzialmente seguita dalla giurisprudenza di merito, si veda ad esempio Tribunale di Roma, ordinanza 18 agosto 2006, in *Riv. Dir. Ind.*, n 4-5/2008, II, 328, e ordinanze conseguenti, c.d. "Caso Peppermint". Per maggiori riferimenti si segnala altresì G. ALPA, G. RESTA, *Le Persone e la Famiglia 1, Le persone fisiche e i diritti della personalità*, cit., 504 e ss.

qualora una parte abbia fornito seri elementi dai quali si possa ragionevolmente desumere la fondatezza delle proprie domande ed abbia individuato documenti, elementi o informazioni detenuti dalla controparte che confermino tali indizi, essa può ottenere che il giudice ne disponga l'esibizione oppure che richieda le informazioni alla controparte. Può ottenere altresì, che il giudice ordini alla controparte di fornire gli elementi per l'identificazione dei soggetti implicati nella produzione e distribuzione dei prodotti o dei servizi che costituiscono violazione dei diritti d'autore. Il comma terzo del medesimo articolo dispone altresì che il giudice, nell'assumere tali provvedimenti adotti le misure idonee a garantire la tutela delle informazioni riservate, sentita la controparte[192].

L'art. 156-bis non consiste in un mezzo per ottenere informazioni tramite un processo esplorativo, in quanto viene richiesta la dimostrazione di sufficienti prove da cui desumere la violazione del diritto d'autore. Si connatura come una misura cautelare, come tale volta ad evitare che le posizioni soggettive di colui che vanta un diritto vengano irrimediabilmente pregiudicate, consentendo il fruttuoso esercizio di un'azione di cognizione o un'azione esecutiva. Essendo una misura cautelare, il ricorso per ottenerne l'esplicazione dovrà contenere una adeguata argomentazione sia circa il "*fumus boni iuris*", la fondatezza del diritto fatto valere, e del "*periculum in mora*", il rischio di un danno imminente ed irreparabile.

Nel 2006, con decreto legislativo n. 140, è stato introdotto anche un successivo articolo 156-ter il quale dispone che l'autorità giudiziaria sia nei giudizi cautelari che di merito può ordinare, su istanza giustificata e proporzionata del richiedente, che vengano fornite informazioni sull'origine e sulle reti di prestazione di servizi che violano un diritto d'autore da parte dell'autore della violazione e da ogni altra persona che: "*a)sia stata trovata in possesso di merci oggetto di violazione di un diritto, su scala commerciale; sia stata sorpresa a utilizzare servizi oggetto di violazione di un diritto, su scala commerciale; b) sia stata sorpresa a fornire su scala commerciale servizi utilizzati in attività di violazione di un diritto; c) sia stata indicata dai soggetti di cui alle lettere a) o b) come persona implicata nella produzione, fabbricazione o distribuzione di tali prodotti o nella fornitura di tali servizi*". Il comma secondo dell'articolo in commento specifica che tali informazioni comprendono solitamente dati quali il nome e l'indirizzo dei produttori, dei fabbricanti, nonché informazioni sulle quantità prodotte di beni in violazione dei diritti d'autore.

Quanto emerge dalla analisi delle disposizioni legislative italiane è intrinsecamente differente da quanto previamente citato in merito a quelle statunitensi. Sebbene l'art. 156-bis possa apparire come uno strumento di *discovery* sullo stampo del DMCA *subpoena*, non esiste invece uno strumento generale come quello offerto dai *John Doe proceedings*. Tuttavia, si può notare che la legislazione analizzata è particolarmente attenta *all'enforcement* del diritto d'autore e garantisce un mezzo per svelare, potenzialmente, l'identità dei pirati. I titolari dei diritti d'autore, quindi, potrebbero sfruttare questi strumenti per chiedere agli *Internet Service Provider* di svelare l'identità degli utenti connessi alla rete con uno specifico indirizzo IP, così consentendo di procedere con azioni giudiziarie direttamente contro gli utenti finali. Tuttavia, nel sistema italiano ed europeo pare che minor spazio possa essere lasciato alla sorveglianza per la presenza di regolamentazioni molto forti in merito al trattamento dei dati personali. Vedremo infatti che, nella giurisprudenza, quantomeno in un primo momento, la presenza di una forte tutela della privacy, nonché l'intervento delle "*privacy authorities*" abbia fatto propendere il bilanciamento per la tutela della riservatezza, non lasciando spazio alla sorveglianza. Anticipando le conclusioni, vedremo come in sede europea la giurisprudenza sia più altalenante e vi siano forti aperture verso un'esasperata tutela del diritto d'autore.

---

[192] L.C. UBERTAZZI, *Commentario breve alle leggi su proprietà intellettuale e concorrenza, Volume 5 di Breviaria iuris, Padova, 2019.*

Nell'attività di *enforcement* del diritto d'autore, come visto, si rende necessaria la collaborazione degli intermediari di servizi online, di cui si procede ad analizzare la funzione e la responsabilità[193].

6. La necessaria collaborazione degli ISP: la dimensione della responsabilità

Come abbiamo potuto constatare, gli *Internet Service Provider* svolgono sicuramente un ruolo cruciale nella dimensione *dell'enforcement* dei diritti d'autore. Richiamando quanto previamente visto, possiamo affermare che la strategia principalmente adottata dai titolari dei diritti d'autore consisteva nel fare affidamento a delle *service companies* in grado di collezionare dati di utilizzo del traffico delle reti P2P individuando gli indirizzi IP degli utenti, presunti pirati. Le società, quindi, comunicavano i risultati della loro ricerca ai titolari del diritto d'autore i quali necessitavano della collaborazione degli *Internet Service Provider* che sono gli unici a conoscenza delle identità degli utenti cui tali indirizzi sono associati. Sfruttando strumenti quali quelli analizzati nel precedente paragrafo (*John Doe procedings*, DMCA *subpoena* o gli artt. 156 e 156-bis), avrebbero ottenuto la completa *disclosure* della identità degli utenti. Essenziale appare quindi la collaborazione dei *Service Provider*, in quanto in sua assenza non potrebbe essere attuabile tale strategia volta a colpire gli utenti.

Prima di analizzare la giurisprudenza in merito alle tecniche di *enforcement* dei diritti d'autore, è bene fornire notazioni circa la legislazione in merito alla responsabilità dei *Service Provider* in quanto base legale per colpire direttamente le piattaforme di *file-sharing*. *Mutatis mutandis,* in chiosa al primo capitolo si è avuto modo di analizzare il caso antesignano di queste azioni volte a colpire i *provider*: il caso "Betamax". Sebbene esso si riferisse ad un mondo ancora analogico, riuscì a tracciare una linea direttrice di *enforcement* del *copyright* volto a colpire gli intermediari non potendo raggiungere direttamente gli utenti. Chiaramente, come vedremo subito appresso, per esistere una responsabilità secondaria dei *Service Provider* deve prima esistere una responsabilità principale degli utenti, esclusa proprio nel caso Betamax. La questione del ritenere "*fair*" o meno il "*time-shifting*", come visto, si risolveva nella considerazione della sacralità domestica e nella minaccia alla privacy dei cittadini. Escludendo un comportamento integrante "*copyright infringement*" da parte degli utenti, si escludeva altresì la responsabilità della Sony. Queste implicazioni, come anticipato, vennero sfruttate nel passaggio al digitale dalle reti *peer-to-peer*, prima fra tutte Napster[194], poi Aimster[195] ed infine Grokster[196], sicure della vittoria ottenuta nel caso Betamax.

L'importanza della disamina della responsabilità dei *Service Provider*, come apparirà meglio in seguito, è data dal fatto che in primo luogo, l'attacco frontale ai *Service Provider* costituisce, come detto, la prima e principale attività di *enforcement* del diritto d'autore. Sebbene non concerna nello specifico un conflitto diretto con la tutela dei dati personali, consente di procedere ordinatamente ad una completa esposizione delle possibili interrelazioni fra *provider*

---

[193] Per maggiori informazioni sulla legislazione italiana in merito agli articoli 156, 156-bis e 156-ter si faccia riferimento a: A. SIRIOTTI GAUDENZI, *Proprietà intellettuale e diritto della concorrenza. La tutela dei diritti di privativa,* vol. 2, Milano-Torino, 2010; L.C. UBERTAZZI, *Commentario breve alle leggi su proprietà intellettuale e concorrenza,* cit.; F. GIOVANELLA, *Copyright and Information Privacy. Conflicting Rights in Balance*, cit., 113 e ss.

[194] A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (2001), liberamente accessibile presso: «https://casetext.com/case/a-m-records-inc-v-napster-inc-3» (Ultimo accesso: 10 maggio 2022).

[195] In re Aimster Copyright Litigation, 334 F.3d 643 (7th Cir. 2003), liberamente accessibile presso: «https://caselaw.findlaw.com/us-7th-circuit/1484806.html» (Ultimo accesso: 10 maggio 2022).

[196] MGM Studios, Inc. v. Grokster, Ltd., 545 U.S. 913 (2005), liberamente accessibile presso: «https://casetext.com/case/metro-goldwyn-mayer-studios-inc-v-grokster-ltd-3» (Ultimo accesso: 10 maggio 2022).

e titolari dei diritti d'autore, dimostrando lo stretto legame oppositivo che li contrappone. Al contempo, un riferimento compiuto alla giurisprudenza in tema di bilanciamento fra *enforcement* e tutela dei dati personali non può esimersi dal citare quei casi che hanno segnato la storia dei sistemi di *file-sharing* su *reti peer-to-peer*, per i quali la normativa di riferimento è appunto quella sulla responsabilità dei *Service Provider*.

Abbiamo infatti già affermato che gli ISP si sono trasformati in una forma di *governance* privata nel ciberspazio perché conservano una notevole quantità di informazioni sui consumatori relative alle attività online degli utenti.

I titolari dei diritti d'autore hanno ben presto compreso che minacciando ISP di azioni legali per responsabilità concorsuale negli illeciti degli utenti, con un comportamento essenzialmente estorsivo, hanno imposto ai *provider* un governo degli scambi su Internet. Come vedremo, lo standard di responsabilità contributiva di Napster ha creato, secondo parte della dottrina[197], una sorta di accordo di condivisione del potere, in cui i titolari di diritti d'autore procedevano a scandagliare, monitorando, Internet alla ricerca di prove di usi non autorizzati delle opere da loro possedute e gli ISP si trovavano ad affrontare la responsabilità di disabilitare l'accesso a queste opere dopo aver ricevuto un avviso adeguato ai sensi del DMCA. È evidente che quindi la legge ha privatizzato, o ha consentito di privatizzare, la protezione del diritto d'autore, creando incentivi per i proprietari di contenuti protetti dal diritto d'autore a realizzare una sorveglianza degli utenti.

Inoltre, gli ISP svolgono un ruolo chiave nell'applicazione della legge sul *copyright* per due motivi[198]. In primo luogo, fungono da canale attraverso il quale i *copyright holders* identificano l'utente e, in secondo luogo, ai sensi del DMCA, sono costretti a rimuovere il materiale illecito o a interrompere l'accesso a Internet. Pertanto, sono spesso le uniche barriere tra i cittadini comuni e le misure di sorveglianza utilizzate dai proprietari di contenuti per identificarli. Di conseguenza, gli ISP si trovano spesso fra le *simplegadi* di due motivazioni contrastanti: la necessità di proteggere la proprietà intellettuale altrui e la necessità di proteggere privacy, autonomia e libertà di espressione dei loro consumatori.

6.1. 17 U.S.C §512: le "Safe Harbor Provisions"

La legislazione statunitense in merito alla responsabilità dei Service Provider è stata introdotta grazie all'Online Copyright Infringement Liability Limitation Act (OCILLA). Tale riforma riguarda essenzialmente materiale protetto dal diritto d'autore che si collochi nella dimensione online. Riformando il Digital Millennium Copyright Act, introducendo il paragrafo 17 U.S.C §512, stabilisce le c.d. "*Safe Harbor Provisions*". L'obiettivo della riforma, come emerge dai lavori in Senato, era destinato a preservare gli incentivi per i fornitori di servizi online e proprietari di diritti d'autore a collaborare per rilevare e affrontare le violazioni del *copyright* che si verificano nella rete digitale[199].

---

197 S. KATYAL, *Privacy vs. Piracy,* cit., 271 e ss.

198 S. KATYAL, *Privacy vs. Piracy,* cit, 271 e ss.

199 Il riferimento è a quanto affermato dal Senatore Leahy in 144 *Cong. Rec.* S11890 (8 ottobre 1998), liberamente accessibile presso:«https://www.congress.gov/105/crec/1998/10/08/CREC-1998-10-08-pt2-PgS11887.pdf» (Ultimo accesso: 10 maggio 2022). Citando la parte maggiormente interessante nel testo originario: "*Title I of the DMCA will implement the two World Intellectual Property Organization (WIPO) copyright treaties. These treaties will fortify intellectual property rights around the world and will help unleash the full potential of America's most creative industries, including the computer software, publishing, movie, recording and other copyrighted industries that are subject to online piracy. By ensuring better protection of the creative works available online, the DMCA will also encourage the continued growth of the Internet and the global information infrastructure. It will encourage the ingenuity of the American people and will send a powerful message to*

L'approccio adottato dal §512 è volto ad individuare le c.d. "zone franche", i "Safe Harbors" appunto, ossia una serie di circostanze che, ove si verifichino, consentono di non ritenere responsabile il *provider* per violazioni compiute dagli utenti sulla rete.

Si può infatti ricordare come le responsabilità elaborate dalla giurisprudenza americana per la violazione del *copyright* possano essere classificate in tre categorie: "*direct liability", "vicarious liability*" e "*contributory liability*".

La "*direct liability*", disposta dal 17 U.S.C §501 (a), potrebbe essere applicata al *Service Provider* nel caso di contenuti immessi in rete dall'utente sulla considerazione per cui il *provider* memorizzerebbe e duplicherebbe i contenuti caricati sulla piattaforma dall'utente, compiendo non solo una riproduzione, ma altresì una distribuzione illecita. Unico celebre caso in cui tale responsabilità venne applicata, come vedremo, fu il caso "Playboy"; tuttavia, non seguito dalla successiva giurisprudenza e definitivamente superato con il DMCA.

Non potendosi rinvenire una *direct liability*, l'attenzione si spostò nelle parole della giurisprudenza ad una "*vicarious liability*" la quale può assumere due differenti vesti: "*participant-based*" ovvero "*relationship-based*"[200]. Il primo caso si verifica ove il *provider* abbia contribuito o facilitato la violazione dell'utente, necessitando una conoscenza (*knowledge*) della condotta dell'autore dell'illecito ed un contributo alla lesione perpetrata. La seconda ipotesi riflette il principio del "*respondeat superior*", in quanto si rinviene necessaria una relazione fra il *provider* e l'autore dell'illecito ed un beneficio tratto dal *provider* stesso. Il principio è infatti analogo a quello per cui il datore di lavoro dovrebbe rispondere degli illeciti commessi dai suoi dipendenti[201].

---

intellectual property pirates that we will not tolerate theft. I should note that there are provisions in Title I that address certain technologies used to control copying of motion pictures in analog form on video cassette recorders which were not part of either the original Senate or House DMCA bills. These provisions establish certain requirements only for analog videocassette recorders, analog videocassette camcorders and professional analog videocassette recorders. It is my understanding that these provisions do not establish any obligations with respect to digital technologies, including computers or software. It is also my understanding that the intent of the conferees is that these provisions neither establish, nor should be interpreted as establishing, a precedent for Congress to legislate specific standards or specific technologies to be used as technological protection measures, particularly with respect to computers and software. Generally, Congress should not establish technology specific rules; technology develops best and most rapidly in response to marketplace forces. Title II of the DMCA will limit the infringement liability of online Service Providers. This title is intended to preserve incentives for online Service Providers and copyright owners to cooperate to detect and address copyright infringements that occur in the digital networked environment. Title III will provide a minor, yet important, clarification in Section 117 of the Copyright Act to ensure that the lawful owner or lessee of a computer machine may authorize an independent Service Provider, a person unaffiliated with either the owner or lessee of the machine, to activate the machine for the sole purpose of servicing its hardware components. Title IV will begin to update our nation's copyright laws with respect to library, archives, and educational uses of copyrighted works in a digital environment. It includes provisions relating to the Commissioner of Patents and Trademarks and the Register of Copyrights and clarifies the role of the Copyright Office. It also addresses the assumption of contractual obligations related to the transfer of rights in motion pictures. Finally, this title creates a fair and efficient licensing mechanism to address the complex issues facing copyright owners and users of copyrighted materials as a result of the rapid growth of digital audio services. […]".

[200] B. DINWOODIE GRAEME, *A Comparative Analysis of the Secondary Liability of Online Service Providers* (May 17, 2017). *Secondary Liability of Internet Service Providers* (Graeme Dinwoodie ed., Springer 2017); *Oxford Legal Studies Research Paper* No. 47/2017, 2017, 7, liberamente accessibile presso *SSRN*: «https://ssrn.com/abstract=2997891» (Ultimo accesso: 10 maggio 2022); Shapiro, Bernstein and Co. v. H. L. Green Co., 316 F.2d 304 (2d Cir. 1963); Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259 (9th Cir. 1996)

[201] Tale ipotesi venne introdotta in via giurisprudenziale nel celeberrimo caso Shapiro, Bernstein and Co. v. H. L. Green Co., 316 F.2d 304 (2d Cir. 1963), liberamente accessibile presso: «https://www.casemine.com/judgement/us/5914c8f5add7b049347ee60c» (Ultimo accesso: 10 maggio 2022), ma ripreso anche in Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259 (9th Cir. 1996), liberamente accessibile presso: «https://caselaw.findlaw.com/us-9th-circuit/1343384.html» (Ultimo accesso: 10 maggio 2022).

In terzo luogo, la giurisprudenza identifica una "*contributory liability*" colpendo "*colui che, con conoscenza dell'attività illecita, induce, provoca o contribuisce materialmente alla condotta illecita di un altro*"[202]. Si rinvengono nella giurisprudenza almeno due requisiti: la conoscenza dell'illecito ed il concorso all'illecito del terzo. Il punto cruciale in questa forma di responsabilità riguarda proprio la conoscenza che il *provider* deve possedere, potendosi distinguere fra una "*actual knowledge*", una conoscenza effettiva della violazione che comporta sempre una responsabilità, ed una "*constructive knowledge*" in cui il *provider* si suppone a conoscenza dell'illecito essendo stato sollecitato al controllo. In questo secondo caso, la natura ed il grado di responsabilità si complica, rendendosi necessario indagare ulteriormente il livello di conoscenza del *provider* caso per caso[203].

Senza ulteriormente dissertare la estrema problematicità della dimensione di responsabilità dei *provider*, si deve guardare a quanto dispone la Section §512.

I Safe Harbors prevedono quattro principali attività che forniscono quattro diversi livelli di protezione contro le forme di responsabilità applicabili ai *provider*, dipendenti dalla attività che essi realizzano.

In particolare, la Section §512 (a) si occupa della attività di c.d. "*transmission*"[204], ossia dell'attività di coloro che si occupano della trasmissione, conservazione o connessione di dati o informazioni fra diversi punti della rete. Tali *provider* possono andare esenti da responsabilità ove (1) la trasmissione del materiale sia stata avviata da o sotto la direzione di una persona diversa dal fornitore del servizio; (2) la trasmissione, la fornitura di connessioni o l'archiviazione sia avvenuta attraverso un processo tecnico automatico senza selezione del materiale da parte del fornitore del servizio; (3) il prestatore di servizi non abbia selezionato i destinatari del materiale se non come risposta automatica alla richiesta di un'altra persona; (4) nessuna copia del materiale realizzata dal fornitore di servizi nel corso di tale memorizzazione intermedia o transitoria sia stata conservata sul sistema o sulla rete in modo normalmente accessibile a chiunque non sia il destinatario previsto, e tale copia non sia

---

[202] Gershwin Publ'g Corp. v. Columbia Artists Management, Inc., 443 F.2d 1159, 1162 (2d Cir. 1971), liberamente accessibile presso: «https://h2o.law.harvard.edu/cases/4446» (Ultimo accesso: 10 maggio 2022) nel testo originale "*one who, with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another, may be held liable as a 'contributory' infringer*"; si veda anche Religious Tech. Ctr. v. Netcom On-Line Communication Servs., Inc., 907 F. Supp 1361, 1371 (N.D. Cal. 1995); Demetriades v. Kaufmann, 690 F. Supp. 289, 293 (S.D.N.Y. 1988)

[203] Esemplare caso giurisprudenziale in tema è Religious Technology Center v. Netcom On-Line Communication Services, Inc. 907 F. Supp. 1361 (N.D. Cal. 1995), liberamente accessibile presso: «https://www.courtlistener.com/opinion/2249916/religious-tech-center-v-netcom-on-line-comm/» (Ultimo accesso: 10 maggio 2022). Nel caso Netcom la Corte ritiene sufficienti, ai fini dell'integrazione del requisito della conoscenza in capo all'ISP, quelle segnalazioni in grado di far sorgere un ragionevole sospetto di un'effettiva attività illecita.

[204] 17 U.S.C. §512 (a), nel testo originale dispone che: "*(a) Transitory Digital Network Communications.—A Service Provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the provider's transmitting, routing, or providing connections for, material through a system or network controlled or operated by or for the Service Provider, or by reason of the intermediate and transient storage of that material in the course of such transmitting, routing, or providing connections, if— (1) the transmission of the material was initiated by or at the direction of a person other than the Service Provider; (2) the transmission, routing, provision of connections, or storage is carried out through an automatic technical process without selection of the material by the Service Provider; (3) the Service Provider does not select the recipients of the material except as an automatic response to the request of another person; (4) no copy of the material made by the Service Provider in the course of such intermediate or transient storage is maintained on the system or network in a manner ordinarily accessible to anyone other than anticipated recipients, and no such copy is maintained on the system or network in a manner ordinarily accessible to such anticipated recipients for a longer period than is reasonably necessary for the transmission, routing, or provision of connections; and (5) the material is transmitted through the system or network without modification of its content".*

conservata sul sistema o in rete in un modo normalmente accessibile a tali destinatari previsti per un periodo più lungo di quanto sia ragionevolmente necessario per la trasmissione, l'instradamento o la fornitura di connessioni; e (5) il materiale sia trasmesso attraverso il sistema o la rete senza modificarne il contenuto.

La seconda categoria riguarda i c.d. "*System Caching*", ossia di quei *provider* che si occupano del "*web caching*", un meccanismo di archiviazione temporanea di contenuti. Tali materiali vengono in questo modo memorizzati temporaneamente in una "*cache*" volta a rendere più agevole e veloce la navigazione. Tali *provider*, ex §512(b), possono andare esenti da responsabilità ove rispettino le indicazioni ivi elencate.

La terza categoria riguarda i *provider* che si occupano della conservazione di materiale caricato dagli utenti sui propri sistemi. I c.d "*hosting providers*"[205]possono andare esenti da responsabilità ove (i) non siano a conoscenza effettiva che il materiale o un'attività che utilizza il materiale sul sistema o sulla rete stia violando il *copyright*; (ii) in assenza di tale effettiva conoscenza, non sia a conoscenza di fatti o circostanze da cui risulti un'attività illecita; o(iii) dopo aver acquisito tale conoscenza o consapevolezza, agisca tempestivamente per rimuovere o disabilitare l'accesso al materiale. È inoltre necessario che tale *provider* (B) non percepisca un vantaggio finanziario direttamente attribuibile all'attività illecita, nel caso in cui il prestatore di servizi abbia il diritto e la capacità di controllare tale attività; e (C) alla notifica della presunta violazione, risponda tempestivamente per rimuovere, o disabilitare l'accesso al materiale che si ritiene essere in violazione del *copyright* o essere oggetto di attività illecita.

La quarta categoria riguarda infine i *provider* che forniscono "*information-location tools*", ossia l'ipotesi i cui l'intermediario fornisca agli utenti un link ad un sito contenente il materiale richiesto dall'utente: l'ipotesi tipica dei motori di ricerca.

I Safe Harbor, quindi, chiedono al *provider* di non essere a conoscenza dell'attività dell'utente attuata in violazione del diritto d'autore e quindi di attivarsi prontamente per rimuovere o disabilitare l'accesso ai materiali in violazione del diritto d'autore nel momento stesso in cui ricevono una notifica che indichi l'avvenuta violazione del *copyright*. Questa procedura è generalmente conosciuta come il "*notice and takedown*". Tale notifica deve rispettare quanto previsto dal §512 (c)(3), anche in termini di forma[206].

---

[205] 17 U.S.C. §512 (c), nel testo originale dispone che: "*A Service Provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the Service Provider, if the Service Provider— (A) (i) does not have actual knowledge that the material or an activity using the material on the system or network is infringing; (ii) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or (iii) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material; (B) does not receive a financial benefit directly attributable to the infringing activity, in a case in which the Service Provider has the right and ability to control such activity; and (C) upon notification of claimed infringement as described in paragraph (3), responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity".*

[206] Nel testo della legislazione statunitense si legge: "*(A) To be effective under this subsection, a notification of claimed infringement must be a written communication provided to the designated agent of a Service Provider that includes substantially the following:*

(i) A physical or electronic signature of a person authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

(ii) Identification of the copyrighted work claimed to have been infringed, or, if multiple copyrighted works at a single online site are covered by a single notification, a representative list of such works at that site.

(iii) Identification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the Service Provider to locate the material.

(iv) Information reasonably sufficient to permit the Service Provider to contact the complaining party, such as an address, telephone number, and, if available, an electronic mail address at which the complaining party may be contacted.

Ove dovesse mancare anche uno solo dei requisiti la "*notice*" non potrà essere considerata effettiva e quindi non potrà essere presa in considerazione ai fini della presunzione di conoscenza del *provider* dell'attività in violazione dei diritti d'autore posta in essere dagli utenti.

La conoscenza da parte del *provider* è solitamente rinvenuta attraverso il c.d "*red flag test*". Esso si compone di una parte "oggettiva" ed una "soggettiva": la prima analizza se la violazione avrebbe potuto apparire evidente ad una persona ragionevole, la seconda guarda invece alla concreta conoscenza dei fatti o delle circostanze del *provider*. Ne consegue che il punto cruciale è quello di come e quanto il *provider* si curi dei contenuti sulla propria piattaforma, se non se ne cura non vi sarà alcuna responsabilità[207].

Più attentamente, in merito alle forme di conoscenza in capo al provider, si deve fare riferimento a quanto ha recentemente notato il Copyright Office statunitense. In un suo report, esso ha notato come il Congresso non avesse definito la "*actual knowledge*" nella sezione 512, ma che tuttavia si dovesse ritenere che il concetto di "conoscenza effettiva" dovesse essere inteso in un senso differente sia dal test del "*red flag*" che dalla "*constructive knowledge*". Sebbene gli ISP possano ottenere una conoscenza effettiva tramite la ricezione di un avviso di rimozione che sostanzialmente soddisfa i requisiti di legge, allo stesso tempo l'Ufficio per il Copyright afferma che un avviso di rimozione non è un prerequisito necessario affinché un ISP ottenga una "*actual knowledge*". Sul punto quindi il Copyright Office ribadisce che, come riconosciuto dal Congresso, gli ISP possono ottenere conoscenze effettive in diversi modi, ad esempio: (a) utilizzando personalmente il servizio e scoprendo materiale o attività illecite; (b) facendo in modo che un sistema di monetizzazione identifichi ripetutamente una corrispondenza di contenuto o (c) ricevendo un'e-mail che segnala la violazione di un'opera sul sito, in assenza di impegno a monitorare affermativamente il servizio per le violazioni. [208]

Il Copyright Office poi ribadisce anche che in assenza di "*actual knowledge*", la sezione 512 considera per ISP uno standard di conoscenza bastato sul test del "*red flag*". La frase "*red flag*" non compare nello statuto, ma il Congresso è solito farne uso per riferirsi a fatti o circostanze da cui emerga l'esistenza di evidenti attività illecite. Il Congresso, secondo il Copyright Office, intendeva che questo standard di "*red flag*" obbligasse gli ISP a rimuovere o disabilitare l'accesso a contenuti illeciti per i quali avevano appreso informazioni sufficienti

---

(v) A statement that the complaining party has a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law.
(vi) A statement that the information in the notification is accurate, and under penalty of perjury, that the complaining party is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed".

[207] Riferimento alla giurisprudenza sul punto può essere rinvenuto nei casi: 7 v. Corbis Corp. v. Amazon.com, Inc., 351 F. Supp. 2d 1090, (W.D. Wash. 2004), liberamente accessibile presso: «https://casetext.com/case/corbis-corporation-v-amazoncom-2» (Ultimo accesso: 10 maggio 2022); Perfect 10, Inc. v. CCBill LLC, 448. F.3d 1102 (9th Cir. 2007), liberamente accessibile presso:«https://casetext.com/case/perfect-10-inc-v-ccbill-llc» (Ultimo accesso: 10 maggio 2022); UMG Recordings, Inc. v. Veoh Networks, Inc., 665 F. Supp. 2d 1099, (C.D. Cal. 2009), liberamente accessibile presso: «https://casetext.com/case/umg-recordings-56» (Ultimo accesso: 10 maggio 2022), Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19, (2d Cir. 2012), liberamente accessibile presso:«https://cyber.harvard.edu/people/tfisher/cx/2012_Viacom.pdf» (Ultimo accesso: 10 maggio 2022). In questo ultimo caso la giurisprudenza ha affermato che vi è *actual knowledge* quando il *provider* ha una conoscenza soggettiva di una specifica violazione, mentre vi è *red flag knowledge* quando la conoscenza dovrebbe derivare da fatti dai quali un soggetto ragionevole potrebbe oggettivamente comprendere la presenza di una violazione.

[208] Per maggiori riferimenti in merito si veda: United States Copyright Office, *Section 512 of Title 17, A Report Of The Register Of Copyrights*, cit., 113 e ss

e volte ad indicare una probabilità di violazione, ma senza ottenere da queste una "*actual knowledge*". In questo senso, allora, il Congresso intendeva che la conoscenza derivante dallo standard del "*red flag*" bilanciasse attentamente l'obiettivo politico dichiarato di non imporre un onere agli ISP di monitorare il loro servizio o cercare affermativamente fatti che fossero indice di attività illecite con l'obbligo, invece, che un ISP agisca repentinamente ove venga a conoscenza di una "*red flag*" da cui risulti un'attività illecita.[209]

6.2. La Direttiva 2000/31

Anche il contesto euro-italiano si occupa, al pari di quello statunitense, della responsabilità dei Service Provider. Il testo normativo di riferimento è la Direttiva 2000/31/CE, relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno (c.d. "Direttiva sul commercio elettronico" o "Direttiva e-commerce")[210]. Tale Direttiva è stata recepita nel sistema normativo italiano con decreto legislativo 9 aprile 2003 n. 70 tramite una trasposizione essenzialmente *verbatim*[211].

Anche prima dell'intervento comunitario gli ISP erano oggetto di intenso dibattito dottrinale e giurisprudenziale con il quale si resero applicabili le consuete regole di responsabilità civile in assenza di esplicite disposizioni in materia. La questione era tuttavia di particolare complessità per la distinzione sottile fra *"content", "access", "cache"* e *"hosting" provider*. La questione più ostica riguardava il caso in cui l'illecito fosse stato perpetrato da una terza parte che avesse poi immesso e diffuso il contenuto tramite il servizio offerto dal *provider* stesso. Secondo parte della dottrina in questi casi, l'attività compiuta dal *provider* era "*del tutto autonoma rispetto a quella illecita del terzo, pur essendo causalmente la prima condicio sine qua non della verificazione della seconda*"[212]

---

[209] United States Copyright Office, *Ibidem*, 113 e ss.

[210] T. VERBIEST, G. SPINDLER, G. M. RICCIO, *Study on the Liability of Internet Intermediaries*, in *SSRN*, 2007, liberamente accessibile presso: «https://ssrn.com/abstract=2575069» (Ultimo accesso: 10 maggio 2022) o «http://dx.doi.org/10.2139/ssrn.2575069» (Ultimo accesso: 10 maggio 2022); G. M. RICCIO, G. GIANNONE CODIGLIONE, *Copyright Collecting Societies, Monopolistic Positions and Competition in the EU Single Market*, in *Masaryk University Journal of Law and Technology* (MUJLT), Vol. 7, Fall, 2013, liberamente accessibile presso *SSRN*: «https://ssrn.com/abstract=2398891» (Ultimo accesso: 10 maggio 2022); M. L. MONTAGNANI, *A New Interface between Copyright Law and Technology: How User-Generated Content Will Shape the Future of Online Distribution*, in *Bocconi Legal Studies Research Paper* No. 1275326, 2009, liberamente accessibile presso: «https://ssrn.com/abstract=1275326» (Ultimo accesso: 10 maggio 2022) o «http://dx.doi.org/10.2139/ssrn.1275326» (Ultimo accesso: 10 maggio 2022).

[211] Per una analisi anche critica della trasposizione della Direttiva nel contesto normativo italiano si faccia riferimento a: G. M. RICCIO, *La responsabilità civile degli Internet Service Providers, Torino, 2002,* 207-208*;* G. M. RICCIO, *La responsabilità degli Internet providers nel d.lgs. n. 79/03,* in *Danno e Resp.* 1157, 1158ff, 2012*;* T. PASQUINO, *Servizi telematici e criteri di responsabilità*, Milano, 2003*;* M. DE CATA, *La responsabilità civile dell'Internet Service Provider,* Milano, 2010.

[212] G. CASSANO; F. BUFFA, *Responsabilità del content provider e dell'host provider*, in *Il Corriere giuridico*, fasc. 1, 2003, 77-81, liberamente consultabile presso: «https://www.altalex.com/documents/news/2005/07/19/responsabilita-del-content-*provider*-e-dell-host-*provider*» (Ultimo accesso: 10 maggio 2022), i quali in particolare affermano: "*Il vero problema della responsabilità del provider riguarda invece il caso in cui questo debba rispondere del fatto illecito altrui posto in essere valendosi delle infrastrutture di comunicazione del network provider, del server dell'access provider, del sito creato sul server dell'host provider, dei servizi dei Service Provider, delle pagine memorizzate temporaneamente dai cache-providers: in tali casi, infatti, l'attività del provider è del tutto autonoma rispetto quella illecita del terzo, pur essendo causalmente la prima condicio sine qua non della verificazione della seconda.*"

Anche la giurisprudenza ricercava nel diritto vigente improbabili analogie per estendere una qualche forma di responsabilità ai *Service Provider*, oscillando fra una estensione delle norme sulla stampa[213] ad una lata applicazione dell'art. 2055 cod. civ[214].

La Direttiva e-commerce dissipa i dubbi intorno alle precedenti interpretazioni dottrinali, procedendo ad affermare normativamente una responsabilità dei *Service Provider* in ipotesi di violazione dei diritti d'autore online, in considerazione del peculiare ruolo che essi svolgono nella gestione dei contenuti sulla rete.

Le attività che vengono prese in considerazione dalla Direttiva, e di conseguenza dalla legislazione italiana, sono tre: "*mere conduit", "caching" e "hosting"*. Sullo stampo del DMCA, tale responsabilità viene delimitata "in negativo" nel senso che si individuano una serie di condizioni che, ove si verifichino, rendono esenti da responsabilità i *provider* con un meccanismo simile a quello dei "Safe Harbors".

L'art. 12 della Direttiva e l'art. 14 del d.lgs. 70/2003 prendono in considerazione l'attività dei "*mere conduit provider*s" ossia quella consistente nel trasmettere, su una rete di comunicazione, informazioni fornite da un destinatario del servizio, o nel fornire un accesso alla rete di comunicazione. In questo caso, il *provider* potrà essere ritenuto esente da responsabilità a condizione che egli: a) non dia origine alla trasmissione; b) non selezioni il destinatario della trasmissione; e c) non selezioni né modifichi le informazioni trasmesse. Questa è la fattispecie che dimostra un maggior occhio di favore da parte del legislatore comunitario in quanto, per andare esenti da responsabilità, è sufficiente mantenere una posizione neutrale. Inoltre, il *provider*, ove abbia conoscenza di attività illecite poste in essere dai propri utenti, non sarebbe obbligato ad attivarsi per rimuovere tali illeciti, salvo ordine diretto proveniente da un organo giurisdizionale o da un'autorità amministrativa[215].

In secondo luogo, l'art. 13 della Direttiva, o l'art. 15 del decreto legislativo, si occupano dei c.d. "*caching providers*", ossia di coloro che si occupano di una memorizzazione automatica, intermedia e temporanea di informazioni effettuata al solo scopo di rendere più efficace il successivo inoltro ad altri destinatari a loro richiesta. Un tale *provider* potrebbe ritenersi esente da responsabilità a condizione che: a) non modifichi le informazioni; b) si conformi alle condizioni di accesso alle informazioni; c) si conformi alle norme di aggiornamento delle informazioni, indicate in un modo ampiamente riconosciuto e utilizzato dalle imprese del settore, d) non interferisca con l'uso lecito di tecnologia per ottenere dati sull'impiego delle informazioni, ed e) agisca prontamente per rimuovere le informazioni che ha memorizzato,

---

213 Riferimenti rinvenibili in Trib. Napoli, 8 agosto 1997, in *Dir. inf.*, 1997, 970 (caso Cirino Pomicino) e in *Riv. dir. ind.*, 1999, II, 38; Trib. Teramo, 11 dicembre 1997, in *Dir. Informatica*, 1998, 370 con nota di COSTANZO, *Libertà di manifestazione del pensiero e "pubblicazione"*, in Internet nota Tribunale Teramo, 11/12/1997, in *Riv. inf. e informatica* 1998, 2, 372; Trib. Cuneo, 23 giugno 1997 in *Giur. Piemontese*, 1997, 493. In particolare, il tribunale di Napoli afferma che il titolare di un nome di dominio Internet risponde degli eventuali illeciti integrati dal contenuto delle pagine inserite nel sito da lui gestito: su di lui grava infatti un obbligo di diligente verifica circa la legittima titolarità del segno distintivo usato dall'inserzionista e di controllo preventivo circa il contenuto del messaggio, al fine di verificare che la pubblicità sia palese, veritiera e corretta. Tale principio rimane fermo anche se il titolare del nome di dominio si limita alla manutenzione tecnica del sito, mentre la creazione, la gestione e la negoziazione commerciale delle pagine da mettere in rete è affidata ad un soggetto terzo.

214 Trib. Roma 22 marzo del 1999, in *Riv. dir. comm.*, 1999, II, 273, ma si veda anche J. LIGUORI, *La responsabilità degli Internet Service Provider*, Tesi di dottorato, in Diritto, economia e finanza internazionali, Università degli Studi di Parma, 2012, 33-35, liberamente accessibile presso: «https://www.repository.unipr.it/bitstream/1889/1787/3/Tesi%20Jacopo%20Liguori%20La%20Responsabilità%20degli%20Internet%20Service%20Provider.pdf» (Ultimo accesso: 10 maggio 2022).

215 Per maggiori informazioni si faccia riferimento a R. D'ARRIGO, *Recenti sviluppi in tema di responsabilità degli Internet Service Providers*, Milano, 2012, 22-23.

o per disabilitare l'accesso, non appena venga effettivamente a conoscenza del fatto che le informazioni sono state rimosse dal luogo dove si trovavano inizialmente sulla rete o che l'accesso alle informazioni è stato disabilitato oppure che un organo giurisdizionale o un'autorità amministrativa ne ha disposto la rimozione o la disabilitazione dell'accesso.

Infine, l'attività di "*hosting*" è definita dagli artt. 14 della Direttiva e 16 del decreto italiano come quella attività di memorizzazione di informazioni fornite da un utente o destinatario del servizio. Il *provider* in questi casi non è ritenuto responsabile ove a) non sia effettivamente al corrente del fatto che l'attività o l'informazione è illecita e, per quanto attiene ad azioni risarcitorie, non sia al corrente di fatti o di circostanze che rendono manifesta l'illegalità dell'attività o dell'informazione, o b) non appena al corrente di tali fatti, agisca immediatamente per rimuovere le informazioni o per disabilitarne l'accesso. Questa disposizione compie un palese richiamo a quanto abbiamo già avuto modo di indicare in merito alla 17 U.S.C §512 (c)(1)(A), con le connesse notazioni in merito alla "*actual knowledge*" ed al "*red flag test*"[216].

Fra le altre disposizioni, non meno significativa anche la previsione di cui all'art. 15[217], a norma del quale, in queste attività, gli Stati membri non impongono ai prestatori un obbligo generale di sorveglianza sulle informazioni che trasmettono o memorizzano né un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite. Esplicitazione necessaria di un importante principio, infatti, dato che in alcuni Stati membri, come in Italia, la giurisprudenza soleva ritenere civilmente responsabile un ISP per non aver adempiuto ai suoi doversi di sorveglianza[218].

Il secondo comma del medesimo articolo, tuttavia, stabilisce che gli Stati membri possono stabilire che i prestatori di servizi della società dell'informazione (a) siano tenuti ad informare senza indugio la pubblica autorità competente di presunte attività illecite o (b) a comunicare alle autorità competenti, a loro richiesta, informazioni che consentano l'identificazione dei propri utenti.

Nel recepimento di questo articolo, il legislatore italiano aggiunge un comma terzo all'art. 17 del decreto legislativo 70/2003, prevedendo che il *provider* sia altresì civilmente responsabile del contenuto dei suoi servizi nel caso in cui, richiesto dalle competenti autorità, non abbia agito prontamente per impedire l'accesso a detto contenuto, ovvero se, avendo avuto conoscenza del carattere illecito o pregiudizievole per un terzo del contenuto in questione, non abbia provveduto ad informarne l'autorità competente. Tale comma è diretta espressione non già del testo della Direttiva, bensì del suo Considerando 48 il quale consente agli Stati membri di imporre ai prestatori di servizi di adempiere al dovere di diligenza che è ragionevole attendersi da loro al fine di individuare e prevenire taluni tipi di attività illecite. Tuttavia, la giurisprudenza in merito è stata discontinua nell'interpretazione[219].

---

[216] G.M. RICCIO, *La responsabilità civile degli Internet providers*, Torino, 2002, 207-208, liberamente accessibile presso:«https://www.researchgate.net/publication/286454131_La_responsabilita_civile_degli_Internet_providers» (Ultimo accesso: 10 maggio 2022); U. DRAETTA, *Internet e commercio elettronico*, Milano, 2001, 81.

[217] Tale articolo, come vedremo sarà oggetto di particolare attenzione della Corte di Giustizia nei casi CGUE 24 novembre 2011, C-70/10, *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, (Terza Sezione), liberamente accessibile presso: «https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:62010CJ0070&from=EN» (Ultimo accesso: 10 maggio 2022).

[218] Trib. Cuneo, (ord) 23 agosto 1997, in *AIDA*, 1997, 500.

[219] Riferimenti a: Trib. Milano 9 settembre 2011, in *Rivista Diritto Industriale* 2011, 375; ma anche in senso contrario Corte di Appello di Milano 7 gennaio 2015 in *Resp. Civ. Prev.*, 2015, 1245, sulla qualificazione di "Yahoo!" come un hosting *provider*.

La normativa ha attirato molte critiche da parte della dottrina, la quale ritenne che tale regolamentazione non garantisse sufficientemente il diritto alla libertà di pensiero e di informazione, tanto che venne sollevata altresì una questione di costituzionalità proprio in merito a queste censure, prontamente rigettate tuttavia dalla Corte Costituzionale[220].

Con queste notazioni si chiude la disamina della legislazione in merito alla responsabilità dei *provider*, soggetti che svolgono un ruolo primario nella lotta fra *l'enforcement* del diritto d'autore e la tutela della privacy e dei dati personali. Di seguito si passa a proporre, sempre in chiave comparatistica, una analisi della giurisprudenza che segna il cammino *dell'enforcement* del diritto d'autore. Nelle parole della giurisprudenza vedremo attuarsi quelle due strategie da cui si è voluto partire. Innanzitutto, il riferimento sarà alle azioni giudiziarie volte ad inibire servizi informativi per il *file-sharing*, ed in un secondo momento l'attenzione verrà spostata sulle azioni giudiziarie e stragiudiziarie volte a colpire gli utenti delle reti P2P.

7. Il bilanciamento nelle parole della giurisprudenza

7.1. Casi statunitensi: I primi attacchi ai Service Provider

7.1.1. CASO PLAYBOY: una vicenda isolata

Il primo caso da analizzare costituisce un precedente isolato in ambito statunitense, prontamente superato dalla giurisprudenza più accorta[221]. In esso si stabiliva una responsabilità diretta del *provider* per i contenuti caricati dall'utente sulla piattaforma online. Nel momento in cui un utente avesse proceduto a caricare del materiale, per meccanismi informatici intrinseci al funzionamento delle piattaforme, il *provider* avrebbe memorizzato e dunque copiato i contenuti per renderli visibili sulla rete. In tal modo il *provider* avrebbe commesso una riproduzione illecita ed una distribuzione del materiale, con connessa violazione del diritto di "*public display*". La presa di posizione della Corte distrettuale degli Stati Uniti per il distretto centrale della Florida per una forma di "*direct liability*" non venne seguita dalla successiva giurisprudenza. Le ragioni sono anche dovute ad una prospettiva di politica del diritto in quanto si affermò la consapevolezza che una tale responsabilità avrebbe frenato lo sviluppo tecnologico delle piattaforme online, ostacolandone irrimediabilmente il funzionamento. È bene comunque riaffermare che con il DMCA il Congresso considerò definitivamente superata tale affermazione.

Nonostante la singolarità nel panorama giurisprudenziale di questo caso, è bene tratteggiare brevemente il ragionamento della Corte segnalando il punto di diritto che ha condotto all'affermazione di una "*direct liability*".

La fattispecie concreta è un *topos* ricorrente di questo elaborato, ossia il caricamento di contenuti online da parte dell'utente in violazione del *copyright*. Infatti, il convenuto George Frena gestiva un servizio di bacheca informatica, Techs Warehouse BBS ("BBS"). Le

---

[220] In merito si veda la sentenza C. Cost. 3 dicembre 2015 n. 247, in *Foro.it,* 2016, I, 405 la cui massima dispone: "*È inammissibile, in quanto formulata in maniera contraddittoria, ambigua ed oscura, la questione di legittimità costituzionale degli art. 5, 1° comma, 14, 3° comma, 15, 2° comma, 16, 3° comma, d.leg. 9 aprile 2003 n. 70 e 32 bis, 3° comma, d.leg. 31 luglio 2005 n. 177, nella parte in cui consentono all'autorità per le garanzie nelle comunicazioni (Agcom), quale autorità amministrativa di vigilanza, di limitare la libera circolazione di un «servizio della società dell'informazione» e, segnatamente, di intervenire anche in via d'urgenza su attività quali il trasporto o la memorizzazione di informazioni, attribuendole anche il potere di emanare le disposizioni regolamentari considerate necessarie a rendere effettiva l'osservanza dei diritti di proprietà intellettuale da parte dei prestatori di servizi sulle reti di comunicazione elettronica, in riferimento agli art. 2, 21, 24, 25, 1° comma, e 41 cost".*

[221] Playboy Enterprises, Inc. v. Frena, 839 F.Supp. 1552 (1993), liberamente accessibile presso: «https://casetext.com/case/playboy-enterprises-inc-v-frena» (Ultimo accesso: 10 maggio 2022).

fotografie protette da *copyright* dell'attore Playboy Entertainment, Inc. ("PEI") erano state caricate su BBS senza autorizzazione. Gli utenti di BBS, infatti, potevano sfogliare e scaricare le fotografie in immagini di alta qualità che potevano poi essere archiviate sul computer personale dell'utente. Centosettanta delle immagini disponibili su BBS erano copie di fotografie tratte da materiali protetti da *copyright* di Playboy. George Frena era stato chiaro sin da subito: nessuna di quelle immagini era stata caricata direttamente dai propri server: "la colpa" era degli utenti. Tanto è confermato anche dal fatto che Frena affermava che non appena gli venne notificata la violazione dei diritti autorali aveva provveduto a rimuovere le fotografie e sin da allora aveva monitorato le bacheche BBS per impedire il caricamento di ulteriori immagini di Playboy.

In diritto, la Corte Distrettuale ricorda che il Copyright Act del 1976 conferiva ai titolari del *copyright* il controllo sulla maggior parte, se non su tutte, le attività di concepibile valore commerciale di sfruttamento delle opere protette. Infatti, per la normativa statunitense, il titolare di un diritto d'autore "*ha il diritto esclusivo di fare e di autorizzare una delle seguenti azioni: (1) riprodurre l'opera protetta da copyright; (2) preparare opere derivate basate sull'opera protetta da copyright; (3) distribuire copie dell'opera protetta da copyright al pubblico e (5) nel caso di opera figurativa, di mostrare pubblicamente (c.d "public display") l'opera protetta da copyright*"[222]. Compiere dunque una qualsiasi di queste attività senza il permesso del titolare del *copyright* viola i diritti esclusivi dello stesso sulla base del 17 USC § 501(a).

Playboy, per affermare una violazione diretta del *copyright* da parte di George Frena avrebbe dovuto dimostrare l'attività di riproduzione posta in essere dal convenuto. Poiché la Corte riconosce che una prova diretta della copia è raramente disponibile in un'azione di violazione del diritto d'autore, la copia può essere provata inferenziale mostrando che il convenuto Frena aveva avuto accesso all'opera presumibilmente violata e di conseguenza che essa era sostanzialmente simile ("*substantially similar*") a quella protetta da *copyright*[223].

Secondo la Corte, l'accesso all'opera protetta da *copyright* non è in discussione in quanto, a suo tempo, ogni mese la rivista Playboy vendeva oltre 3,4 milioni di copie. Altresì afferma che la prova delle "*substantial similarities*" non costituisce un ostacolo in quanto Frena aveva ammesso che ciascuna delle immagini contestate era sostanzialmente simile alla fotografia protetta da *copyright* di Playboy. Non potendosi dunque contestare la riproduzione compiuta, secondo la Corte diviene necessario investigare anche altri diritti di esclusiva economica potenzialmente violati da George Frena.

---

[222] Nelle parole della Corte si legge: "*The Copyright Act of 1976 gives copyright owners control over most, if not all, activities of conceivable commercial value. The statute provides that the owner of a copyright . . . has the exclusive rights to do and to authorize any of the following: (1) to reproduce the copyrighted work in copies . . .; (2) to prepare derivative works based upon the copyrighted work; (3) to distribute copies . . . of the copyrighted work to the public . . . and (5) in the case of . . . pictorial . . . works . . . to display the copyrighted work publicly. 17 U.S.C. § 106. Engaging in or authorizing any of these categories without the copyright owner's permission violates the exclusive rights of the copyright owner and constitutes infringement of the copyright. See 17 U.S.C. § 501(a)*"

[223] Nello stesso senso si pone anche la giurisprudenza richiamata dalla Corte stessa: Howard v. Sterchi , 974 F.2d 1272 (11° Cir. 1992); Ford Motor Co. contro Summit Motor Products, Inc., 930 F.2d 277, 291 (3d Cir. 1991).

Nello specifico, la Corte riconosce come il convenuto avesse altresì violato il diritto di distribuzione dell'opera[224] ed il diritto di c.d. "Public Display"[225].

Anche i tentativi di invocare il *fair use* o la "*de minimis doctrine*" non furono fruttuosi, tanto che la Corte afferma: "*there is irrefutable evidence of direct copyright infringement in this case. It does not matter that Defendant Frena may have been unaware of the copyright infringement. Intent to infringe is not needed to find copyright infringement. Intent or knowledge is not an element of infringement, and thus even an innocent infringer is liable for infringement; rather, innocence is significant to a trial court when it fixes statutory damages, which is a remedy equitable in nature*"[226].

La decisione della Corte, quindi, ritenne applicabile la tradizionale "*direct liability*" sulla considerazione che l'intenzionalità della violazione del diritto d'autore o la conoscenza dell'illecito non costituiscono elementi essenziali della responsabilità, andandosi a configurare una sorta di responsabilità oggettiva in capo al *provider* per le violazioni in realtà commesse dai suoi utenti.

L'evidente disequilibrio della decisione, nonché i potenziali ostacoli ad una affermazione della rete e dei servizi su essa offerti, portarono ad un rapido superamento della decisione.

7.1.2. CASO NAPSTER

---

[224] Nelle parole della Corte: "*Public distribution of a copyrighted work is a right reserved to the copyright owner, and usurpation of that right constitutes infringement. See Cable/Home Communication Corp. v. Network Productions, Inc., 902 F.2d 829, 843 (11th Cir. 1990). PEI's right under 17 U.S.C. § 106(3) to distribute copies to the public has been implicated by Defendant Frena. Section 106(3) grants the copyright owner "the exclusive right to sell, give away, rent or lend any material embodiment of his work." 2 MELVILLE B. NIMMER, Nimmer on Copyright § 8.11[A], at 8-124.1 (1993). There is no dispute that Defendant Frena supplied a product containing unauthorized copies of a copyrighted work. It does not matter that Defendant Frena claims he did not make the copies itself. See JAY DRATLER, JR., Intellectual Property Law: Commercial, Creative and Industrial Property § 6.01[3], at 6-15 (1991).*"

[225] Nelle parole della Corte*: "Furthermore, the "display" rights of PEI have been infringed upon by Defendant Frena. See 17 U.S.C. § 106(5). The concept of display is broad. See 17 U.S.C. § 101. It covers "the projection of an image on a screen or other surface by any method, the transmission of an image by electronic or other means, and the showing of an image on a cathode ray tube, or similar viewing apparatus connected with any sort of information storage and retrieval system." H.R. Rep. No. 1476, 94th Cong., 2d Sess. 64 (Sept. 3, 1976), reprinted in 1976 U.S. Code Cong. Admin. News 5659, 5677. The display right precludes unauthorized transmission of the display from one place to another, for example, by a computer system. See H.R. Rep. No. 1476, 94th Cong., 2d Sess. 80 (Sept. 3, 1976), reprinted in 1976 U.S. Code Cong. Admin.News 5659, 5694; JAY DRATLER, JR., Intellectual Property Law: Commercial, Creative and Industrial Property § 6.01[4], at 6-24 (1991). "Display" covers any showing of a "copy" of the work, "either directly or by means of a film, slide, television image or any other device or process." 17 U.S.C. § 101. However, in order for there to be copyright infringement, the display must be public. A "public display" is a display "at a place open to the public or . . . where a substantial number of persons outside of a normal circle of family and its social acquaintenances is gathered." 2 MELVILLE B. NIMMER, Nimmer on Copyright § 8.14[C], at 8-169 (1993). A place is "open to the public" in this sense even if access is limited to paying customers. 2 MELVILLE B. NIMMER, Nimmer on Copyright § 8.14[C], at 8-169 n. 36 (1993); see Columbia Pictures Indus., Inc. v. Redd Horne Inc., 749 F.2d 154 (3d Cir. 1984). Defendant's display of PEI's copyrighted photographs to subscribers was a public display. Though limited to subscribers, the audience consisted of "a substantial number of persons outside of a normal circle of family and its social acquaintenances." 2 MELVILLE B. NIMMER, Nimmer on Copyright § 8.14[C], at 8-169 (1993). See also Thomas v. Pansy Ellen Products, 672 F. Supp. 237, 240 (W.D.North Carolina 1987) (display at a trade show was public even though limited to members); Ackee Music, Inc. v. Williams, 650 F. Supp. 653 (D.Kan. 1986) (performance of copyrighted songs at defendant's private club constituted a public performance).*"

[226] Traducendo liberamente, la Corte afferma che "*Ci sono prove inconfutabili di violazione diretta del copyright in questo caso. Non importa che il convenuto Frena non fosse a conoscenza della violazione del copyright. L'intenzione non è necessaria per rinvenire una violazione del copyright. L'intenzione o la conoscenza non sono elementi essenziali per dimostrare tale violazione, e quindi anche un trasgressore innocente è responsabile della violazione; piuttosto, l'innocenza è significativa per un tribunale quando determina i danni legali, che sono un rimedio di natura equitativa.*"

La necessaria introduzione con il Caso Playboy conduce l'attenzione del presente elaborato al caso forse più noto in tema di *file-sharing*, capace di attirare l'attenzione della stampa a livello globale. Questo caso rientra nell'ambito di interesse della nostra trattazione in quanto Napster è stato il primo esempio di una architettura di *file-sharing* strutturata secondo il modello *peer-to-peer* in cui gli utenti iniziarono a scambiarsi principalmente, sebbene non esclusivamente, materiale protetto dal diritto d'autore. *L'enforcement* del diritto d'autore allora non poteva esimersi dal colpire queste piattaforme.

Napster era stato fondato nel 1999 da Shawn Fanning, allora uno studente di informatica presso Northeastern University, appena maggiorenne. L'ideatore aveva fornito agli utenti una piattaforma per scaricare file musicali digitali, in particolare MP3, dalle macchine di altri utenti. A differenza di molti altri servizi *peer-to-peer* che vedremo in seguito, Napster includeva un server centrale che indicizzava gli utenti connessi e i file disponibili sui loro computer, creando un elenco ricercabile di musica disponibile sulla rete di Napster. La facilità d'uso di Napster rispetto ad altri servizi *peer-to-peer* lo rese rapidamente un servizio popolare per gli appassionati di musica per trovare e scaricare gratuitamente file di brani digitali.

Gli utenti della rete potevano infatti scaricare da Internet il software di Napster che avrebbe consentito loro di interconnettersi ad un sistema di scambio online di materiali. Ebbe un largo successo tanto che vennero scaricate illegalmente centinaia di migliaia di canzoni protette dal *copyright*. Non servì attendere molto allora affinché i titolari dei diritti d'autore si muovessero legalmente contro Napster[227]. Questa azione legale costituisce piena espressione della prima di quelle due strategie che questo capitolo si proponeva di investigare ossia di quelle "*Azioni giudiziarie, di prima generazione, volte ad inibire servizi informativi per il file sharing*"[228].

Sebbene il caso sia denominato A&M Records, Inc. v. Napster, l'elenco completo degli attori includeva un certo numero di case discografiche, tutti membri della Recording Industry Association of America (RIAA). Quindi, come accennato, le principali case discografiche contestarono la distribuzione gratuita su larga scala della loro musica e citarono in giudizio Napster per "*direct", "vicarious"* e *"contributory" infringement*.

La Corte, prima di passare ad analizzare i punti di diritto, parte da una costatazione informatica, mostrando come la tecnologia abbia modificato le modalità di violazione del diritto d'autore, profondendosi copiosamente nel funzionamento del sistema Napster. In particolare, essa afferma che nel 1987, il Moving Picture Experts Group aveva introdotto un formato di file standard per l'archiviazione di registrazioni audio in un formato digitale chiamato MPEG-3, abbreviato in "MP3". I file MP3 digitali venivano creati attraverso un processo chiamato colloquialmente "*ripping*". Il software di *ripping* consentiva al proprietario

---

[227] Per maggiori informazioni sul caso Napster si veda: G. PASCUZZI, *Opere musicali su Internet: il formato MP3* in *Foro it.,* 2001, IV, 101-111.; P. AUTIERI, *Il Caso Napster alla luce del diritto comunitario*", in Luigi Carlo Ubertazzi (ed.), *TV, Internet e "new trends" di diritti d'autore e connessi*, 2003; Case Study: *A&M Records, Inc. v. Napster, Inc.*, Washington University In Saint Louis, School of Law, 2013, liberamente accessibile presso: «https://onlinelaw.wustl.edu/blog/case-study-am-records-inc-v-napster-inc/» (Ultimo accesso: 10 maggio 2022); *A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004* (9th Cir. 2001), *U.S. Copyright Office Fair Use Index,* liberamente accessibile presso: «https://www.*copyright*.gov/fair-use/summaries/a&mrecords-napster-9thcir2001.pdf» (Ultimo accesso: 10 maggio 2022); A&M Records, Inc v. Napster, 114 F. Supp. 2d 896, 900 (N.D. Cal 2000), liberamente accessibile presso: «https://law.justia.com/cases/federal/district-courts/FSupp2/114/896/2343353/» (Ultimo accesso: 10 maggio 2022); A&M Records, Inc v. Napster, Inc., 239 F.3d 1004 (2001), liberamente accessibile presso: «https://casetext.com/case/a-m-records-inc-v-napster-inc-3» (Ultimo accesso: 10 maggio 2022).

[228] R. CASO, *Il conflitto tra copyright e privacy nelle reti Peer to Peer: il caso Peppermint – Profili di diritto comparato*, cit., 3 e ss.

di un computer di copiare un compact disk audio ("CD audio") direttamente sul disco rigido di un computer, comprimendo le informazioni audio del CD nel formato MP3. Il formato compresso consentiva dunque la trasmissione rapida di file audio digitali da un computer all'altro tramite posta elettronica o qualsiasi altro protocollo di trasferimento file.

Napster, in questo, facilitava la trasmissione di file MP3 tra i suoi utenti. Consentiva infatti ai suoi utenti di: (1) rendere disponibili file musicali MP3 archiviati sui dischi rigidi dei singoli computer per la copia da parte di altri utenti Napster; (2) cercare file musicali MP3 archiviati sui computer di altri utenti; e (3) trasferire copie esatte dei contenuti dei file MP3 di altri utenti da un computer all'altro tramite Internet. Queste funzioni erano rese possibili dal software *MusicShare* di cui il sistema di *file-sharing* si avvaleva[229].

Ove un utente avesse desiderato mettere a disposizione su Napster i file audio presenti sul proprio disco rigido, affinché altri ne avessero accesso, avrebbe dovuto per prima cosa creare una *directory* "libreria utente" sul proprio disco rigido. L'utente avrebbe dovuto quindi salvare i suoi file MP3 nella *directory* della libreria. Successivamente avrebbe dovuto accedere al sistema Napster utilizzando il proprio nome utente e password. Il software *MusicShare* ricercava quindi la libreria utente e verificava che i file disponibili fossero formattati correttamente. Il contenuto dei file MP3 rimaneva memorizzato nel computer dell'utente.

Una volta caricati sui server Napster, i nomi dei file MP3 dell'utente venivano archiviati in una "libreria" sotto il nome dell'utente e diventano parte di una *directory* collettiva di file disponibili per il trasferimento.

Per trasferire una copia del contenuto di un file MP3 richiesto, il software del server Napster otteneva l'indirizzo Internet dell'utente richiedente e l'indirizzo Internet dell'utente *host* (l'utente con i file disponibili). Il computer dell'utente richiedente stabiliva dunque una connessione con l'utente *host* e scaricava una copia del contenuto del file MP3 da un terminale all'altro tramite Internet.

In primo grado, la Corte distrettuale[230] rinveniva come, diversamente dalla Sony nel caso Betamax, Napster effettivamente facilitasse la distribuzione di materiale protetto dal diritto d'autore in quanto manteneva un continuo controllo sugli accessi degli utenti e sul materiale caricato. Questo in quanto il suo software creava una libreria utente in ciascun dispositivo e consentiva la ricerca dei file e lo scambio *peer-to-peer*. Dato tale coinvolgimento, la Corte distrettuale affermò che Napster non potesse godere della Section §512, dei *Safe Harbors*; quindi, ritenne il *provider* responsabile per "*vicarious infringement*".

In sede di gravame, la Corte di appello[231] confermò la presa di posizione della Corte distrettuale affermando come Napster fosse sicuramente consapevole delle violazioni del diritto d'autore commesse dagli utenti, affermando altresì che avesse la possibilità di controllare l'uso della piattaforma da parte degli utenti ma scelse invece di incoraggiare ed assistere gli utenti nelle loro attività illecite. Le difese di *fair use*[232] di Napster non ressero gli attacchi degli attori.

---

[229] Nelle parole della Corte: "*Through a process commonly called "peer-to-peer" file sharing, Napster allows its users to: (1) make MP3 music files stored on individual computer hard drives available for copying by other Napster users; (2) search for MP3 music files stored on other users' computers; and (3) transfer exact copies of the contents of other users' MP3 files from one computer to another via the Internet. These functions are made possible by Napster's MusicShare software, available free of charge from Napster's Internet site, and Napster's network servers and server-side software*"

[230] A&M Records, Inc v. Napster, 114 F. Supp. 2d 896, 900 (N.D. Cal 2000), cit.

[231] A&M Records, Inc v. Napster, Inc., 239 F.3d 1004 (2001), cit.

[232] Il tribunale si è poi rivolto ai tre usi che Napster ha identificato come *fair* use nella condotta dei suoi utenti. Il primo era il c.d. *sampling*, in cui gli utenti facevano copie temporanee di un'opera per testarla prima

In particolare, nell'escludere le difese di *fair use*, i giudici di appello concordarono con la conclusione del tribunale distrettuale che aveva constatato come il download di un MP3 non consistesse in un "atto trasformativo" e che, sebbene Napster non avesse beneficiato finanziariamente, in via diretta, dei download degli utenti, il ripetuto sfruttamento della copia di opere protette da *copyright*, anche se non vendute, avrebbe potuto essere considerato un uso commerciale. La Corte ha anche confermato la conclusione del tribunale distrettuale secondo cui le opere creative, come le canzoni in questione, sono "*closer to the core*" della prevista protezione del diritto d'autore rispetto alle opere non creative. Infine, il Nono Circuito ha concordato con la conclusione del tribunale distrettuale secondo cui il diffuso trasferimento all'ingrosso della musica dell'attore ha influito negativamente sul mercato delle vendite di CD e che ha messo anche a rischio il futuro dell'industria discografica nei mercati digitali. [233]

Infine, come la Corte distrettuale, anche la Corte di appello ha ritenuto che i proprietari di Napster potessero controllare il comportamento illecito degli utenti, e quindi avessero il dovere di farlo, imponendo una responsabilità secondaria. Infatti, secondo la Corte, per provare un "*contributory infringement*", un attore deve dimostrare che il convenuto era a conoscenza della violazione (qui, che Napster sapeva che i suoi utenti stavano distribuendo contenuti protetti da *copyright* senza autorizzazione attraverso la sua rete) e che il convenuto avesse fornito supporto materiale a tale violazione. In merito al requisito della conoscenza, il tribunale distrettuale ha stabilito che "*law does not require knowledge of specific acts of infringement*" e ha respinto le difese di Napster circa l'assenza di una effettiva conoscenza, basate sul presupposto per cui non sarebbe stato in grado di distinguere tra file leciti od illeciti. Il Nono Circuito ha confermato questa analisi, accettando che Napster avesse *"knowledge, both actual and constructive, of direct infringement*".

Il Nono Circuito ha anche affermato che Napster non avrebbe potuto invocare in propria difesa il precedente dato da Sony Corp. of America v. Universal City Studios, Inc., "il caso Betamax", a causa della "*conoscenza effettiva e specifica di violazione diretta*" di Napster. Tuttavia, il Nono Circuito ha rilevato che, "*indipendentemente dal numero di usi illeciti rispetto a quelli non illeciti di Napster*", la questione potrebbe essere risolta sulla base del fatto che "*Napster sapeva o aveva motivo di sapere della violazione dei diritti d'autore dei ricorrenti da parte dei suoi utenti*".

Per il secondo requisito la Corte nota che, in base ai fatti accertati dal tribunale distrettuale, Napster contribuisce altresì materialmente all'attività illecita. La Corte, infatti,

---

dell'acquisto, che il tribunale distrettuale ha ritenuto essere un uso commerciale anche se un utente avesse dovuto acquistare l'opera in un secondo momento. Il "*sampling*" è stato ritenuto non un *fair use*, perché i "campioni" erano in realtà permanenti e copie complete del supporto desiderato. In secondo luogo, si prende in considerazione il c.d "*space-shifting*" , in cui gli utenti accedono a una registrazione audio tramite Napster ma che in realtà già possiedono in formato CD audio; qui il tribunale distrettuale ha ritenuto che nessuna delle analisi utilizzate nei casi Sony-betamax o RIAA v. Diamond Multimedia si applicasse in questo caso perché lo "spostamento" in nessuno dei due casi includeva o consentiva la distribuzione. L'argomento dello spostamento dello spazio non ha avuto successo perché, mentre il passaggio a un formato digitale potrebbe essere stato un uso di archiviazione personale, è stato accompagnato dal rendere il file disponibile al resto degli utenti del sistema. In terzo luogo, Napster proponeva il concetto di "*permissive distribution*" di registrazioni da parte di artisti sia nuovi che affermati che hanno autorizzato la diffusione della loro musica nel sistema Napster. In questo caso la Corte ha stabilito che tale utilizzo non fosse illecito e quindi ne consentiva la continuazione.

[233] Maggiori informazioni rinvenibili presso *Case Study: A&M Records, Inc. v. Napster, Inc.*, *Washington University In Saint Louis*, School of Law, 2013, liberamente accessibile presso: «https://onlinelaw.wustl.edu/blog/case-study-am-records-inc-v-napster-inc/» (Ultimo accesso: 10 maggio 2022); *Case study: A&M Records, Inc. v Napster Inc. (2001),* liberamente accessibile presso: «https://www.dcs.k12.oh.us/site/handlers/filedownload.ashx?moduleinstanceid=1862&dataid=1923&FileName=Napster_Case_Summary.pdf» (Ultimo accesso: 10 maggio 2022).

statuisce che, senza i servizi di supporto forniti dal convenuto, gli utenti non avrebbero potuto trovare e scaricare la musica che desideravano con la facilità offerta invece dal sistema Napster.

Per queste ragioni, quindi, Napster venne ritenuto responsabile per *contributory lability*. Con Napster l'industria musicale poté considerare vinta la prima battaglia legale contro le tecnologie *peer-to-peer*. Nonostante Napster abbia subito i colpi delle *majors* discografiche, la sua attività ha segnato un importante precedente storico: gli utenti avevano avuto modo di fruire della circolazione della musica online.

Come notato da parte della dottrina, gli esiti della sentenza vanno oltre la mera declamazione di una responsabilità secondaria di Napster. Sonia Katyal[234] in merito afferma che il caso Napster ha creato una sorta di accordo di condivisione del potere, in cui i titolari dei diritti d'autore si assumevano la responsabilità di sorvegliare Internet alla ricerca di prove di usi non autorizzati delle proprie opere e gli ISP si trovavano ad affrontare la responsabilità di disabilitare l'accesso a queste opere illecite dopo aver ricevuto un avviso adeguato ai sensi del DMCA: una funzione di governo e di *enforcement* dei diritti d'autore sul web. A sua volta, la legge ha privatizzato la protezione del diritto d'autore, creando incentivi per i *copyright holders* verso la sorveglianza delle attività dei consumatori.

Se quindi così si imposta la dinamica all'alba di Napster, appare subito chiaro che, in questo quadro, manca qualcosa: un impegno per la tutela della privacy dei consumatori. Se infatti gli ISP sono indirettamente incoraggiati a monitorare i propri consumatori per sottrarsi a responsabilità, i rischi di trattamenti dei dati personali illeciti, nonché i rischi per l'autodeterminazione degli utenti online, sono alti. Più le tecnologie di sorveglianza dei consumatori alterano il tessuto del cyberspazio e si espandono per smascherare e registrare le attività e le identità degli abbonati Internet, più diventa difficile proteggere adeguatamente le aspettative di riservatezza dei cittadini.

7.1.3. CASO AIMSTER

Analogamente a quanto avvenuto con Napster, anche nel Caso Aimster[235] i titolari dei diritti d'autore su opere musicale, le *majors* discografiche, citarono in giudizio il server P2P per "*contributory"* e *"vicarious infringement*" dei rispettivi diritti di esclusiva economica.

Le modalità di funzionamento del *file-sharing peer-to-peer* di Aimster erano molto simili a quelle di Napster per molti aspetti, ma differivano in un punto: la crittografia impediva agli operatori del sistema Aimster di conoscere il contenuto dei file condivisi dai suoi utenti. Tuttavia, le intenzioni dei creatori di Aimster erano ragionevolmente chiare dato che

---

234 S. KATYAL, Privacy vs. Piracy, cit., 263 e ss.

235 In re Aimster Copyright Litigation, 334 F.3d 643 (7th Cir. 2003), il cui testo è liberamente rinvenibile presso: «https://law.justia.com/cases/federal/appellate-courts/F3/334/643/636193/» (Ultimo accesso: 10 maggio 2022); notazioni in merito possono rinvenirsi principalmente L. A. HOLLAAR, *Sony Revisited: A new look at contributory copyright infringement*, in *University of Utah*, 2004, liberamente accessibile presso: «http://digital-law-online.info/papers/lah/sony-revisited-june6.pdf» (Ultimo accesso: 10 maggio 2022); E. MILES, *In re Aimster & MGM, Inc. v. Grokster, Ltd.: Peer-to-Peer and the Sony Doctrine,* in *Berkeley Technology Law Journal*, 19(1), 2004, 21–57, liberamente accessibile presso: «http://www.jstor.org/stable/24117528» (Ultimo accesso: 10 maggio 2022); R. AXBERG, *File-Sharing Tools and Copyright Law: A Study of In re Aimster Copyright Litigation and MGM Studios, Inc. v. Grokster, Ltd.*, Volume 35 Issue 1 Fall 2003, *Loyola University Chicago Law Journal*, 2003, liberamente accessibile presso:
«https://lawecommons.luc.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1280&context=luclj» (Ultimo accesso: 10 maggio 2022).

fornivano agli utenti tutorial online che mostravano loro come utilizzare il sistema per scambiare registrazioni audio, la maggior parte delle quali sarebbe probabilmente stata soggetta alla protezione del *copyright*. Lo scopo della crittografia, inclusa nel progetto di Aimster, era, ovviamente, quello di evitare il ricorrere di una "*actual knowledge*" del comportamento illecito degli utenti, elemento che aveva condotto i giudici del Nono Circuito a condannare Napster.

Aimster forse non era consapevole del punto di partenza del ragionamento della Corte. Essa, infatti, parte dal presupposto che "*adolescenti e giovani adulti che hanno accesso a Internet amano scambiare file contenenti musica popolare. Se la musica è protetta da copyright, tale scambio, che implica la creazione e la trasmissione di una copia digitale della musica, viola il copyright. Gli "swappers", che ignorano o più comunemente disdegnano il diritto d'autore e, in ogni caso, sottostimano la possibilità di essere citati in giudizio o perseguiti per violazione del diritto d'autore, sono i trasgressori diretti. Ma le aziende che facilitano la loro violazione, anche se non sono esse stesse trasgressori perché non stanno materialmente compiendo copie della musica, possono essere responsabili nei confronti dei proprietari del copyright in quanto "contributory infringers"*. […]*Riconoscendo l'impraticabilità o l'inutilità di un titolare del diritto d'autore di citare in giudizio una moltitudine di singoli trasgressori, la legge consente invece a un detentore del copyright di citare in giudizio direttamente il provider come aiutante e complice*"[236]. Così impostato il punto di partenza, il bilanciamento già propendeva per *l'enforcement* del *copyright*.

La Corte del settimo circuito analizzava il modo di funzionare del sistema di *file-sharing* ideato da Aimster. In particolare, essa notava che tutte le comunicazioni fra gli utenti di Aimster fossero crittografate dal mittente e venissero decifrate dal destinatario utilizzando lo stesso pacchetto software fornito da Aimster. Gli utenti, quindi, elencavano sui loro computer i file che erano disposti a condividere. Digitando il nome del file che un utente desiderava ottenere nel campo "Cerca", il server di Aimster ricercava fra i file disposti in possibile condivisione e se trova il file che era stato richiesto indicava al computer in cui era ospitato di trasmettere il file al destinatario via Internet affinché lo scaricasse sul suo terminale.

Ma poiché le copie dei brani risiedevano sui computer degli utenti e non sul server di Aimster, esso non poteva essere considerato un trasgressore diretto dei diritti d'autore su quei brani. Questo, tuttavia, non riuscì a salvare Aimster dalle censure in termini di "*contributory liability*", essendo state altresì rigettate dalla Corte le difese in tema di *fair use* nonché i retorici richiami alla decisione Betamax ed ai "*substantial non infringing uses*".

La decisione della Corte si basava sul seguente ragionamento[237]: la "*willful blindness*" è conoscenza, nella legge sul diritto d'autore. "*Colui che, sapendo o sospettando fortemente di essere*

---

[236] Nel testo originale della Corte: "*Teenagers and young adults who have access to the Internet like to swap computer files containing popular music. If the music is copyrighted, such swapping, which involves making and transmitting a digital copy of the music, infringes copyright. The swappers, who are ignorant or more commonly disdainful of copyright and in any event discount the likelihood of being sued or prosecuted for copyright infringement, are the direct infringers. But firms that facilitate their infringement, even if they are not themselves infringers because they are not making copies of the music that is shared, may be liable to the copyright owners as contributory infringers. Recognizing the impracticability or futility of a copyright owner's suing a multitude of individual infringers ("chasing individual consumers is time consuming and is a teaspoon solution to an ocean problem," Randal C. Picker, "Copyright as Entry Policy: The Case of Digital Distribution," 47 Antitrust Bull. 423, 442 (2002)) the law allows a copyright holder to sue a contributor to the infringement instead, in effect as an aider and abettor. Another analogy is to the tort of intentional interference with contract, that is, inducing a breach of contract. See, e.g., Sufrin v. Hosier, 128 F.3d 594, 597 (7th Cir. 1997)"*

[237] Nel testo della Corte: "*We also reject Aimster's argument that because the Court said in Sony that mere "constructive knowledge" of infringing uses is not enough for contributory infringement, 464 U.S. at 439, 104 S.Ct. 774, and the encryption feature of Aimster's service prevented Deep from knowing what songs were being copied by the users of his system, he lacked the knowledge of infringing uses that liability for contributory infringement requires. Willful blindness is knowledge, in copyright law (where indeed it may be enough that the defendant should have known of the direct infringement, Casella v. Morris, 820 F.2d*

coinvolto in affari loschi, si adopera per assicurarsi di non acquisire una conoscenza completa o esatta della natura e della portata di tali rapporti è ritenuto avere un intento criminale perché uno sforzo deliberato per evitare la conoscenza colpevole è tutto ciò che la legge richiede per stabilire uno stato mentale colpevole. Non è sfuggita alla responsabilità con questa manovra; Aimster non può invocare quindi il software di crittografia per far finta di non sapere ciò che sicuramente sospetta fortemente ossia: che gli utenti del suo servizio - forse tutti gli utenti del suo servizio - violano il copyright".

Quindi, un prestatore di servizi che rientri nelle caratteristiche di "*contributor*" non ottiene alcun tipo di immunità utilizzando la crittografia, onde evitare la conoscenza delle finalità illecite per le quali il servizio viene utilizzato. Il risultato sembra quasi paradossale: la presenza di tecnologie che migliorano la privacy, come la crittografia, richiede nei fatti una maggiore sorveglianza sul web per sfuggire alle censure di responsabilità secondaria. In altre parole, l'uso di tecnologie che migliorano la tutela della privacy richiede l'adozione di pratiche di monitoraggio e di sorveglianza che necessariamente vanno ad infirmarla e ad eroderne la tutela.

7.1.4. CASO GROKSTER

Ultimo caso di questa trilogia che abbiamo impostato a partire dal caso Napster è il caso Grokster[238].

Grokster era una società che distribuiva un software che avrebbe consentito agli utenti di scambiarsi digitalmente file multimediali attraverso una *rete peer-to-peer*, non dissimile, come concetto, da quelle già incontrate nei casi Aimster e Napster. Differiva tuttavia dai suoi predecessori, in qualche modo, nella struttura. Nello specifico, venne decentralizzata la tecnologia del proprio software (*FastTrack*) in modo che un utente interessato allo scambio di file avrebbe potuto localizzare, con l'ausilio di un *server* centrale, uno dell'insieme di computer collegati a Internet che fungevano da cosiddetti supernodi, coordinanti le richieste

---

362, 365 (11th Cir. 1987); 2 Goldstein, supra, § 6.1, p. 6:6), as it is in the law generally. See, e.g., Louis Vuitton S.A. v. Lee, 875 F.2d 584, 590 (7th Cir. 1989) (contributory trademark infringement). One who, knowing or strongly suspecting that he is involved in shady dealings, takes steps to make sure that he does not acquire full or exact knowledge of the nature and extent of those dealings is held to have a criminal intent, United States v. Giovannetti, 919 F.2d 1223, 1228 (7th Cir. 1990), because a deliberate effort to avoid guilty knowledge is all that the law requires to establish a guilty state of mind. United States v. Josefik, 753 F.2d 585, 589 (7th Cir. 1985); AMPAT/Midwest, Inc. v. Illinois Tool Works Inc., 896 F.2d 1035, 1042 (7th Cir. 1990) ("to know, and to want not to know because one suspects, may be, if not the same state of mind, the same degree of fault)." In United States v. Diaz, 864 F.2d 544, 550 (7th Cir. 1988), the defendant, a drug trafficker, sought "to insulate himself from the actual drug transaction so that he could deny knowledge of it," which he did sometimes by absenting himself from the scene of the actual delivery and sometimes by pretending to be fussing under the hood of his car. He did not escape liability by this maneuver; no more can Deep by using encryption software to prevent himself from learning what surely he strongly suspects to be the case: that the users of his service — maybe all the users of his service — are copyright infringers".

[238]MGM Studios, Inc v. Grokster, Ltd, 259 F. Supp. 2d 1029 (C.D. Cal. 2003) liberamente consultabile presso: «https://law.justia.com/cases/federal/district-courts/FSupp2/259/1029/2362925/» (Ultimo accesso: 10 maggio 2022); MGM Studios, Inc v. Grokster, Ltd 380 F.3d 1154 (9th Circuit, 2004), liberamente accessibile presso: «https://casetext.com/case/metro-goldwyn-mayer-v-grokster-ltd» (Ultimo accesso: 10 maggio 2022); MGM Studios, Inc v. Grokster, Ltd 545 U.S. 913 (2005), liberamente accessibile presso: «https://supreme.justia.com/cases/federal/us/545/913/» (Ultimo accesso: 10 maggio 2022); per una approfondita analisi del caso si rimanda a F. GIOVANELLA, *Copyright and Information Privacy. Conflicting Rights in Balance*,cit., 213 e ss. ; D. R. LEVIN, *The Future of Copyright Infringement: Metro-Goldwyn-Mayer Studios, Inc. v. Grokster Ltd*, in *John's Journal Legal Comment* 271, 2006, liberamente accessibile presso: «https://scholarship.law.stjohns.edu/cgi/viewcontent.cgi?article=1083&context=jcred» (Ultimo accesso: 10 maggio 2022); R. AXBERG, *File-Sharing Tools and Copyright Law: A Study of In re Aimster Copyright Litigation and MGM Studios, Inc. v. Grokster, Ltd*, cit.

di ricerca tra *cluster* di utenti. Una volta inserito nel sistema, l'utente avrebbe potuto inviare una richiesta per un determinato file multimediale, come una registrazione audio. Se una copia della registrazione richiesta si fosse trovata su uno dei computer degli utenti collegati, sarebbe stata inviata alla parte richiedente senza ulteriore coinvolgimento di Grokster. In parte a causa della struttura, il sistema è stato utilizzato per scopi non illeciti, ma allo stesso tempo per lo scambio illegale di registrazioni.

Non sorprende dunque che, anche in questo caso, l'azione volta a colpire le piattaforme provenne dai titolari dei diritti d'autore, minacciati nei loro monopoli di sfruttamento delle opere dell'ingegno dalla struttura del *file-sharing*. Alcuni colossi dell'industria musicale e cinematografica quindi citarono in giudizio Grokster per "*contributory*" e per "*vicarious liability*". Insomma, una storia che si ripete.

Il tribunale distrettuale degli Stati Uniti per il distretto centrale della California aveva inizialmente respinto il caso nel 2003, citando la decisione del caso Betamax. In sede di gravame, la Corte d'Appello del Nono Circuito, aveva confermato la decisione del tribunale di grado inferiore dopo aver riconosciuto che il software *peer-to-peer* poteva avere usi legittimi e legali. Infatti, non poteva ritenersi applicabile la *"rule of law"* del caso Napster in quanto, mentre quest'ultimo operava con un sistema centralizzato, come visto, Grokster operava invece con un sistema decentralizzato e come tale mai direttamente implicato in alcuna attività di *file-sharing*. L'esito del giudizio sommario svoltosi in primo grado veniva dunque confermato anche in appello, rigettando le pretese di parte attrice, che, di conseguenza, adiva la Corte Suprema.

Nonostante il successo ottenuto presso le Corti di merito, la difesa di Grokster non resse in sede di legittimità in quanto la Suprema Corte si convinse della effettiva conoscenza, da parte del convenuto, dell'uso che gli utenti facevano del proprio sistema di *file-sharing*.

La Corte ha infatti ritenuto che *provider* come Grokster potessero essere responsabili per "*contributory infringement*", indipendentemente dagli usi legittimi del software, sulla base dell'evidenza che il software era stato distribuito con l'obiettivo principale, se non esclusivo, di promuoverne l'uso in violazione del diritto d'autore. Oltre alla conoscenza delle numerose violazioni[239], Grokster aveva espressamente pubblicizzato agli utenti la capacità del software di copiare opere ed aveva espresso chiaramente l'intenzione di attirare gli ex utenti di Napster[240].

---

[239] La Corte nota come "*Discovery revealed that billions of files are shared across peer-to-peer networks each month. Respondents are aware that users employ their software primarily to download copyrighted files, although the decentralized networks do not reveal which files are copied, and when. Respondents have sometimes learned about the infringement directly when users have e-mailed questions regarding copyrighted works, and respondents have replied with guidance. Respondents are not merely passive recipients of information about infringement. The record is replete with evidence that when they began to distribute their free software, each of them clearly voiced the objective that recipients use the software to download copyrighted works and took active steps to encourage infringement. After the notorious file-sharing service, Napster, was sued by copyright holders for facilitating copyright infringement, both respondents promoted and marketed themselves as Napster alternatives. They receive no revenue from users, but, instead, generate income by selling advertising space, then streaming the advertising to their users. As the number of users increases, advertising opportunities are worth more. There is no evidence that either respondent made an effort to filter copyrighted material from users' downloads or otherwise to impede the sharing of copyrighted files".*

[240] La Corte infatti nota che "*The evidence that Grokster sought to capture the market of former Napster users is sparser but revealing, for Grokster launched its own OpenNap system called Swaptor and inserted digital codes into its Web site so that computer users using Web search engines to look for "Napster" or "[f]ree file sharing" would be directed to the Grokster Web site, where they could download the Grokster software. Id., at 992-993. And Grokster's name is an apparent derivative of Napster*".

Per questi motivi, dunque, Grokster è stata condannata in quanto, nelle parole del Justice Souter [241], "*inducing*" o "*encouraging*" costituiscono una forma di "*contributory infringement*". Infatti, la Corte nota come tre caratteristiche siano particolarmente degne di nota. In primo luogo, Grokster ha mirato a soddisfare una nota fonte di domanda di mercato che comprendeva gli ex utenti di Napster. In secondo luogo, la società non aveva tentato di sviluppare strumenti di filtraggio o altri meccanismi per ridurre l'attività illecita utilizzando il proprio software. Sebbene il Nono Circuito abbia considerato tale mancanza come irrilevante per l'inesistenza, nel sistema statunitense, di un obbligo di monitorare l'attività degli utenti, questa prova sottolinea la facilitazione intenzionale della violazione dei loro utenti. In terzo luogo, Grokster guadagnava vendendo spazi pubblicitari, quindi indirizzando gli annunci sugli schermi dei computer che utilizzavano tale software.

Con questi casi alla mano si possono allora sciogliere i nodi che celano la rilevanza esemplare di questa nota giurisprudenza. Nell'attacco sferrato ai *Service Provider* dai titolari dei diritti d'autore si comprende come nel sistema americano, superando le iniziali statuizioni del Caso Betamax, si arrivi ad affermare una tutela molto forte del diritto d'autore, con le Corti che danno seguito alle richieste di *enforcement* del diritto d'autore.

Analizzando il contesto americano, infatti, quello che emerge non solo dalla legislazione ma anche dalla giurisprudenza è una grande protezione affidata *all'enforcement* del *copyright* che quindi conferisce una vittoria sostanzialmente facile ai titolari del diritto d'autore. Chiaramente, l'elemento essenziale, capace di mutare la prospettiva, potrebbe essere solo quello del bilanciamento con la tutela della privacy. Infatti, in tutte le sentenze così esaminate, mancava un elemento fondamentale ai fini di questo elaborato, ossia il coinvolgimento degli utenti, capace di cambiare la prospettiva delle Corti. Questi casi aprono però ad una seconda stagione di iniziative volte a tutelare il *copyright*, tuttavia, questa volta, intese a colpire gli utenti. Eppure, anticipando quando vedremo nel prossimo paragrafo, le richieste di protezione dei dati personali non vennero davvero ascoltate dalle Corti.

Il 7 novembre 2005 Grokster ha annunciato che non avrebbe più offerto il suo servizio di condivisione di file *peer-to-peer*. L'avviso sul sito Web[242] afferma ancora oggi: "*La Corte Suprema degli Stati Uniti ha confermato all'unanimità che l'utilizzo di questo servizio per lo scambio di materiale protetto da copyright è illegale. La copia di filmati e file musicali protetti da copyright, utilizzando servizi peer-to-peer non autorizzati, è illegale ed è perseguita dai proprietari dei diritti d'autore*". Tuttavia, è il monito finale che prelude al problema di cui si occuperà il prossimo paragrafo: "*Il tuo indirizzo IP è […] ed è stato registrato. Non pensare di non poter essere scoperto. Non sei anonimo*".

7.2. Si inizia a cercare di colpire gli utenti finali

Il punto focale della nostra analisi consegue strettamente ai casi appena analizzati: i titolari dei diritti d'autore comprendono che colpire i *Service Provider* non è più conveniente proprio a causa della struttura decentralizzata dei sistemi di *file-sharing*. Nonostante la Corte

[241] Egli infatti afferma che "*One infringes contributorily by intentionally inducing or encouraging direct infringement and infringes vicariously by profiting from direct infringement while declining to exercise the right to stop or limit it. Although "[t]he Copyright Act does not expressly render anyone liable for [another's] infringement," Sony, 464 U. S., at 434, these secondary liability doctrines emerged from common law principles and are well established in the law, e.g., id., at 486. Pp. 10-13.*"

[242] Sul sito si legge infatti: "*The United States Supreme Court unanimously confirmed that using this service to trade copyrighted material is illegal. Copying copyrighted motion picture and music files using unauthorized peer-to-peer services is illegal and is prosecuted by copyright owners. There are legal services for downloading music and movies. This service is not one of them*". "*YOUR IP ADDRESS IS […] AND HAS BEEN LOGGED. Don't think you can't get caught. You are not anonymous.*" Per visualizzare la scritta procedere sul sito: «http://www.grokster.com» (Ultimo accesso: 10 maggio 2022).

Suprema, nel caso Grokster, abbia dato la vittoria ai *copyright holders*, è bene ricordare come invece per ben due volte nei gradi di merito i ricorrenti non abbiano ottenuto ragione delle loro aspettative. Con la chiusura di questa fase giurisprudenziale se ne aprì una nuova: quella volta a colpire gli utenti finali.

Ecco che le lunghe premesse sin qui tracciate si fondono in un delicato bilanciamento fra *l'enforcement* del diritto d'autore e la tutela della riservatezza, della privacy in senso lato, della tutela dei dati personali degli utenti. Sono infatti gli utenti ad essere tacciati come pirati. Quasi un secolo dopo il furgone della BBC capace di triangolare la posizione degli ascoltatori pirata, la storia si ripete con le campagne delle RIAA e l'identificazione degli indirizzi IP.

Dal 2003 la RIAA iniziò a perseguire legalmente gli utenti finali[243] in riguardo ai quali aveva sospetto che compissero violazioni del *copyright* scambiando file illecitamente sulle reti *peer-to-peer*. Con ciò si aprono le porte a quella quarta strategia che avevamo enucleato e che accompagna questo elaborato ossia, come ricorda Roberto Caso,[244] quelle *"Azioni giudiziarie e stragiudiziarie volte a colpire gli utenti delle reti P2P*".

L'iniziale strategia della RIAA consisteva nel collegarsi alla rete in un sistema di *file-sharing peer-to-peer*, cercare nei repertori del sistema le registrazioni detenute dal titolare dei diritti d'autore e quindi registrare l'IP di coloro che risultavano dalla ricerca. Così impostato il problema, quantomeno ad una sensibilità europea, è evidente che la questione controversa fosse quella del monitoraggio massiccio e della sorveglianza degli utenti sul web per ragioni di *enforcement* dei monopoli economici dei titolari dei diritti d'autore. E tornano tutte le direttive che sin dalle prime pagine ci hanno accompagnato, l'affidarsi alla tecnologia, la dimensione privatistica dell'autotutela, l'alleanza con il mondo degli affari.

Chiaramente, come già notato, non sarebbe stato possibile per i *copyright holders* associare l'indirizzo IP dell'utente alla sua reale identità, necessaria invece per citarlo in giudizio, con conseguente bisogno della collaborazione dei *Service Provider*. La legislazione, come visto, uno strumento lo forniva, ossia il *subpoena* della Section §512 DMCA.

7.2.1. Strumento del §512 Subpoena: Il CASO VERIZON

Una prima strategia, quindi, si basava sulla collaborazione con i *Service Provider*. La RIAA in questi casi avrebbe proceduto a fare richiesta della emissione di un *subpoena* grazie alla Section §512 DMCA, ottenendo dai *provider* i nomi e i dati personali degli utenti. Di conseguenza, avrebbe azionato gli strumenti offerti dalla normativa in tema di *copyright* per colpire l'utente con pesanti richieste risarcitorie[245].

---

[243] Riferimenti alla strategia concretamente adottata dalla RIAA sono rinvenibili presso R. BACKERMAN, *How the RIAA Litigation Process Work,* in *recordindustryvspeople.blogspot.it*, 11 gennaio 2008, liberamente accessibile presso: «http://recordingindustryvspeople.blogspot.com/2007/01/how-riaa-litigation-process-works.html» (Ultimo accesso: 10 maggio 2022).

[244] R. CASO, *Il conflitto tra copyright e privacy nelle reti Peer to Peer: il caso Peppermint – Profili di diritto comparato*, cit. 3 e ss.

[245] Ricordiamo infatti che grazie al "*Digital Theft Deterrence and Copyright Damages Improvement Act*" del 1999 la gamma dei danni legali ammissibili nelle azioni civili per violazione del *copyright* passa da essere stabilita con un minimo di $ 500 per opera ed un massimo di $ 20.000 o $ 100.000 per opera, ad un minimo di $ 750 ed un massimo di $ 30.000 e $ 150.000, con un conseguente aumento del 50%. Il testo dell'atto è liberamente accessibile presso: «https://www.congress.gov/bill/106th-congress/house-bill/3456/text» (Ultimo accesso: 10 maggio 2022).

Mentre alcuni *provider* diedero seguito ai *subpoena* loro emessi, altri decisero invece di opporsi e fra questi ultimi, il primo e più importante esempio fu quello di Verizon[246].

La Recording Industry Association of America si era infatti mossa per far rispettare un *subpoena* notificato a Verizon Internet Services ai sensi del Digital Millennium Copyright Act del 1998, 17 U.S.C. § 512. Per conto dei proprietari dei diritti d'autore, la RIAA tentava di rinvenire l'identità degli utenti anonimi del servizio di Verizon che si presumeva avesse violato i diritti d'autore rispetto a più di 600 canzoni scaricate da Internet in un solo giorno. Chiaramente, la RIAA poteva discernere l'indirizzo del protocollo Internet, ma non l'identità, del presunto trasgressore, per la cui ostensione si rendeva invece necessaria la collaborazione dei *Service Provider*. Verizon sosteneva che la citazione si riferisse al materiale trasmesso sulla rete di Verizon, non memorizzato su di essa, e quindi non rientrava nell'ambito del potere di citazione autorizzato nel DMCA[247]".

La Corte distrettuale non accolse le difese di Verizon e la RIAA ottenne un dispositivo che obbligava il *provider* a fornire le identità degli utenti. La Corte giunse ad affermare che "*sulla base del linguaggio e della struttura dello statuto, come confermato dallo scopo e dalla storia della normativa, il potere del subpoena ex 17 U.S.C. § 512(h) si applica a tutti i fornitori di servizi Internet nell'ambito del DMCA, non solo a quei provider che archiviano informazioni su un sistema o una rete sotto la direzione di un utente*". Pertanto, la Corte accolse la mozione della RIAA per l'esecuzione ed ordinò a Verizon di conformarsi al *subpoena* adeguatamente emesso e supportato dalla RIAA per cercare l'identità del presunto contraffattore[248].

Nel giudizio di primo grado, Verizon sollevava anche alcuni possibili dubbi di costituzionalità del *subpoena* del DMCA in particolare con riferimento all'articolo III della Costituzione. Verizon, tuttavia, dedicò solo due frasi e una nota a piè di pagina alle questioni costituzionali, sostenendo che la sezione riguardante il potere di *subpoena*, se interpretata in modo ampio, sollevava questioni sostanziali sull'articolo III (potere giudiziario) e sul primo

---

[246] In re Verizon Internet Services, Inc. 240 F. Supp. 2d 24 (D.D.C. 2003), liberamente accessibile presso: «https://casetext.com/case/in-re-verizon-Internet-services-inc-5» (Ultimo accesso: 10 maggio 2022); RIAA v. Verizon Internet Services, 351 F.3d 1229 (DC Cir. 2003), liberamente accessibile presso: «https://law.justia.com/cases/federal/appellate-courts/F3/351/1229/525976/» (Ultimo accesso: 10 maggio 2022); In Re Verizon Internet Services, 257 F.Supp 2d 244 (D.D.C. 2003) (In Re Verizon 2), liberamente accessibile presso:«https://casetext.com/case/in-re-verizon-Internet-services-inc-4» (Ultimo accesso: 10 maggio 2022). Per una analisi dottrinale del caso nonché per un commento, si veda: D. GROSKI, *The future of the Digital Millennium Copyright Act (DMCA) Subpoena Power on the Internet in light of the Verizon Cases*, in *Review of Litigation* 149, 2005; T. A. DUTCHER, *A Discussion of the Mechanics of the DMCA Safe Harbor and Subpoena Power, as applied in RIAA v. Verizon Internet Services,* in *Santa Chiara Computer & High Tech Law Journal* 493, 2005, liberamente accessibile presso: «https://digitalcommons.law.scu.edu/chtlj/vol21/iss2/6/» (Ultimo accesso: 10 maggio 2022).

[247] Traduzione libera del testo proveniente da In re Verizon Internet Services, Inc. 240 F. Supp. 2d 24 (D.D.C. 2003), cit., qui riportato nel testo originale: "*The Recording Industry Association of America ("RIAA") has moved to enforce a subpoena served on Verizon Internet Services ("Verizon") under the Digital Millennium Copyright Act of 1998 ("DMCA" or "Act"), 17 U.S.C. § 512. On behalf of copyright owners, RIAA seeks the identity of an anonymous user of Verizon's service who is alleged to have infringed copyrights with respect to more than 600 songs downloaded from the Internet in a single day. The copyright owners (and thus RIAA) can discern the Internet Protocol address, but not the identity, of the alleged infringer — only the Service Provider can identify the user. Verizon argues that the subpoena relates to material transmitted over Verizon's network, not stored on it, and thus falls outside the scope of the subpoena power authorized in the DMCA.*"

[248] Traduzione libera del testo proveniente da In re Verizon Internet Services, Inc. 240 F. Supp. 2d 24 (D.D.C. 2003), cit., qui riportato nel testo originale: "*Based on the language and structure of the statute, as confirmed by the purpose and history of the legislation, the Court concludes that the subpoena power in 17 U.S.C. § 512(h) applies to all Internet Service Providers within the scope of the DMCA, not just to those Service Providers storing information on a system or network at the direction of a user. Therefore, the Court grants RIAA's motion to enforce, and orders Verizon to comply with the properly issued and supported subpoena from RIAA seeking the identity of the alleged infringer".*

emendamento. Tuttavia, in quanto non sollevata direttamente, la questione di costituzionalità non venne presa in considerazione nella decisione della Corte distrettuale. In particolare, la Corte statuisce, brevemente, che "*è anche chiaro che il Primo Emendamento non tutela la violazione del diritto d'autore. Inoltre, la Corte Suprema ha recentemente confermato in Eldred v. Ashcroft*[249] *che la vicinanza della clausola sul diritto d'autore e del primo emendamento è espressione del punto di vista dei padri fondatori, ossia che i monopoli limitati del diritto d'autore sono compatibili con i principi della libertà di parola e che il diritto d'autore serve a promuovere gli ideali del primo emendamento inteso come the engine of free expression",* il motore della libertà di espressione. [250]

Per la Corte, infatti, questo non è un caso in cui l'anonimato di un utente di Internet merita di beneficiare della tutela della libertà di parola e della protezione della privacy. La Corte distrettuale nota sicuramente come la Suprema Corte avesse riconosciuto che, in alcune situazioni, il Primo Emendamento tutelasse l'anonimato[251] o come alcuni tribunali federali avessero specificamente riconosciuto che il Primo Emendamento potesse proteggere l'anonimato di un individuo su Internet[252]. Tuttavia, nota come né Verizon né alcun *amicus curiae* avesse osato suggerire che il download anonimo di più di 600 canzoni da Internet senza autorizzazione fosse un'espressione protetta legalmente ai sensi del Primo Emendamento. Citando la Corte, essa afferma, a tal proposito, che il caso di Verizon non è assimilabile al caso in cui un utente utilizzi Internet in modo anonimo per distribuire discorsi di Lenin, brani biblici, materiale didattico o critiche al governo, situazioni in cui si potrebbe sostenere con maggior plausibilità una protezione del primo emendamento. Come ha spiegato la Corte Suprema[253], lo scopo della protezione dell'espressione anonima sarebbe quella di salvaguardare coloro che sostengono le proprie cause in modo anonimo *("who support causes anonymously"*) e coloro che temono ritorsioni economiche o ufficiali, l'ostracismo sociale o un'intrusione indesiderata nella privacy *("fear economic or official retaliation," "social ostracism," or an "unwanted intrusion into privacy*")[254].

In sede di gravame avverso la statuizione della Corte distrettale, la Corte d'appello modificò il proprio orientamento, seppur senza affrontare ulteriormente ogni questione riguardante il primo emendamento. La Corte, in particolare, ritenne che il § 512(h) si applicasse a un ISP il quale avesse archiviato materiale illecito sui suoi server e non si

---

[249] Eldred v. Ashcroft, 537 U.S. 186 (2003), liberamente accessibile presso: «https://supreme.justia.com/cases/federal/us/537/186/» (Ultimo accesso: 10 maggio 2022).

[250] Traduzione libera del testo proveniente da In re Verizon Internet Services, Inc. 240 F. Supp. 2d 24 (D.D.C. 2003), cit., qui riportato nel testo originale: "*It is also clear that the First Amendment does not protect copyright infringement. See Harper Row, Publs., Inc. v. Nation Enters., 471 U.S. 539, 555-60 (1985); Zacchini v. Scripps-Howard, 433 U.S. 562, 574-78 (1977). Moreover, the Supreme Court recently confirmed in Eldred v. Ashcroft that the proximity of the Copyright Clause and the First Amendment demonstrates "the Framers' view [that] copyright's limited monopolies are compatible with free speech principles," and that copyright serves to promote First Amendment ideals as "`the engine of free expression.*'"

[251] Si veda, ad esempio, Watchtower Bible Tract Society of New York, Inc. v. Village of Stratton, 122 S.Ct. 2080, 2090 (2002) Buckley contro Am. Constitutional Law Foun., Inc., 525 US 182 (1999); McIntyre v. Ohio Elections Comm., 514 US 334 (1995).

[252] Si veda, ad esempio, Doe v. 2TheMart.com, Inc., 140 F. Supp.2d at 1097; ACLU v. Johnson, 4 F. Supp.2d 1029, 1033 (DM 1998), aff'd, 194 F.3d 1149 (10th Cir. 1999);

[253] Watchtower Bible Tract Society of New York, Inc. v. Village of Stratton, 122 S.Ct. 2080, 2090 (2002), liberamente accessibile presso «https://supreme.justia.com/cases/federal/us/536/150/» (Ultimo accesso: 10 maggio 2022).

[254] Traduzione libera del testo proveniente da In re Verizon Internet Services, Inc. 240 F. Supp. 2d 24 (D.D.C. 2003), cit., qui riportato nel testo originale: "*To be sure, this is not a case where Verizon's customer is anonymously using the Internet to distribute speeches of Lenin, Biblical passages, educational materials, or criticisms of the government — situations in which assertions of First Amendment rights more plausibly could be made. As the Supreme Court explained in Watchtower Bible Tract Society, the purpose of protecting anonymous expression is to safeguard those "who support causes anonymously" and those who "fear economic or official retaliation," "social ostracism," or an unwanted intrusion into "privacy.*"'"

applicasse invece a un ISP che avesse trasferito meramente materiale illecito da o verso un personal computer di proprietà e utilizzato da un utente[255].

Come ricorda Roberto Caso: "*Le argomentazioni della Corte si arrestano su un piano formale. La 17 U.S.C. § 512 (h) va interpretata nel senso che non è possibile fare ricorso allo strumento del subpoena, quando l'ISP non proceda a memorizzare sui propri computer il materiale in violazione, ma si limiti ad offrire – come nel caso delle reti P2P – la mera connessione ad Internet*[256]".

I giudici di appello altresì affermano di non essere contrari né alla preoccupazione della RIAA riguardo alla diffusa violazione dei diritti d'autore dei suoi membri, né alla necessità di strumenti legali per proteggere tali diritti. Non spetta ai tribunali, tuttavia, riscrivere il DMCA per adattarlo a una nuova e imprevista architettura Internet, non importa quanto tale sviluppo sia stato dannoso per l'industria musicale o minacci di essere per l'industria cinematografica e del software . La difficile situazione dei titolari dei diritti d'autore deve essere affrontata in prima istanza dal Congresso; solo il "*Congresso ha l'autorità costituzionale e la capacità istituzionale di accogliere pienamente le varie permutazioni di interessi concorrenti che sono inevitabilmente implicate da tale nuova tecnologia*".[257]

Avverso la sentenza di secondo grado la RIAA promosse una azione per ottenere un "*writ of certioriari*" e quindi una revisione da parte della Corte Suprema che tuttavia non venne concessa. Verizon aveva vinto. "*La sentenza Verizon ha rappresentato un argine solo per la deriva più estremista della privatizzazione della tutela del copyright: quella appunto che fa leva sul subpoena previsto dal DMCA*"[258].

Altri casi[259] seguirono le sorti di Verizon, con argomentazioni in larga parte riprese dal visto precedente. In un solo caso, tuttavia, venne affrontata la questione connessa alla privacy

---

255 Traduzione libera del testo proveniente da RIAA v. Verizon Internet Services, 351 F.3d 1229 (DC Cir. 2003), liberamente accessibile presso: «https://law.justia.com/cases/federal/appellate-courts/F3/351/1229/525976/» (Ultimo accesso: 10 maggio 2022), nel testo originario: "*We think it clear, therefore, that the cross-references to § 512(c) (3) in §§ 512(b)-(d) demonstrate that § 512(h) applies to an ISP storing infringing material on its servers in any capacity — whether as a temporary cache of a web page created by the ISP per § 512(b), as a web site stored on the ISP's server per § 512(c), or as an information locating tool hosted by the ISP per § 512(d) — and does not apply to an ISP routing infringing material to or from a personal computer owned and used by a subscriber*".

256 R. CASO, *Il conflitto tra copyright e privacy nelle reti Peer to Peer: il caso Peppermint – Profili di diritto comparato,* cit. 3 e ss.

257 Traduzione libera del testo proveniente da RIAA v. Verizon Internet Services, 351 F.3d 1229 (DC Cir. 2003), cit., nel testo originario: "*We are not unsympathetic either to the RIAA's concern regarding the widespread infringement of its members' copyrights, or to the need for legal tools to protect those rights. It is not the province of the courts, however, to rewrite the DMCA in order to make it fit a new and unforeseen Internet architecture, no matter how damaging that development has been to the music industry or threatens being to the motion picture and software industries. The plight of copyright holders must be addressed in the first instance by the Congress; only the "Congress has the constitutional authority and the institutional ability to accommodate fully the varied permutations of competing interests that are inevitably implicated by such new technology*".

258 R. CASO, *Il conflitto tra copyright e privacy nelle reti Peer to Peer: il caso Peppermint – Profili di diritto comparato*, cit. 3 e ss.

259 In Re Charter Communications, Inc., Subpoena Enforcement Matter, 393 F.3d 771, 773, (8th Cir., 2005), liberamente accessibile presso: «https://casetext.com/case/in-re-charter-communications-inc-2» (Ultimo accesso: 10 maggio 2022); In Re Subpoena to University of North Carolina at Chapel Hill, 367 F. Supp. 2d 945 (M.D.N.C., 2005), liberamente accessibile presso: «https://www.casemine.com/judgement/us/5914b65eadd7b04934778bb2» (Ultimo accesso: 10 maggio 2022). Per notazioni dottrinali in merito si veda: F. GIOVANELLA, *Copyright and Information Privacy. Conflicting Rights in Balance,* cit. 227 e ss.; M. R. BOEVE, *Will Internet Service Providers Be Forced to Turn in Their Copyright Infringing Customers? The powerof the Digital Millennium Copyright Act's Subpoena Provision after In Re Charter Communication*, in *Hamline Law Review* 177, 2006, liberamente accessibile presso: «https://heinonline.org/HOL/LandingPage?handle=hein.journals/hamlrv29&div=3&id=&page=» (Ultimo accesso: 10 maggio 2022).

degli utenti per escluderne categoricamente la rilevanza nel caso. In particolare, il riferimento è alla *dissenting opinion* del Justice Murphy nel caso In Re Charter Communications, Inc., Subpoena Enforcement Matter, 393 F.3d 771, 773, (8th Cir., 2005). Secondo i ricorrenti, ai sensi del Cable Act, agli operatori via cavo era vietato divulgare informazioni personali che potessero identificare gli abbonati senza ottenere il loro previo consenso scritto o elettronico e gli operatori sarebbero tenuti ad intraprendere azioni per impedire l'accesso non autorizzato a tali informazioni, cosa che apertamente contraddiceva invece il disposto del §512 *subpoena*.

Tuttavia, il Justice Murphy ricorda come il DMCA affermasse esplicitamente nel § 512 (h) che un fornitore di servizi citato in giudizio dovesse "*divulgare rapidamente [...] le informazioni richieste dalla citazione, nonostante (notwithstanding) qualsiasi altra disposizione di legge*". La disposizione "nonostante" nel § 512 (h) indica che il potere di citazione DMCA ha lo scopo di "*sostituire altri statuti che potrebbero interferire o ostacolare il raggiungimento del suo obiettivo*". Per tale ragione, nella *dissenting opinion*, egli giunge ad affermare che la sezione 551 (c) del Cable Act è stata quindi sostituita dalla disposizione del DMCA e un operatore via cavo può conformarsi a una citazione § 512 (a) senza violare lo statuto precedente[260].

Alla fine, Verizon ottenne effettivamente vittoria in appello, ma solo dopo che quasi quattrocento persone erano già state citate in giudizio dalla RIAA e le loro identità pubblicamente esposte ai media[261].

I titolari dei diritti d'autore, dunque, consci della impossibilità di utilizzare uno strumento quale quello della Section §512 DMCA, lungi da desistere dai tentativi di colpire gli utenti[262], si orientarono verso una diversa possibilità, quella prevista dalle regole ordinarie di procedura civile statunitensi regolanti, come visto, i c.d. *"John Doe proceedings*". Tali regole offrono infatti una prospettiva migliore rispetto a quella offerta dal DMCA in quando i titolari di diritti d'autore sarebbero tenuti a intentare una causa contro l'individuo ai sensi dell'articolo 27 delle norme federali di procedura civile. Poiché un titolare del *copyright* è ora tenuto a intentare una causa contro il presunto trasgressore, almeno vi sarà un giudice chiamato a valutare l'opportunità di concedere la citazione e conseguentemente a bilanciare meglio le prerogative della privacy con quelle *dell'enforcement* del diritto d'autore, anche se, come ci apprestiamo a notare, gli esiti non furono confortanti.

7.2.2. Strumento del John Doe: Il caso Arista Records LLC v. Does 1-12 2008

---

[260] Nelle parole della Corte, tratte da In Re Charter Communications, Inc., Subpoena Enforcement Matter, 393 F.3d 771, 773, (8th Cir., 2005), cit., si legge "*The DMCA explicitly states in § 512(h) that a subpoenaed Service Provider must "expeditiously disclose . . . the information required by the subpoena, notwithstanding any other provision of law." § 512(h)(5) (emphasis added). The "notwithstanding" provision in § 512(h) indicates that the DMCA subpoena power is intended to "supersede[ ] other statutes that might interfere with or hinder the attainment of [its] objective." See Campbell v. Minneapolis Pub. Hous. Auth. ex rel City of Minneapolis, 168 F.3d 1069, 1075 (8th Cir. 1999); see also Cisneros v. Alpine Ridge Group, 508 U.S. 10, 18, 113 S.Ct. 1898, 123 L.Ed.2d 572 (1993) ("As we have noted previously in construing statutes, the use of such a `notwithstanding' clause clearly signals the drafter's intention that the provisions of the `notwithstanding' Section override the conflicting provisions of any other Section."). Section 551(c) of the Cable Act is thus superseded by the subpoena provision in the DMCA, and a cable operator can comply with a § 512(a) subpoena without violating the earlier statute*".

[261] In merito si veda K. PHILIPKOSKI, *Battle Not over for File Sharers*, in *WIRED NEWS*, 23 dicembre 2003, liberamente accessibile presso: «https://www.wired.com/2003/12/battle-not-over-for-file-sharers/» (Ultimo accesso: 10 maggio 2022).

[262] Secondo il conteggio tenuto dall'Electronic Frontier Foundation. Si veda il documento intitolato *RIIA v. The People: Five Years Later,* September 30, 2008, disponibile all'URL: «https://www.eff.org/it/wp/riaa-v-people-five-years-later» (Ultimo accesso: 10 maggio 2022).

Visto l'insuccesso conseguito con lo strumento del §512 *subpoena*, la RIAA, e con essa la MPAA (Motion Pictures Association of America), si orientarono verso lo strumento del *John Doe*.

Il caso sicuramente più significativo fu quello originante da Arista Records[263] in cui la casa discografica, insieme ad altre società, promosse un'azione giudiziale sostenendo che i convenuti avessero utilizzato un software di *file-sharing* su reti *peer-to-peer* per scaricare e distribuire al pubblico materiale protetto dal *copyright* appartenente alla società, chiaramente senza autorizzazione.

Come già abbiamo avuto modo di vedere in plurime occasioni, Arista aveva potuto rinvenire, grazie ad una sorveglianza sul web dei sistemi di *file-sharing*, gli indirizzi IP dei soggetti intenti a questa forma di pirateria digitale; tuttavia, non poteva associare il nome dell'utente al suo indirizzo IP senza l'assistenza degli *Internet Service Provider*. In questo specifico caso, gli indirizzi erano forniti dalla California State University of Fresno, che quindi agiva in qualità di *Internet Service Provider*.

Arista presentava la propria azione il 19 settembre 2007, sostenendo che ogni convenuto, senza il permesso o il consenso degli attori, aveva utilizzato, e continuava a utilizzare, un sistema di distribuzione dei media online per scaricare e/o distribuire al pubblico determinate registrazioni. L'atto introduttivo del giudizio dell'attore identificava ciascun convenuto tramite un indirizzo di protocollo Internet (IP) e includeva elenchi corrispondenti delle registrazioni presumibilmente violate da ciascun convenuto.

Contestualmente al deposito di questa azione, sempre il 19 settembre 2007, gli attori presentarono una *ex parte* "*Motion for Leave to Take Immediate Discovery*". Con tale atto, Arista spiegava che, senza la possibilità di procedere a notificare ai *Service Provider* un ordine di immediata "*discovery*", non avrebbe potuto ottenere l'ostensione delle vere identità dei convenuti citati come "*John Doe*". Avverso il *subpoena*, per queste ragioni garantito, venne proposto ricorso.

Dopo aver esaminato la domanda *ex parte*, la Corte distrettuale trovò ragione di accogliere la domanda dei ricorrenti sulla base del fatto che, altrimenti, i convenuti non avrebbero potuto essere identificati senza queste informazioni[264]. Per queste ragioni, la Corte stabilì che dovessero essere rilasciate indicazioni concernenti nomi, indirizzi, i numeri di telefono e gli indirizzi e-mail per ciascun convenuto come identificato dai numeri IP elencati nel reclamo[265]. Tuttavia, nell'interesse della tutela dei diritti alla privacy degli utenti, nonché di eventuali tutele fornite da primo emendamento, per quanto limitate possano essere, il tribunale richiese che si tentasse di contattare gli utenti prima del rilascio delle loro informazioni.

---

[263] Arista Records, LLC v. Does 1-12, 2008 U.S Dist. LEXIS 825448, liberamente accessibile presso: «https://www.casemine.com/judgement/us/591469a7add7b049342dc137» (Ultimo accesso: 10 maggio 2022).

[264] Nelle parole della Corte nel caso Arista Records, LLC v. Does 1-12, 2008 U.S Dist. LEXIS 825448, cit., si legge: "*1) the allegations of copyright infringement in the Complaint, 2) the possibility that the ISP may destroy the information or delete information that could identify the Does identified in the Complaint, 3) the discovery request is narrowly tailored, 4) the request will substantially con- tribute to moving this case forward, and 5) Defendants will not be able to be identified without this information*."

[265] Nelle parole della Corte nel caso Arista Records, LLC v. Does 1-12, 2008 U.S Dist. LEXIS 825448, cit., si legge: "*Plaintiffs may immediately serve Rule 45 Subpoenas on CSUF seeking information sufficient to identify Does 1-12, including the names, current and permanent addresses, telephone numbers, email addresses, and Media Access Control addresses for each Defendant as identified by the IP numbers listed in the Complaint"*

Anche in questo caso non veniva tenuto in debito conto sia che già la raccolta degli indirizzi IP era un trattamento dei dati personali senza il consenso degli utenti, sia i pericoli per la privacy derivanti dalla ostensione dei nominativi connessi agli IP.

Il medesimo anno, le medesime società fecero causa ad altri *John Doe*, utenti della State University of New York at Albany[266]. Il risultato fu il medesimo e nemmeno gli appelli al primo emendamento ebbero successo. La Corte, infatti, giunse ad affermare che "*Sì, esiste un certo livello di protezione del Primo Emendamento offerto alle espressioni anonime da parte di un utente di Internet, ma è piuttosto limitato e […], pertanto, l'aspettativa di privacy è limitata*". La Corte distrettuale ha infatti riscontrato che una persona che si coinvolga nella condivisione P2P non si cimenta in una "*true expression*". Tale espressione, infatti, non è ampia come quella politica, e, quindi, è considerabile come discorso limitato. Come la Corte Suprema ha chiaramente affermato, il Primo Emendamento non è un paradiso sicuro (*safe heaven*) per la violazione del *copyright*[267].

Secondo la Corte, ove vi sia un'accusa di violazione del diritto d'autore, il giudice dovrebbe bilanciare la tensione tra il diritto all'anonimato, quale diritto costituzionale "*minimamente protetto*", e il diritto ad ottenere l'ostensione dell'identità di un possibile pirata. È quindi già chiaro come il bilanciamento in questo caso non avvenga fra pari, esistono due pesi e due misure, e la privacy soccombe al peso importuno *dell'enforcement* del *copyright*.

Nel soppesare i fattori relativi alla necessità di divulgazione rispetto al diritto limitato del Primo Emendamento di un utente di Internet di rimanere anonimo, l'onorevole Dennis Chinn, giudice distrettuale degli Stati Uniti, ha ideato un'analisi a cinque fattori per assistere i tribunali nell'esecuzione di questo approccio di bilanciamento. Questi cinque fattori sono: (1) se i ricorrenti hanno compiuto una dimostrazione concreta di una pretesa *prima facie* di danno perseguibile; (2) la specificità della richiesta di *discovery*; (3) l'assenza di mezzi alternativi per ottenere le informazioni citate in giudizio; (4) una necessità centrale di ottenere le informazioni citate in giudizio per avanzare la richiesta; e (5) l'aspettativa di privacy della parte[268].

---

[266] Arista Records, LLC v. Does 1-16, 2009 U.S. Dist. LEXIS 12159, liberamente accessibile presso: «https://www.anylaw.com/case/arista-records-llc-v-does-1-16/n-d-new-york/02-172009/o5ngRGYBTlTomsSBeJhp» (Ultimo accesso: 10 maggio 2022).

[267] Nelle parole della Corte nel caso Arista Records, LLC v. Does 1-16, 2009 U.S. Dist. LEXIS 12159, cit., si legge "*Yes, there is some level of First Amendment protection afforded anonymous expressions by an Internet user, but it is quite confined, and such expression qualifies as speech only to a finite degree, and, therefore, the expectation of privacy is limited. Id. at 564 (in a thorough, cogent, and highly persuasive analysis of the First Amendment anonymous speech issue, the district court found that a person who engages in P2P sharing is not engaging in true expression, since it is not as broad as political expression, and, thus, is deemed limited speech); Elektra Entm't Group, Inc. v. Does 1-9, 2004 WL 2095581, at *5 (S.D.N.Y. Sept. 8, 2004) (noting that there is only a minimal expectation of privacy in downloading and distributing copyrighted songs without permission). As the Supreme Court has made evidently clear, which Doe Defendants concede, the First Amendment is not a safe haven for copyright infringement.*

[268] Riportando le parole della Corte: *"Because of the modest First Amendment right to remain anonymous when there is an allegation of copyright infringement, the Court must balance the tension between this minimally protected constitutional right and a copyright owner's right to disclosure of the identity of a possible trespasser of its intellectual property interest. In weighing the factors regarding the need for disclosure versus an Internet user's limited First Amendment right to remain anonymous, the Honorable Dennis Chinn, United States District Judge, devised a five-factor analysis to assist courts in performing this balancing approach. Sony Music Entm't Inc. v. Does 1-40, 326 F. Supp. 2d at 565-67. Those five factors are: (1) whether plaintiffs have made a concrete showing of a prima facie claim of actionable harm; (2) the specificity of the discovery request; (3) the absence of alternative means to obtain the subpoenaed information; (4) a central need to obtain the subpoenaed information to advance the claim; and (5) the party's expectation of privacy. Elektra Entm't Group, Inc. v. Does 1-9, 2004 WL 2095581, at *4 (citing, inter alia, Sony Music, 326 F. Supp. 2d at 565-67 & In re Verizon Internet Servs. Inc., 257 F. Supp. at 260-61). This Court is persuaded by the profundity of this methodology and we will apply these factors in our case"*

Proprio in merito al quinto requisito, punto in cui massimamente dovrebbe emergere la potenza della tutela della riservatezza sul web, la Corte afferma che i "*Doe*" in questo caso, non sarebbero nemmeno nella posizione di sostenere di avere un'aspettativa di privacy. Infatti, essi vi hanno implicitamente rinunciato nel momento in cui hanno posto contenuti protetti dal *copyright* sulle reti *peer-to-peer* affinché altri potessero scaricarle illegalmente, calpestando così i diritti di esclusiva economica dei titolari del diritto d'autore[269].

Tuttavia, il ragionamento è criticabile. Non è vero che per il sol fatto di navigare in Internet, con necessaria esposizione del proprio indirizzo IP, un utente rinunci alla propria privacy. Non vi sono elementi concreti per poter desumere un tale concetto, considerando che anche lo scambio su *reti peer-to-peer* è una attività privata, quindi bisognosa di essere protetta dalla riservatezza. Come già la Corte Suprema aveva affermato, il right to privacy "*protects people rather than places*[270]", eppure questa protezione viene costantemente tradita in un bilanciamento che appare retorico e in definitiva falso. Se davvero si fosse data alla riservatezza la posizione costituzionale che merita allora forse il bilanciamento sarebbe stato fra esigenze di pari rilevanza e magari gli esiti differenti. Questo a maggior ragione quando queste attività compiute su Internet "*riguardano la sfera delicatissima del consumo dei prodotti intellettuali, consumo che si pone alla base dell'autonomia e della libertà di pensiero. Il fatto che l'utente consenta ad altro utente di "entrare" nel proprio computer allo scopo specifico del prelievo dei file messi a disposizione non può essere considerato un consenso implicito al monitoraggio ed al tracciamento, mediante potenti tecnologie che permettono l'aggregazione di immense quantità di dati, delle proprie attività*"[271].

In tutti i casi così analizzati vediamo che le Corti statunitensi propendono per una tutela molto forte del diritto d'autore e invece una considerazione molto debole del diritto alla privacy. Sia la legislazione che la giurisprudenza, in sostanza, non solo consentono, ma anzi incoraggiano la violazione costante della riservatezza degli utenti, ammettendo indiscriminatamente attività di sorveglianza degli utenti tramite collezione degli indirizzi IP e garantendo poi l'ostensione dei nominativi e dei dati connessi agli stessi. Tale alleanza con il mondo degli affari e con le tecnologie antipirateria porta ad un potere di sorveglianza smisurato e le Corti faticano a tracciare i contorni di questo potere opponendo ad esso altre istanze quali quelle alla tutela della vita privata o la stessa libertà di pensiero e di consumo di prodotti intellettuali.

Il timore di azioni legali per *contributory infringement* ha portato a regimi di monitoraggio istituzionale da parte di ISP, college ed enti privati.[272] Alcune scuole hanno utilizzato regimi di monitoraggio che impediscono agli studenti di condividere determinati tipi di file; altri intraprendono pratiche di controllo o sorveglianza variamente inquadrabili. Il risultato è una

---

[269] *"They are not in the position of even arguing that they had an expectation of privacy. If the allegation that the Doe Defendants placed copyrighted recording into index files for others to take at will and hereby trampled upon the exclusive owner's copyright domain are true, they have forfeited any expectation of privacy they may have had. Even if the information was illegally obtained, this does not necessarily foretell its inadmissibility during a civil trial. Other than an errant citation to a United States Supreme Court case, the Doe Defendants do not proffer any other precedent to uphold this notion that illegally obtained evidence is somehow excluded from a civil trial, and this Court has been unable to unearth any case to confirm this novel concept".*

[270] Katz v. United States, 389 U.S. 347 (1967), liberamente consultabile presso: «https://supreme.justia.com/cases/federal/us/389/347/» (Ultimo accesso: 10 maggio 2022).

[271] R. CASO, *Il conflitto tra copyright e privacy nelle reti Peer to Peer: il caso Peppermint – Profili di diritto comparato,* cit. 1 e ss.

[272] N. REED, *Computers Seized in File-Sharing Raid*, *THE LANTERN OF OHIO* ST. U., May 27, 2003, liberamente accessibile presso: «https://www.thelantern.com/2003/05/computers-seized-in-file-sharing-raid/» (Ultimo accesso: 10 maggio 2022); S. CARLSON, *Tending the Net: Computer-Discipline Offices Offer a Human Touch When Investigating Student Complaints*, *CHRON. OF HIGHER EDUC.*, June 7, 2002, acessibile presso: «https://www.chronicle.com/article/tending-the-net/» (Ultimo accesso: 10 maggio 2022).

rete di monitoraggio prolungata e in gran parte invisibile che tiene traccia di molti degli stessi strumenti coinvolti nell'attuale contenzioso sulla privacy[273].

Una ultima notazione poi si rende essenziale e consente un rapido collegamento con la casistica italiana. La Corte distrettuale, nel caso in commento, afferma, in chiusura, che anche se le informazioni sugli utenti rinvenute tramite questa attività di attivo monitoraggio sono state ottenute illegalmente, ciò non ne predice necessariamente l'inammissibilità in un processo civile. Questo sarà proprio il punto che, grazie ad una diversa legislazione in materia, porterà l'Italia, almeno in un primo momento, a soluzioni diametralmente opposte.

7.3. Casi italiani ed europei

7.3.1. CASO PEPPERMINT

Spostando l'attenzione dal contesto giurisprudenziale statunitense a quello italiano[274] si può notare come il caso principe in questa materia sia il caso Peppermint[275].

La Peppermint Jam Records GmbH era una casa discografica tedesca, detentrice di molti diritti di sfruttamento economico di opere musicali. Nell'autunno del 2006 la Peppermint accusò un gran numero di utenti della rete di essere dei pirati, avendo condiviso illegalmente su sistemi di *file-sharing peer-to-peer* molte registrazioni coperte dal *copyright*. Per fare questo la Peppermint si avvalse dell'assistenza della Logistep[276], una società attiva nell'ambito dello "*scouring*" ossia del rilevamento di queste attività illecite online. Collegandosi la Logistep alle maggiori reti di *file-sharing* procedette a sorvegliare i consumatori ed ottenne numerosi

---

273 M. A. O'ROURKE, *Property Rights and Competition on the Internet: In Search of an Appropriate Analogy*, 16 *BERKELEY TECH. L.J.* 561, 570-71 (2001), liberamente accessibile presso: «https://www.jstor.org/stable/24115693» (Ultimo accesso: 10 maggio 2022); L. QUILTER, *Note, The Continuing Expansion of Cyberspace Trespass to Chattels*, 17 *BERKELEY TECH.* L.J. 421, 423-24 (2002) accessibile presso: « https://www.jstor.org/stable/24120114» (Ultimo accesso: 10 maggio 2022).

274 Per un'attenta analisi del delicato bilanciamento in commento ed un chiaro riferimento alla casistica euro-italiana si faccia riferimento a C. SGANGA, *A Decade of Fair Balance Doctrine, and How to Fix It: Copyright Versus Fundamental Rights Before the CJEU from Promusicae to Funke Medien, Pelham and Spiegel Online,* in *European Intellectual Property Review* (n.11/2019), 2019, liberamente accessibile presso SSRN: «https://ssrn.com/abstract=3414642». (Ultimo accesso: 10 maggio 2022). Si veda inoltre C. SGANGA, *A New Era for EU Copyright Exceptions and Limitations? Judicial Flexibility and Legislative Discretion in the Aftermath of the CDSM Directive and the Trio of the Grand Chamber of the CJEU,* in *ERA Forum*, vol.21, 2020, pp.311-339, liberamente accessibile presso: «https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3804228» (Ultimo accesso: 10 maggio 2022).

275 Tribunale di Roma, ordinanza 18 agosto 2006, in *Riv. Dir. Ind.*, n 4-5/2008, II, 328. Riferimenti dottrinali più diffusi in merito possono essere rinvenuti in R. CASO, *Il conflitto tra copyright e privacy nelle reti Peer to Peer: il caso Peppermint – Profili di diritto comparato*, cit.; M. DE CATA, *Il caso Peppermint. Ulteriori riflessioni anche alla luce del caso Promusicae*, in *Riv. Dir. Ind.* 404, 411 ff.; F. GIOVANELLA, *Copyright and Information Privacy. Conflicting Rights in Balance,* cit., 250 e ss.

276 La Logistep si occupava del rastrellamento sul web degli indirizzi IP appartenenti agli utenti di piattaforme di *file sharing.* R. CASO, in *Il conflitto tra copyright e privacy nelle reti Peer to Peer: il caso Peppermint – Profili di diritto comparato*, cit., ricorda in nota che sul sito della Logistep si poteva leggere: "*by means of its "illogical network" (patent Pending), LOGISTEP fulfils a variety of tasks; which to date were only possible to complete with the use of enormous server capacity. A sole, specially developed server, which handles the entire process, is capable of identifying more than 2 million illegal down- and up-loads per day. The monitoring software used has already been evaluated by several IT experts and has been described as one of the most innovative procedures in the last years. In addition, a publicly sworn IT expert has rendered an expert opinion iro. of LOGISTEP's protocolled data. This certifies that all protocolled information is correct. Through the "illogical network" for IP filters systems, as for example Peer Guardian, LOGISTEP cannot be detected. In full compliance with all relevant laws and regulations we produce a history for each user. IP Jumps, Firewalls or Proxy have no influence on the unambiguous identification of the users. The user identification in all P-2-P protocols is fully accurate".* Le vicende che riguardano la società si chiudono con il Tribunale Federale Svizzero che ha dichiarato illegale la pratica di raccolta indirizzi IP da parte di Logistep AG.

dati relativi alle loro attività sul web ed in particolare gli indirizzi IP degli utenti. Con la collaborazione dei Service Providers, la Peppermint procedette a notificare migliaia di lettere[277] agli utenti accusandoli dell'illecita distribuzione del materiale protetto.

Le lettere vennero inviate in seguito ad una ordinanza proveniente dal Tribunale di Roma, la quale ordinava a Wind Telecomunicazioni s.p.a., in qualità di *Internet Service Provider*, di ostendere i dati associati agli indirizzi IP rilevati dalla Logistep per conto della Peppermint. Chiaramente, come abbiamo visto, l'azione si basava sugli articoli 156 e 156-bis della legge sul diritto d'autore. Come già era stato per la RIAA, anche la Peppermint sapeva che solo gli *Internet Service Providers* potevano conoscere l'identità dell'utente celata dietro l'indirizzo IP e quindi decisero di agire in via analoga a quanto, poco prima, avevano compiuto le controparti statunitensi.

Come abbiamo avuto modo di vedere, l'art. 156-bis consente ai titolari dei diritti d'autore di ottenere che il giudice disponga l'esibizione di documenti, elementi o informazioni detenuti dalla controparte. Può ottenere altresì, che il giudice ordini alla controparte di fornire gli elementi per l'identificazione dei soggetti implicati nella produzione e distribuzione dei prodotti o dei servizi che costituiscono violazione del *copyright*.

Fra le molte difese apprestate da Wind, la più interessante ai nostri fini è sicuramente la contestazione che Peppermint aveva ottenuto dati personali degli utenti in violazione della legislazione sulla privacy. Come al tempo richiesto dall'art. 152 del Codice Privacy, il giudice cautelare procedette a segnalare il ricorso al Garante per la protezione dei dati personali, il quale tuttavia, almeno in questo primo momento, decise di non intervenire.

Il Tribunale di Roma accolse in prima istanza il ricorso della Peppermint. Secondo il Tribunale, infatti, la Logistep aveva condotto un'attività di ricerca degli indirizzi IP non solo in modo affidabile ma anche lecitamente dal momento che un utente che decide di usare un sistema di *file-sharing* implicitamente accetta il fatto che il proprio indirizzo IP possa essere conosciuto da ogni altro utente sulla rete. Un simile ragionamento, come visto, aveva guidato anche le Corti statunitensi nel caso Arista Records, tuttavia, come notato in tal sede, un ragionamento fortemente criticabile non tenendo conto del fatto che accettare che un altro utente conosca un certo dato non equivale ad accettare che chiunque e con qualunque intento possa entrare nel computer di ciascuno.

Altresì, il Tribunale richiamava l'attenzione all'art. 24 co. 1 l. f. (oggi abrogato) del Codice Privacy il quale consentiva il trattamento dei dati personali ove fosse "*necessario ai fini dello svolgimento delle investigazioni difensive di cui alla Legge 7 dicembre 2000, n. 397, o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento, nel rispetto della vigente normativa in materia di segreto aziendale e industriale*". Richiamandosi dunque alla necessità di esercitare un diritto in sede giudiziaria, il Tribunale ritenne non in discussione la possibilità per la Peppermint di ottenere le informazioni richieste. Tuttavia, questa decisione fu solo la prima di una lunga serie in quanto, poco dopo, nel novembre del 2006, la pronuncia venne riformata e l'accesso alle informazioni negato. Avverso quest'ultimo provvedimento la Peppermint decise di impugnare e, con decisione resa da una diversa sezione del Tribunale di Roma[278], il bilanciamento fra l'esigenza di privacy degli utenti e *l'enforcement* del diritto

[277] Scannerizzazioni della lettera inviata agli utenti dallo studio legale rappresentate la Peppermint possono essere rinvenute presso:«https://www.diesis.eu/wp-content/uploads/2007/07/rr1.jpg», «https://www.diesis.eu/wp-content/uploads/2007/07/rr2.jpg», «https://www.diesis.eu/wp-content/uploads/2007/07/rr3.jpg» (Ultimo accesso: 10 maggio 2022).

[278] Tribunale di Roma, ordinanza 9 febbraio 2007, in *Resp. Civ. e prev.*, n. 7-8/2007, 1699

d'autore, ancora una volta, vide vincitore il diritto d'autore, garantendo alla Peppermint l'accesso alla identità degli utenti.

Data la vittoria, in questo primo scontro, cominciarono ad arrivare lettere su lettere agli utenti[279], punto da cui siamo partiti nell'analisi del caso.

Nelle successive vicende legali [280] che coinvolsero la Peppermint non possiamo affermare che essa ebbe la stessa fortuna. Nel 2007 infatti una seconda vicenda legale vide contrapposte la Peppermint e la Techland sp.z.o.o, una società di videogiochi, contro la Wind s.p.a , anche questa volta con un ricorso basato sull'art. 156-bis della legge 633/1941. Tuttavia, diversamente dai precedenti ricorsi, in questo caso il Garante per la protezione dei dati personali decise di intervenire nella lite offrendo le sue osservazioni in materia[281].

In particolare, il Garante denota l'errata interpretazione data dal Tribunale di Roma all'art. 24 Cod. Priv. il quale dovrebbe avere un ambito di applicazione ristretto meramente ai profili penali delle vicende giudiziarie. Interpretare altrimenti, secondo il Garante, sarebbe una violazione del diritto fondamentale alla privacy ed alla segretezza nelle comunicazioni, così come protetto sia dalla Carta Costituzionale che dalla Carta di Nizza. In questo senso, un bilanciamento che comprimesse tale diritto sarebbe possibile solo in vista ed alla luce di un superiore principio, quale l'interesse pubblico garantito dalla legislazione penale.

In aggiunta, il Garante afferma che il trattamento dei dati personali degli utenti perpetrato dalla Peppermint per mezzo della Logistep doveva considerarsi illecito in quanto condotto in aperta violazione del Codice Privacy. L'attività di sorveglianza attuata da queste avrebbe dovuto essere previamente sottoposta ad autorizzazione da parte del Garante stesso, come richiesto dagli articoli 37 e 13 del Codice Privacy[282]. In virtù dell'art. 11[283] del Codice Privacy quindi, i dati personali, trattati in violazione della disciplina rilevante in materia di trattamento dei dati, non potevano essere utilizzati. Questa affermazione rappresenta un punto decisivo per la soluzione del caso perché la statuizione legale dell'inutilizzabilità dei dati era proprio ciò che non veniva affermato nel caso Arista Records, comprendendo quindi sin da ora come il risultato del bilanciamento possa essere diverso nel nostro sistema.

La decisione del Tribunale, chiaramente influenzata dalle statuizioni del Garante, sostenne quindi che dal bilanciamento fra *l'enforcement* del diritto d'autore e la privacy degli

---

[279] Come segnalato, le scannerizzazioni della lettera inviata agli utenti dallo studio legale rappresentate la Peppermint possono essere rinvenute presso:«https://www.diesis.eu/wp-content/uploads/2007/07/rr1.jpg», «https://www.diesis.eu/wp-content/uploads/2007/07/rr2.jpg», «https://www.diesis.eu/wp-content/uploads/2007/07/rr3.jpg» (Ultimo accesso: 10 maggio 2022).

[280] Tribunale di Roma, ord. 16 luglio 2007 *in Dir. Informatica* n 4-5/2007, 828; Tribunale di Roma, ordinanza 14 luglio 2007 in *Rivista Diritto Industriale*, n. 4-5/200, II, 330.

[281] Comunicati stampa 17 luglio 2007 e 13 marzo 2008: *Internet - Caso Peppermint: il Garante privacy si costituisce in giudizio*, liberamente consultabili presso: «https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1406297» (Ultimo accesso: 10 maggio 2022).

[282] Oggi abrogati.

[283] Oggi abrogato, il testo originario così disponeva: "*1. I dati personali oggetto di trattamento sono:*
a) trattati in modo lecito e secondo correttezza;
b) raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi;
c) esatti e, se necessario, aggiornati;
d) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;
e) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.
2. I dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati".

utenti dovesse uscire vincitrice la privacy. I limiti posti all'art. 156-bis direttamente dagli articoli 2 e 15 della Costituzione non potevano essere superati se non sulla base di altrettanti interessi di pari o superiore portata che, nel caso di specie, non potevano essere rinvenuti. La "*disclosure*" dei dati personali non poteva essere garantita.

Non convinte della sconfitta riportata, per una terza volta Peppermint e Techland promossero una azione giudiziaria: questa volta avverso Tiscali s.p.a. Affiancando quest'ultima intervennero altresì il Garante per la protezione dei dati personali, il Codacons e l'Adiconsum.

Sulla scorta della decisione del caso Promusicae, per la cui trattazione si rimanda al paragrafo seguente, il Tribunale ha ritenuto necessario anche in questo caso compiere un attento bilanciamento fra il trattamento dei dati personali e *l'enforcement* del diritto d'autore. La Corte si dimostra coerente con il precedente europeo appena citato il quale affermava che non sussisteva alcuna imposizione per gli Stati membri di prevedere una forma di "*disclosure*" nei procedimenti civili, così confermando l'interpretazione per cui il legislatore italiano avrebbe scelto di limitare la protezione dei dati personali alle sole fattispecie penali.

Da questa costatazione deriva che, secondo il Tribunale, il legislatore aveva già compiuto, in sede di norme generali ed astratte, il corretto bilanciamento fra *enforcement* del diritto d'autore e tutela dei dati personali, affermando che la proprietà intellettuale potesse prevalere sulla privacy solo in ipotesi di fattispecie penali, tutelanti un superiore interesse pubblico, mentre in tutti gli altri casi sarebbe stata la protezione dei dati personali a prevalere. Il Tribunale, alla luce di ciò, respinse le richieste dei ricorrenti.

Appare chiaro che la vittoria ottenuta nel bilanciamento dalla privacy è stato sicuramente, quantomeno in parte, merito del contributo dell'Autorità Garante, intervenuto con provvedimento[284] del 2008 per censurare la condotta della Logistep, della Peppermint e della Techland.

In particolare, il Garante ha affermato che l'attività realizzata da queste ultime violava, segnatamente, il principio di liceità, in ragione del fatto che la raccolta dei dati era stata effettuata in mancanza di una base legale esplicita. Si è ritenuto in secondo luogo violato il principio di finalità, in quanto la registrazione sistematica dei dati degli utenti aveva perseguito scopi diversi da quelli tipici delle reti *peer-to-peer*. Non erano stati, altresì, rispettati i princìpi di buona fede e trasparenza, in quanto la raccolta dei dati era avvenuta senza che gli interessati potessero esserne consapevoli, sia per le circostanze nelle quali la raccolta era avvenuta, sia perché non informati. Infine, è risultato violato il principio di proporzionalità in quanto il diritto alla segretezza delle comunicazioni è risultato limitabile solo nell'ambito di un bilanciamento con un diritto di pari grado e, quindi, allo stato, non per l'esercizio di un'azione civile. Principi, questi, afferma il Garante, tutti "*richiamati sia dalla Convenzione di Strasburgo, sia dalla Direttiva 95/46/Ce e dalla stessa disciplina nazionale di protezione dati*".

Secondo il Garante infatti, "*i trattamenti in esame effettuati in modo massivo e capillare per un periodo di tempo prolungato e nei riguardi di un numero elevato di soggetti, hanno consentito di tenere traccia analitica delle operazioni compiute da innumerevoli, singoli utenti relativamente a specifici contenuti protetti dal diritto d'autore"* e quindi *"per le modalità con le quali la raccolta dei dati è stata svolta, si è configurata un'attività di monitoraggio vietata a soggetti privati dalla Direttiva 2002/58/CE*".

[284] Provvedimento Garante per la protezione dei dati personali 28 febbraio 2008 n. 1495246, nei confronti di Peppermint Jam Records GmbH, Techland sp. z. o.o. e Logistep AG, liberamente accessibile presso: «https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1495246» (Ultimo accesso: 10 maggio 2022).

Per queste ragioni, con tale provvedimento, il Garante si pronuncia nei confronti di Peppermint Jam Records GmbH, Techland sp. z. o.o. e Logistep AG, imponendo loro il divieto dell'ulteriore trattamento dei dati personali relativo a soggetti ritenuti responsabili di aver scambiato file protetti dal diritto d'autore tramite reti peer-to-peer, nonché dispone la cancellazione di quei dati già in possesso da parte dei condannati.

In seguito a questi provvedimenti ed alle statuizioni del Tribunale di Roma, si era compreso che *l'enforcement* del diritto d'autore non poteva oltrepassare, allo stato dell'arte, la protezione conferita agli utenti in tema di privacy.

Brevemente confrontando le risultanze italiane con quelle statunitensi, emerge sin da subito una diversa concezione del diritto alla privacy. Nonostante in ambo gli Stati esso possa essere considerato esistente ed avere una larga copertura costituzionale, come visto, solo in Italia il bilanciamento pare essere avvenuto fra diritti di pari rango. La stessa presenza dell'Autorità Garante dei dati personali in Italia dimostra l'attenzione del nostro ordinamento per la protezione della riservatezza e della vita privata. A differenza delle Corti statunitensi, infatti, quelle italiane si rendono conto della profonda illiceità del trattamento degli indirizzi IP da parte dei titolari del diritto d'autore per mezzo del ricorso all'autotutela. Una simile sorveglianza, come afferma il Garante, non può essere ritenuta lecita e i risultati non possono essere usati. Sebbene anche in Italia la protezione del diritto d'autore sia da considerarsi in largo senso eccessiva sotto molti aspetti, essa è comunque da bilanciare con una legislazione in tema di privacy altrettanto forte che consente di arginare le derive più estreme *all'enforcement* del diritto d'autore. È quindi evidente che in Italia, a differenza degli Stati Uniti, l'estrema difficoltà dell'*enforcement* del diritto d'autore su Internet non consenta di dimenticarsi degli altri diritti costituzionalmente garantiti, raggiungendo risultati di maggior equilibrio.

In questo panorama deve inserirsi anche il diritto comunitario che, pur non smentendo quanto sin qui affermato, dimostra alcune aperture significative, capaci di modificare, nel lungo periodo, il bilanciamento così come delineato dalla giurisprudenza italiana.

7.3.2. CASO PROMUSICAE

In sede europea, la giurisprudenza riguardante il delicato bilanciamento fra l'*enforcement* del diritto d'autore e la tutela dei dati personali è copiosa. La prima sentenza su cui si deve concentrare la nostra analisi è il "caso Promusicae"[285].

La sentenza della Corte di Giustizia ha origine da una domanda di rinvio pregiudiziale[286] presentata nell'ambito di una controversia pendente tra l'associazione senza scopo di lucro Productores de Música de España (Promusicae) e la Telefónica de España SAU in merito al rifiuto, da parte di quest'ultima, di comunicare alla Promusicae una serie di dati personali relativi all'utilizzo di Internet mediante connessioni fornite dalla Telefónica.

Con citazione del 28 novembre 2005, essa ha presentato dinanzi allo Juzgado de lo Mercantil n. 5 de Madrid (Tribunale commerciale n. 5 di Madrid) una domanda di

[285] CGUE 29 gennaio 2008, C-275/06, *Productores de Música de España (Promusicae) v. Telefónica de España SAU*, Grande Sezione, liberamente consultabile presso:«https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:62006CJ0275&from=IT» (Ultimo accesso: 10 maggio 2022). Per notazioni dottrinali in merito si faccia riferimento a R. CASO, *Il conflitto tra diritto d'autore e protezione dei dati personali: appunti dal fronte euro-italiano, n «Diritto dell'Internet», vol. 4, n. 5 IPSOA - Wolters - Kluwer, pp. 466-472, 2008,* disponibile sul sito: «http://eprints.biblio.unitn.it/1637/» (Ultimo accesso: 10 maggio 2022).

[286] All'epoca ex articolo 234 del Trattato della Comunità Europea, corrispondente oggi all'articolo 267 Trattato Sul Funzionamento dell'Unione Europea (TFUE).

accertamento preliminare contro la Telefónica, *Internet Service Provider*. La Promusicae aveva chiesto di ingiungere alla Telefónica di rivelare l'identità e l'indirizzo fisico di talune persone alle quali quest'ultima forniva un servizio di accesso ad Internet ed il cui indirizzo IP, nonché la data e l'ora di connessione, erano noti. Secondo la Promusicae, tali utenti utilizzavano il software denominato "KaZaA", ossia un software di *file-sharing* su reti *peer-to-peer*, attuando violazioni dei diritti d'autore rappresentati dalla Promusicae. Insomma, una storia che si ripete. Non sorprende dunque che, come la RIAA e come Peppermint, anche la Promusicae avesse richiesto che le fossero comunicate le suddette informazioni per poter esercitare azioni civili contro le persone coinvolte.

Con ordinanza 21 dicembre 2005, lo Juzgado de lo Mercantil n. 5 de Madrid ha accolto la domanda di accertamento preliminare presentata dalla Promusicae. La Telefónica ha proposto opposizione avverso tale ordinanza sostenendo che, in conformità alla LSSI[287] (Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico), la trasmissione dei dati richiesti dalla Promusicae fosse autorizzata esclusivamente nell'ambito di un'indagine penale e non nel contesto di un procedimento civile o a titolo di accertamento preliminare relativo ad un siffatto procedimento. Ricordiamo come proprio sulla differenza fra gli interessi sottesi agli accertamenti penali rispetto a quelli civili si era basata, in esito a questa sentenza, la decisione per il caso Peppermint.

In tale contesto, lo Juzgado de lo Mercantil n. 5 de Madrid ha deciso di sospendere il procedimento e rinviare pregiudizialmente una questione alla Corte di Giustizia chiedendo sostanzialmente "*se il diritto comunitario, e in particolare le Direttive 2000/31, 2001/29 e 2004/48, lette anche alla luce degli artt. 17 e 47 della Carta, vadano interpretati nel senso che impongono agli Stati membri di istituire, al fine di garantire l'effettiva tutela del diritto d'autore, l'obbligo di comunicare taluni dati personali nel contesto di un procedimento civile*". Era già chiaro, nel rinvio pregiudiziale, che sebbene sotto altre spoglie, la domanda era potenzialmente un'altra, ossia: in un giudizio civile, prevale *l'enforcement* del diritto d'autore o il diritto alla riservatezza degli utenti online?

La Corte di Giustizia, nel suo ragionamento, parte dalla osservazione preliminare secondo cui le disposizioni del diritto comunitario sono volte a far garantire, dagli Stati membri, l'effettiva tutela della proprietà intellettuale, e in special modo del diritto d'autore, che la Promusicae rivendicava nella causa principale. Tuttavia, il giudice del rinvio partiva dalla premessa che gli obblighi di diritto comunitario, necessari ai fini di tale tutela, possono incontrare, nell'ambito del diritto nazionale, un ostacolo nelle disposizioni dell'art. 12 della LSSI. La Corte di Giustizia tuttavia nota che tale articolo "*è diretto ad attuare le norme di tutela della vita privata altresì imposte dal diritto comunitario in forza delle Direttive 95/46 e 2002/58, l'ultima*

---

[287] Ai sensi dell'art. 12 della legge 11 luglio 2002, n. 34, sui servizi della società dell'informazione e sul commercio elettronico (Ley 34/2002 de servicios de la sociedad de la información y de comercio electrónico; BOE 12 luglio 2002, n. 166, pag. 25388; «LSSI»), intitolato «Obbligo di conservazione dei dati sul traffico relativi alle comunicazioni elettroniche»:

«*1. Gli operatori di rete e di servizi di comunicazione elettronica, i fornitori di accesso a reti di telecomunicazione e i fornitori di servizi di archiviazione di dati dovranno conservare i dati di connessione e di traffico generati dalle comunicazioni effettuate durante la prestazione di un servizio della società dell'informazione per un periodo massimo di dodici mesi, alle condizioni stabilite dal presente articolo e dalla sua normativa di attuazione.*

2. (…) Gli operatori di rete e di servizi di comunicazione elettronica ed i fornitori di servizi cui si riferisce questo articolo non potranno utilizzare i dati conservati per fini diversi da quelli indicati nel seguente paragrafo o da quelli previsti dalla legge e dovranno adottare i provvedimenti idonei ad evitare la perdita o l'alterazione dei dati stessi o l'accesso non autorizzato ai medesimi.

3. I dati verranno conservati al fine del loro utilizzo nell'ambito di un'indagine penale o per la tutela della pubblica sicurezza e della difesa nazionale e saranno posti a disposizione dei giudici o dei tribunali o del pubblico ministero che li richiedano. La trasmissione di tali dati alle forze dell'ordine verrà effettuata nell'osservanza di quanto disposto dalla normativa sulla tutela dei dati personali.(…)».

delle quali riguarda il trattamento dei dati personali nonché la tutela della vita privata nel settore delle comunicazioni elettroniche".

Infatti, la Corte di Giustizia nota come le parti del giudizio a quo non mettevano in discussione che la comunicazione richiesta dalla Promusicae dei nominativi e degli indirizzi degli utenti richiedesse necessariamente la messa a disposizione di dati personali[288].

Anticipando gli esiti giurisprudenziali, notiamo che la Corte giunge quindi alla decisione per cui le disposizioni del diritto comunitario[289] "*non impongono agli Stati membri, in una situazione come quella oggetto della causa principale, di istituire un obbligo di comunicare dati personali per garantire l'effettiva tutela del diritto d'autore nel contesto di un procedimento civile. Tuttavia, il diritto comunitario richiede che i detti Stati, in occasione della trasposizione di tali Direttive, abbiano cura di fondarsi su un'interpretazione delle medesime tale da garantire un giusto equilibrio tra i diversi diritti fondamentali tutelati dall'ordinamento giuridico comunitario. Inoltre, in sede di attuazione delle misure di recepimento delle dette Direttive, le autorità e i giudici degli Stati membri devono non solo interpretare il loro diritto nazionale in modo conforme a tali Direttive, ma anche evitare di fondarsi su un'interpretazione di esse che entri in conflitto con i detti diritti fondamentali o con gli altri principi generali del diritto comunitario, come, ad esempio, il principio di proporzionalità*".

L'elemento principale, ai nostri fini, di interesse per la pronuncia, riguarda tuttavia il ragionamento che ha guidato nel bilanciamento fra la privacy e la tutela dei dati personali e che quindi ha condotto alla decisione della Corte.

Il punto di partenza è lo stesso da cui siamo partiti nella analisi di questo capitolo: entrambi i diritti oggetto della pronuncia e del nostro elaborato sono diritti fondamentali. Secondo la Corte "*il diritto fondamentale di proprietà, di cui fanno parte i diritti di proprietà intellettuale, come il diritto d'autore*[290]*, […] e il diritto fondamentale alla tutela giurisdizionale effettiva costituiscono principi generali del diritto comunitario*". "*Tuttavia, occorre rilevare che nella controversia in relazione alla quale il giudice del rinvio ha sollevato tale questione risulta coinvolto, oltre ai due suddetti diritti, anche un altro diritto fondamentale, vale a dire quello che garantisce la tutela dei dati personali e, quindi, della vita privata*".

La domanda di pronuncia pregiudiziale quindi si risolve nel delicato bilanciamento fra questi diritti. Secondo la Corte i meccanismi che consentono di trovare un giusto equilibrio tra questi diversi diritti e interessi sono contenuti nella stessa Direttiva 2002/58, in quanto essa prevede norme che stabiliscono in quali situazioni ed in qual misura il trattamento dei dati personali è lecito e quali salvaguardie devono essere previste, nonché nelle tre Direttive menzionate dal giudice del rinvio. Infatti, tali meccanismi devono risultare dall'adozione, da

---

288 Ossia, in questo contesto, informazioni concernenti persone fisiche identificate o identificabili, in conformità alla definizione di cui all'art. 2, lett. a), della Direttiva 95/46 (si veda in tal senso, CGUE sentenza 6 novembre 2003, causa C-101/01, Lindqvist, punto 24).

289 In particolare, i testi normativi su cui la decisione si basa sono: la Direttiva del Parlamento europeo e del Consiglio 8 giugno 2000, 2000/31/CE, relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno («Direttiva sul commercio elettronico»), la Direttiva del Parlamento europeo e del Consiglio 22 maggio 2001, 2001/29/CE, sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione, la Direttiva del Parlamento europeo e del Consiglio 29 aprile 2004, 2004/48/CE, sul rispetto dei diritti di proprietà intellettuale, e la Direttiva del Parlamento europeo e del Consiglio 12 luglio 2002, 2002/58/CE, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (Direttiva relativa alla vita privata e alle comunicazioni elettroniche)

290 In tal senso, CGUE 12 settembre 2006, C-479/04, *Laserdisken*, liberamente consultabile presso «https://curia.europa.eu/juris/showPdf.jsf;jsessionid=1CAB14C32344F9E65E7E345FC7A23806?text=&docid=63876&pageIndex=0&doclang=IT&mode=lst&dir=&occ=first&part=1&cid=5175989» (Ultimo accesso: 10 maggio 2022).

parte degli Stati membri, di disposizioni nazionali che garantiscano la trasposizione di queste Direttive e dall'applicazione di queste da parte delle autorità nazionali.

Per quanto riguarda le dette Direttive, le loro disposizioni presentano un carattere relativamente generico, in quanto devono applicarsi a un gran numero di situazioni diverse che possono presentarsi nell'insieme degli Stati membri. Esse contengono quindi logicamente norme che lasciano agli Stati membri il necessario margine di discrezionalità per definire misure di recepimento che possano essere adattate alle diverse situazioni possibili.

La Corte dunque risolve, forse frettolosamente, la questione pregiudiziale affermando che il diritto comunitario richiede che gli Stati, in occasione della trasposizione di queste Direttive, abbiano cura di fondarsi su un'interpretazione delle medesime tale da garantire un giusto equilibrio tra i diversi diritti fondamentali tutelati dall'ordinamento giuridico comunitario. Poi, in sede di attuazione delle misure di trasposizione delle dette Direttive, le autorità e i giudici degli Stati membri devono non solo interpretare il loro diritto nazionale in modo conforme a tali Direttive, ma anche evitare di fondarsi su un'interpretazione di esse che entri in conflitto con i detti diritti fondamentali o con gli altri principi generali del diritto comunitario, come il principio di proporzionalità.

La decisione resa dalla Corte nel Caso Promusicae non può dirsi completamente satisfattoria, non fornendo una vera e propria guida e scaricando, in sostanza, la responsabilità di rinvenire un corretto bilanciamento fra diritti ai giudici nazionali. Non a caso, infatti, venne strettamente seguita da altre richieste di rinvio pregiudiziale[291] vertenti sulle stesse posizioni. Tuttavia, essa può essere intesa come una implicita conferma della necessaria attenta valutazione di tutti gli interessi in gioco, cercando una soluzione che, tenendo in debito conto l'interesse dei titolari dei diritti d'autore, al contempo non dimentichi della tutela dei dati personali, il cui "nucleo essenziale" non può essere compresso fino a essere dimenticato.

7.3.3. CASO BONNIER AUDIO

Un secondo *leading case* nel panorama giurisprudenziale europeo è fornito dal caso "Bonnier Audio"[292].

La Bonnier Audio e gli altri ricorrenti erano case editrici, titolari di diritti esclusivi di riproduzione, di edizione e di messa a disposizione del pubblico di audiolibri. Tali diritti sarebbero stati violati a causa della diffusione al pubblico delle proprie opere senza il loro consenso a mezzo di un server FTP (*file transfer protocol*), che consente la condivisione di file e il trasferimento di dati tra computer connessi a Internet con un sistema di condivisione *peer-*

[291] La Corte riprodusse lo stesso schema di ragionamento anche in altre pronunce fra cui la sentenza CGUE 19 febbraio 2009, C-557/07, *Oberster Gerichtshof, LGS-Gesellschaft zur Wahrnehmung von Leistungschutzrechten GmbH v. Tele2 Telecommunication GmbH,* liberamente accessibile presso: «https://curia.europa.eu/juris/document/document.jsf;jsessionid=62D209BCC7FC7E25F7EDDA663D6D289C?text=&docid=77489&pageIndex=0&doclang=IT&mode=lst&dir=&occ=first&part=1&cid=649194» (Ultimo accesso: 10 maggio 2022). Per una ricostruzione dottrinale delle vicende giurisprudenziali europee si veda P. DI MICO, *Il rapporto tra il diritto d'autore e diritto alla riservatezza: recenti sviluppi nella giurisprudenza comunitaria*, in *Il diritto d'autore* 1, 2010; F. GIOVANELLA, *Copyright and Information Privacy. Conflicting Rights in Balance,* cit., 250 e ss.

[292] CGUE 19 aprile 2012, C-461/10, *Bonnier Audio AB v. Perfect Communication Sweden AB*, liberamente accessibile presso: «https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:62010CJ0461&from=IT» (Ultimo accesso: 10 maggio 2022).

to-peer. L'operatore Internet tramite il quale era avvenuto lo scambio illecito di file era la ePhone.

Venuta a conoscenza delle violazioni del *copyright*, la Bonnier Audio proponeva dinanzi al Solna Tingsrätt (Tribunale di primo grado di Solna) domanda di ingiunzione al fine di ottenere la comunicazione del nome e del recapito della persona facente uso dell'indirizzo IP dal quale si presumeva fossero stati trasmessi i file in questione. Come nei casi precedenti, anche questa volta il *provider*, ePhone, si era opposto a tale domanda sostenendo, segnatamente, che l'ingiunzione richiesta risulterebbe contraria alla Direttiva 2006/24.

In primo grado, il Solna Tingsrätt aveva accolto la domanda di ingiunzione ai fini della comunicazione dei dati di cui trattasi. In sede di appello dinanzi allo Svea Hovrätt (Corte d'appello di Svea), la ePhone aveva chiesto di adire in via pregiudiziale la Corte di Giustizia affinché venisse precisato se la Direttiva 2006/24 ostasse alla comunicazione di informazioni relative ad un abbonato, al quale fosse stato assegnato un indirizzo IP, a soggetti diversi dalle autorità indicate nella Direttiva medesima. Il giudice di secondo grado, tuttavia, respingeva la domanda di rinvio pregiudiziale alla Corte.

Lo Svea Hovrätt aveva parimenti rilevato che le case editrici di audiolibri non avevano dimostrato l'esistenza di indizi effettivi dell'avvenuta violazione del diritto di proprietà intellettuale e decideva di annullare l'ingiunzione. A fronte di tale decisione, la Bonnier Audio quindi proponeva ricorso per Cassazione dinanzi allo Högsta Domstolen, giudice a quo del rinvio pregiudiziale di cui trattasi.

Il giudice del rinvio riteneva che, pur alla luce della sentenza del 29 gennaio 2008, Promusicae, come analizzata, sussistevano dubbi sulla questione se il diritto dell'Unione ostasse all'applicazione dell'articolo 53 quater della legge sul diritto d'autore svedese[293], considerato che tale sentenza non compiva alcun riferimento alla Direttiva 2006/24 (c.d. "Data Retention Directive")[294].

---

[293] Le disposizioni della Direttiva 2004/48 sono state recepite nel diritto svedese con l'introduzione di nuove disposizioni nella legge 1960:729 relativa alla proprietà letteraria e artistica [Lagen (1960:729) Om Upphovsrätt Till Litterära Och Konstnärliga Verk], per mezzo della legge 2009:109, recante modifica della legge 1960:729 [Lag (2009:109) Om Ändring I Lagen (1960:729)], del 26 febbraio 2009. Tale novella è entrata in vigore il 1 aprile 2009. L'articolo 53 quater della legge sul diritto d'autore così dispone:
"*Se il ricorrente può dimostrare la fondatezza dell'avvenuta violazione del diritto d'autore di un'opera, previsto all'articolo 53, il giudice può intimare, a pena di ammende, alla/e persona/e indicata/e supra nel secondo comma di fornire informazioni sull'origine e sulle reti di distribuzione delle merci o di prestazione di servizi che arrechino pregiudizio o costituiscano violazione di un diritto (ingiunzione di fornire informazioni). Una siffatta misura può essere disposta su domanda del titolare del diritto, del suo avente causa o di chiunque goda di un diritto legittimo di sfruttamento dell'opera. Essa può essere disposta solo a condizione che le informazioni richieste possano agevolare le indagini sulla violazione del diritto o sul pregiudizio allo stesso, derivante dalle suddette merci o dai suddetti servizi.*
L'obbligo di fornire informazioni grava su ogni persona:
1)autore o complice della violazione del diritto o del pregiudizio ad esso arrecato;
2)che abbia disposto su scala commerciale di una merce arrecante pregiudizio a un diritto o costituente violazione dello stesso;
3)che abbia utilizzato su scala commerciale un servizio arrecante pregiudizio a un diritto o costituente violazione dello stesso;
4)che abbia fornito su scala commerciale un servizio di comunicazione elettronica o di altra natura utilizzato per commettere atti arrecanti pregiudizio al diritto o la violazione dello stesso,
5)che sia stata identificata da un soggetto indicato ai punti 2)-4) supra come colui che ha partecipato alla produzione o alla distribuzione di una merce o alla fornitura di un servizio costituente violazione di un diritto o recante pregiudizio allo stesso".

[294] La Direttiva europea 2006/24/CE del Parlamento europeo e del Consiglio regolamentava la conservazione (compreso i tempi) di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione. Adottata in seguito agli attentati di Londra e Madrid del 2004 e 2005, armonizzava le disposizioni degli Stati membri dell'UE sulla conservazione dei dati delle conversazioni telefoniche e del traffico telematico, garantendone, quindi, la disponibilità a fini di indagine e di

Con le due questioni pregiudiziali, proposte dalla Corte Suprema svedese, si chiedeva, sostanzialmente, "*se la Direttiva 2006/24 debba essere interpretata nel senso che osta all'applicazione di una normativa nazionale, istituita sulla base dell'articolo 8 della Direttiva 2004/48, la quale consenta, ai fini dell'identificazione di un abbonato a Internet o di un utente Internet, di ingiungere ad un operatore Internet di comunicare al titolare di un diritto d'autore ovvero ad un suo avente causa l'identità di un abbonato al quale sia stato attribuito un indirizzo IP utilizzato ai fini della violazione del diritto di autore stesso e se il fatto che lo Stato membro interessato non abbia ancora provveduto alla trasposizione della Direttiva 2006/24, malgrado la scadenza del termine all'uopo previsto, incida sulla soluzione di tale questione*".

Ancora una volta la questione virava sul bilanciamento fra il trattamento dei dati personali e *l'enforcement* del diritto d'autore. In particolare, la Corte rilevava come la comunicazione richiesta dalla Bonnier Audio "*costituisce un trattamento di dati di carattere personale ai sensi dell'articolo 2, primo comma, della Direttiva 2002/58, in combinato disposto con l'articolo 2, lettera b), della Direttiva 95/46*". Tale comunicazione ricadeva, quindi, nella sfera di applicazione della Direttiva 2002/58, soluzione già incontrata nel caso Promusicae.

La Corte, allo stesso modo, rilevava altresì che la richiesta di comunicazione di dati di carattere personale, al fine di garantire la tutela effettiva del diritto d'autore, rientrava, in considerazione del suo oggetto, nella sfera di applicazione della Direttiva 2004/48, come già la sentenza Promusicae aveva affermato.

Per risolvere la questione pregiudiziale dinnanzi a sé proposta, la Corte ricorda quanto aveva già avuto modo di affermare, ossia che "*l'articolo 8, paragrafo 3, della Direttiva 2004/48, in combinato disposto con l'articolo 15, paragrafo 1, della Direttiva 2002/58, non osta a che gli Stati membri prevedano l'obbligo di trasmissione a soggetti privati di dati di carattere personale per consentire l'avvio, dinanzi ai giudici nazionali, di procedimenti nei confronti delle violazioni del diritto d'autore, senza peraltro obbligare gli Stati medesimi a disporre tale obbligo*[295]". Al contempo ricorda altresì come, con la precedente giurisprudenza, avesse affermato che dovessero essere gli ordinamenti nazionali a trovare il corretto bilanciamento fra la tutela del diritto d'autore e le esigenze di tutela della privacy.

Nel caso di specie, la Corte nota come la Svezia avesse, conseguentemente alla sentenza Promusicae ed in conformità alla stessa, deciso di avvalersi della facoltà di prevedere l'obbligo di trasmissione di dati a carattere personale a soggetti privati anche nell'ambito di un provvedimento civile, richiedendo al contempo che (1) sussistessero indizi reali di violazione di un diritto di proprietà intellettuale su un'opera, (2) che le informazioni richieste fossero tali da facilitare le indagini sulla violazione e (3) che i motivi alla base di tale ingiunzione si ricollegassero ad un interesse superiore agli inconvenienti o agli altri pregiudizi che ne potessero derivare per il destinatario o a qualsivoglia altro contrapposto interesse.

Secondo la Corte allora, "*tale normativa consente così al giudice nazionale al quale sia stata proposta la domanda di ingiunzione di comunicazione dei dati di carattere personale, da parte di un soggetto legittimato ad agire, di ponderare, in funzione delle circostanze della specie e tenendo in debita considerazione*

---

perseguimento di gravi reati. La Corte di Giustizia europea, con sentenza dell'8 aprile 2014 (cause riunite C-293/12 e C-593/12) dichiara tuttavia l'invalidità della Direttiva. Per maggiori informazioni in merito consultare il sito "*Protezione dei dati personali*" in cui B. SAETTA compie una accurata analisi delle vicende concernenti le sorti della Direttiva, accessibile presso: «https://protezionedatipersonali.it/data-retention» (Ultimo accesso: 10 maggio 2022), nonché si veda il sito del Garante per la Protezione dei dati personali in merito alla dichiarata illegittimità di tale Direttiva: «https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/3059819» (Ultimo accesso: 10 maggio 2022).

[295] CGUE 29 gennaio 2008, C-275/06, *Productores de Música de España (Promusicae) v. Telefónica de España SAU*, Grande Sezione, cit.

le esigenze risultanti dal principio di proporzionalità, gli opposti interessi in gioco. Ciò premesso, una siffatta normativa dev'essere ritenuta tale da garantire, in linea di principio, un giusto equilibrio tra la tutela del diritto di proprietà intellettuale, di cui godono i titolari del diritto d'autore, e la tutela dei dati di carattere personale, di cui beneficia un abbonato Internet o un utente Internet".

Per questi motivi, la Corte dichiara che le normative comunitarie devono essere interpretate nel senso che "*non ostano ad una normativa nazionale, come quella oggetto della causa principale, nella parte in cui tale normativa consente al giudice nazionale, dinanzi al quale sia stata proposta, da parte di un soggetto legittimato ad agire, domanda di ingiunzione di comunicare dati di carattere personale, di ponderare, in funzione delle circostanze della specie e tenuto debitamente conto delle esigenze risultanti dal principio di proporzionalità, i contrapposti interessi in gioco*".

Analizzando in chiave sinottica le pronunce Promusicae e Bonnier Audio quello che si può evidenziare è che, come nota Federica Giovanella[296], in nessuna delle due sentenze la Corte si è espressa esplicitamente su quale dei due diritti, il diritto d'autore ed il diritto alla privacy, debba prevalere in simili fattispecie; ed in secondo luogo che almeno la sentenza Bonnier Audio fornisce un criterio, per quanto precario, di soluzione di simili bilanciamenti: una analisi caso per caso. È chiaro, dunque, che questo criterio rimette al giudice la scelta del bilanciamento da compiere alla luce delle peculiarità del caso concreto.

Come sottolinea un'attenta dottrina, il problema in tutti questi casi è che "*non appena si abbandona il terreno della proprietà intellettuale, protetto da reti di filo spinato sempre più fitte ed estese e salvaguardato da* vigilantes *dotati di potenti mezzi tecnologici e ampie risorse finanziarie*" la tutela dei diritti fondamentali diventa difficoltosa. Secondo gli autori, infatti, "*nel campo dei diritti della personalità, in particolare, l'assenza di strumenti normativi tanto incisivi quanto quelli previsti a tutela di posizioni proprietarie sembra indurre le Corti a un atteggiamento molto più remissivo e rispettoso dell'interesse all'anonimato*"[297].

7.3.4. CASO SCARLET EXTENDED v. SABAM

Una terza decisione da analizzare, in seguito ai casi Promusicae e Bonnier Audio, è la sentenza Scarlet Extended SA v. SABAM[298]. Questa domanda è stata presentata nel contesto di una controversia tra la Scarlet Extended SA e la Société Belge des Auteurs, Compositeurs et Éditeurs SCRL (SABAM) vertente sul rifiuto della Scarlet di predisporre un sistema di filtraggio delle comunicazioni elettroniche realizzate tramite programmi per lo scambio di archivi *peer-to-peer*, onde impedire il trasferimento dei file che ledono i diritti d'autore.

La Scarlet era un Internet Service Provider che procurava ai propri clienti meramente l'accesso alla rete, senza proporre altri servizi come lo scaricamento o la condivisione dei file. Nel corso del 2004, la SABAM perveniva alla conclusione che gli utenti di Internet che si avvalevano dei servizi della Scarlet scaricavano da Internet, senza autorizzazione e senza pagarne i diritti, opere contenute nel suo catalogo utilizzando reti *peer-to-peer*. Con atto di ricorso del 24 giugno 2004 essa citava pertanto la Scarlet dinanzi al presidente del Tribunal de Première Instance de Bruxelles, sostenendo che, nella sua qualità di *Service Provider*, tale società avrebbe potuto e conseguentemente dovuto introdurre misure volte a far cessare le violazioni del diritto d'autore commesse dai suoi clienti.

---

296 F. GIOVANELLA, *Copyright and Information Privacy. Conflicting Rights in Balance*, cit. 270 e ss.

297 G. ALPA, G. RESTA, *Le Persone e la Famiglia 1, Le persone fisiche e i diritti della personalità*, cit., 504 e ss.

298 CGUE 24 novembre 2011, Causa C-70/10, *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, liberamente accessibile presso: «https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:62010CJ0070&from=EN» (Ultimo accesso: 10 maggio 2022).

LA SABAM chiedeva, anzitutto, che venisse riconosciuta la violazione dei diritti d'autore sulle opere musicali appartenenti al suo repertorio, in particolare dei diritti di riproduzione e di comunicazione al pubblico, dovuta allo scambio non autorizzato di file musicali, realizzato grazie al software *peer-to-peer*. Essa domandava inoltre che la Scarlet fosse condannata a far cessare tali violazioni rendendo impossibile o bloccando qualsiasi forma di scambio, mediante sistemi *peer-to-peer*, di file contenenti un'opera musicale.

Con sentenza 26 novembre 2004, il presidente Tribunal de Première Instance de Bruxelles accertava l'esistenza delle violazioni del diritto d'autore denunciate dalla SABAM. Tuttavia, prima di statuire sull'istanza di provvedimenti inibitori, esso incaricava un perito di verificare se le soluzioni tecniche proposte dalla SABAM fossero tecnicamente realizzabili, se esse consentissero di filtrare unicamente gli scambi illeciti di file e se esistessero altri dispositivi idonei a controllare l'utilizzo di programmi *peer-to-peer*, nonché di quantificare il costo dei dispositivi considerati. Nella sua relazione, il perito designato traeva la conclusione che, nonostante la presenza di numerosi ostacoli tecnici, non si poteva escludere completamente che il filtraggio ed il blocco degli scambi illeciti di file fosse realizzabile.

Pertanto, vista la relazione del perito informatico, con sentenza 29 giugno 2007, il presidente del Tribunal de Première Instance de Bruxelles condannava la Scarlet a far cessare le violazioni del diritto d'autore accertate con la sentenza 26 novembre 2004, rendendo impossibile qualsiasi forma, realizzata mediante un programma *peer-to-peer*, di invio o di ricezione, da parte dei suoi clienti, di file che contenessero un'opera musicale appartenente al repertorio della Sabam.

La Scarlet proponeva appello contro tale sentenza dinanzi al giudice del rinvio, affermando che detta ingiunzione non potesse essere considerata conforme all'art. 21 della legge 11 marzo 2003, su taluni aspetti giuridici dei servizi della società dell'informazione, che recepisce nel diritto nazionale l'art. 15 della Direttiva 2000/31, in quanto imponeva, de facto, un obbligo generale di sorveglianza sulle comunicazioni veicolate dalla sua rete, posto che qualsiasi dispositivo di blocco o di filtraggio del traffico *peer-to-peer* presuppone una sorveglianza generalizzata su tutte le comunicazioni che passano per tale rete. I rischi per la privacy, quindi, diventavano ancora più seri ed intensi.

Inoltre, la Scarlet argomentava in sede di gravame che la predisposizione di un sistema di filtraggio avrebbe leso le disposizioni del diritto dell'Unione in materia di tutela dei dati personali e di segreto delle comunicazioni, in quanto tale filtraggio implicava il trattamento degli indirizzi IP, che, come giustamente ricordava, sono dati personali.

Una nuova strategia di *enforcement* del diritto d'autore allora, una volta ancora, andava apertamente a scontrarsi con la tutela della privacy. In tale contesto in cui il bilanciamento pareva impossibile da compiere, la Cour d'appel de Bruxelles decise di sospendere il procedimento e di rinviare pregiudizialmente alla Corte di Giustizia.

Con le sue questioni il giudice del rinvio chiede, in sostanza, "*se le Direttive 2000/31, 2001/29, 2004/48, 95/46 e 2002/58, lette nel loro combinato disposto ed interpretate alla luce delle condizioni che la tutela dei diritti fondamentali applicabili implica, debbano essere interpretate nel senso che ostano all'ingiunzione rivolta ad un FAI (ISP) di predisporre un sistema di filtraggio: (1) di tutte le comunicazioni elettroniche che transitano per i suoi servizi, in particolare mediante programmi «peer-to-peer»; (2) che si applichi indistintamente a tutta la sua clientela; (3) a titolo preventivo; (4) a sue spese esclusive, e (5) senza limiti nel tempo, idoneo ad identificare nella rete di tale fornitore la circolazione di file contenenti un'opera musicale, cinematografica o audiovisiva rispetto alla quale il richiedente affermi di vantare diritti di proprietà intellettuale, onde bloccare il trasferimento di file il cui scambio pregiudichi il diritto d'autore*".

Secondo la Corte, l'attuazione di tale sistema di filtraggio presuppone: (1) che il Service Provider identifichi, in primo luogo, nell'insieme delle comunicazioni elettroniche di tutti i suoi clienti, i file che appartengono al traffico *peer-to-peer*; (2) che esso identifichi, in secondo luogo, nell'ambito di tale traffico, i file che contengono opere sulle quali i titolari dei diritti di proprietà intellettuale affermino di vantare diritti; (3) in terzo luogo, che esso determini quali tra questi file sono scambiati in modo illecito e, (4) in quarto luogo, che proceda al blocco degli scambi di file che esso stesso qualifica come illeciti.

Siffatta sorveglianza preventiva richiederebbe così un'osservazione attiva sulla totalità delle comunicazioni elettroniche realizzate sulla rete dell'ISP coinvolto e, pertanto, includerebbe tutte le informazioni da trasmettere e ciascun cliente che si avvale di tale rete. Da ciò si evince che tale ingiunzione imporrebbe a detto ISP una sorveglianza generalizzata, che è vietata dall'art. 15, n. 1, della Direttiva 2000/31[299].

Secondo la Corte, il diritto di privativa autoriale dovrebbe essere bilanciato in una simile circostanza con diritti fondamentali di almeno altrettanto valore. Nel caso di specie, la Corte identifica tre diritti ed interessi contrapposti con cui dover fare i conti: la libera iniziativa economica dei *provider*; la protezione dei dati personali degli utenti ed infine la libertà nelle comunicazioni e nelle informazioni.

Secondo la Corte, infatti, in merito al primo punto, un'ingiunzione di questo genere causerebbe una grave violazione della libertà di impresa degli *Internet Service Providers* in quanto costringerebbe costoro a predisporre un sistema informatico complesso, costoso e permanente.

In secondo luogo, come accennato, secondo la Corte un simile sistema di filtraggio sarebbe idoneo a ledere anche i diritti fondamentali dei clienti di tale *provider* , ossia il loro diritto alla tutela dei dati personali e la loro libertà di ricevere o di comunicare informazioni: diritti, questi ultimi, tutelati dagli artt. 8 e 11 della Carta di Nizza. Questo, infatti, implicherebbe un'analisi sistematica di tutti i contenuti, nonché la raccolta e l'identificazione degli indirizzi IP degli utenti, indirizzi che, come visto, costituiscono dati personali protetti, in quanto consentono di identificare in modo preciso i suddetti utenti[300].

In terzo luogo, poi, secondo la Corte detta ingiunzione rischierebbe di ledere la libertà di informazione, poiché tale sistema potrebbe non essere in grado di distinguere adeguatamente tra un contenuto lecito ed un contenuto illecito, sicché il suo impiego potrebbe produrre il risultato di bloccare comunicazioni aventi un contenuto lecito. Infatti,

---

[299] Come visto infatti, tale articolo recita: "*1. Nella prestazione dei servizi di cui agli articoli 12, 13 e 14, gli Stati membri non impongono ai prestatori un obbligo generale di sorveglianza sulle informazioni che trasmettono o memorizzano né un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite. 2. Gli Stati membri possono stabilire che i prestatori di servizi della società dell'informazione siano tenuti ad informare senza indugio la pubblica autorità competente di presunte attività o informazioni illecite dei destinatari dei loro servizi o a comunicare alle autorità competenti, a loro richiesta, informazioni che consentano l'identificazione dei destinatari dei loro servizi con cui hanno accordi di memorizzazione dei dati*".

[300] Si veda in merito quanto affermato *supra*, nonché si faccia riferimento a Gruppo di Lavoro Articolo 29, (Article 29 – WP), Opinion 2/2002 *On the use of unique identifiers in telecommunication terminal equipment: the example of IPv6*, adottata il 30 maggio 2002, disponibile presso: «http://www.eu.ipv6tf.org/PublicDocuments/wp58_en.pdf» (Ultimo accesso: 10 maggio 2022); Gruppo di Lavoro Articolo 29, (Article 29 – WP), Opinion 4/2007 *On the concept of personal data,* adottata il 20 giugno 2007 disponibile presso: «https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1496512» (Ultimo accesso: 10 maggio 2022). Si vedano altresì le pronunce giurisprudenziali: CGUE C-131/12, *Google Spain SL, Google Inc. c. Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, 13 maggio 2014 (Grande Sezione);CGUE 24 Settembre 2019, n. C-507/17, *Google Inc. v. Commission nationale de l'informatique et des libertés (CNIL)*; CGUE 24 Settembre 2019 n. C-136/17: *G.C., A.F., B.H., E.D. v Commission nationale de l'informatique et des libertés (CNIL).*

è indiscusso che la questione della liceità di una trasmissione dipende anche dall'applicazione di eccezioni di legge al diritto d'autore che variano da uno Stato membro all'altro. Inoltre, in certi Stati membri talune opere possono rientrare nel pubblico dominio o possono essere state messe in linea gratuitamente da parte dei relativi autori.

Per queste ragioni quindi la Corte di Giustizia afferma che ove il giudice nazionale dovesse adottare tale ingiunzione, che costringe i *Service Providers* a predisporre un simile sistema di filtraggio, il giudice nazionale in questione non rispetterebbe l'obbligo di garantire un giusto equilibrio tra, da un lato, il diritto di proprietà intellettuale e, dall'altro, la libertà di impresa, il diritto alla tutela dei dati personali e la libertà di ricevere o di comunicare informazioni.

7.3.5. CASO SABAM V. NETLOG

Un caso molto simile a quello appena analizzato in merito ai sistemi di filtraggio è rinvenibile nella decisione Sabam v. Netlog[301].

La Netlog gestiva una piattaforma social sulla quale ogni iscritto riceveva uno spazio personale, un profilo, che l'utente stesso poteva riempire e che era accessibile a livello mondiale. La funzione principale di tale piattaforma, come molte similari, era quella di creare comunità virtuali che consentissero agli utenti di comunicare tra loro. La SABAM, tuttavia, ritenne che la rete social della Netlog permetteva altresì a tutti gli utenti di utilizzare, tramite il loro profilo, opere musicali ed audiovisive del repertorio della SABAM, mettendo dette opere a disposizione del pubblico in maniera tale che altri utenti della suddetta rete potessero avervi accesso, e questo senza l'autorizzazione della SABAM e senza che la Netlog versasse un compenso a tale titolo.

Nel corso del mese di febbraio 2009, la SABAM si era rivolta alla Netlog al fine di stipulare una convenzione relativa al versamento, da parte di quest'ultima, di un compenso per l'utilizzo del repertorio della SABAM. Con lettera del 2 giugno 2009, la SABAM intimava alla Netlog di impegnarsi a cessare immediatamente e per il futuro la messa a disposizione del pubblico non autorizzata di opere musicali e audiovisive del suo repertorio. Il 23 giugno 2009 la SABAM faceva notificare alla Netlog un atto di citazione dinanzi al presidente del Rechtbank van Eerste Aanleg te Brussel, nell'ambito di un'azione inibitoria chiedendo, in particolare, che venisse ordinato alla Netlog di cessare immediatamente qualsiasi messa a disposizione illecita delle opere musicali o audiovisive del repertorio della SABAM. A tale riguardo, la Netlog sosteneva che l'accoglimento dell'azione della SABAM sarebbe equivalso ad imporre alla Netlog un obbligo generale di sorveglianza, così ponendosi in diretto contrasto con l'articolo 15, paragrafo 1, della Direttiva 2000/31.

Dato che la predisposizione di un simile sistema di filtraggio avrebbe imposto il sorgere di un obbligo di sottoporre i dati personali ad un trattamento che deve essere conforme alle disposizioni del diritto dell'Unione sulla protezione dei dati personali e sul segreto delle comunicazioni, il presidente del Rechtbank Van Eerste Aanleg te Brussel decise di sospendere il procedimento e rinviare la questione pregiudizialmente alla Corte di Giustizia.

---

[301] CGUE 16 febbraio 2012, C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV*, liberamente consultabile presso: «https://curia.europa.eu/juris/document/document.jsf?docid=119512&doclang=IT» (Ultimo accesso: 10 maggio 2022).

Data la similitudine delle richieste operate in questo caso, con quello precedentemente analizzato, le conclusioni cui giunse la Corte di Giustizia furono similari: un tale sistema di filtraggio non potrebbe resistere ad un corretto bilanciamento con i contrapposti diritti alla privacy, alla libertà di impresa ed alla libertà di informazione.

Richiamando il ragionamento della Corte si può notare come l'analisi sia ripresa quasi *verbatim* dalla precedente pronuncia, affermando infatti che: "*l'ingiunzione di predisporre il sistema di filtraggio controverso non può considerarsi conforme all'esigenza di garantire un giusto equilibrio tra, da un lato, la tutela del diritto di proprietà intellettuale, di cui godono i titolari dei diritti d'autore, e, dall'altro, quella della libertà d'impresa, di cui beneficiano operatori come i prestatori di servizi di hosting*", inoltre che " *l'ingiunzione di predisporre il sistema di filtraggio controverso implicherebbe, da un lato, l'identificazione, l'analisi sistematica e l'elaborazione delle informazioni relative ai profili creati sulla rete social dagli utenti della medesima, informazioni, queste, che costituiscono dati personali protetti, in quanto consentono, in linea di principio, di identificare i suddetti utenti*". Ed infine che "*detta ingiunzione rischierebbe di ledere la libertà di informazione, poiché tale sistema potrebbe non essere in grado di distinguere adeguatamente tra un contenuto illecito ed un contenuto lecito, sicché il suo impiego potrebbe produrre il risultato di bloccare comunicazioni aventi un contenuto lecito*".

7.3.6. CONSTANTIN FILM VERLEIH V. YOUTUBE LLC. E GOOGLE INC.

Importante e recente pronuncia che segna il passaggio dalla pirateria su reti peer-to-peer alla pirateria dello streaming è la sentenza Costantin Film contro Google[302]. Tuttavia, la fattispecie concreta, *mutatis mutandis*, si presenta come similare.

La domanda di pronuncia pregiudiziale verteva sull'interpretazione dell'articolo 8, paragrafo 2, lettera a), della Direttiva 2004/48/CE del Parlamento europeo e del Consiglio, del 29 aprile 2004, sul rispetto dei diritti di proprietà intellettuale.

Tale domanda era stata presentata nell'ambito di una controversia tra, da un lato, la Constantin Film Verleih GmbH, società distributrice di film con sede in Germania, e, dall'altro, YouTube LLC e Google Inc., con sede negli Stati Uniti, in merito alle informazioni richieste dalla Constantin Film Verleih a queste due società e riguardanti gli indirizzi di posta elettronica, gli indirizzi IP e i numeri di telefono cellulare di utenti che si sospettava avessero commesso violazioni dei suoi diritti di proprietà intellettuale.

In particolare, la Constantin Film Verleih disponeva in Germania dei diritti di sfruttamento esclusivi, tra le altre, sulle opere cinematografiche *Parker* e *Scary Movie 5*. Fra il 2013 e il 2014 tali opere erano state caricate sulla piattaforma di YouTube, motivo per cui la Constantin Film Verleih esigeva, da parte di YouTube e di Google, società controllante della prima, che le fosse fornito un insieme di informazioni relative a ciascuno degli utenti che avesse proceduto al caricamento delle medesime opere, in violazione dei suoi diritti di esclusiva economica.

Agendo in giudizio contro Google e Youtube, la controversia di primo grado relativa ai nomi e agli indirizzi postali degli utenti era stata formalmente definita, tuttavia la Constantin Film Verleih, avendo ottenuto solo nomi utenti fittizi; dunque, chiese che fosse ordinato a YouTube e Google di fornirle informazioni supplementari. Tali informazioni supplementari avevano ad oggetto gli indirizzi di posta elettronica e i numeri di telefono

[302] CGUE 9 luglio 2020, C-264/19, *Constantin Film Verleih V. Youtube Llc. E Google Inc.*, (Quinta Sezione), disponibile presso: «https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:62019CJ0264&from=it» (Ultimo accesso: 10 maggio 2022).

cellulare nonché gli indirizzi IP utilizzati dagli utenti di cui trattasi per il caricamento dei file, con il momento esatto di tale caricamento, nonché l'indirizzo IP utilizzato da ultimo da tali utenti per entrare nel loro account Google al fine di accedere alla piattaforma YouTube.

Con la sua sentenza del 3 maggio 2016, il Landgericht Frankfurt am Main (Tribunale del Land, Francoforte sul Meno, Germania) respinse la domanda della Constantin Film Verleih. Per contro, su appello di quest'ultima, con sentenza del 22 agosto 2018, l'Oberlandesgericht Frankfurt am Main (Tribunale superiore del Land, Francoforte sul Meno, Germania) accolse parzialmente la domanda della Constantin Film Verleih, e di conseguenza condannò YouTube e Google a fornire gli indirizzi di posta elettronica degli utenti di cui trattasi, respingendo tale appello quanto al resto.

Con il suo ricorso per Revision (Cassazione), proposto dinanzi al giudice del rinvio, il Bundesgerichtshof (Corte federale di giustizia, Germania), la Constantin Film Verleih persisteva nelle sue domande dirette a ottenere la condanna di YouTube e di Google a fornirle i numeri di telefono cellulare nonché gli indirizzi IP degli utenti.

In tale contesto, il Bundesgerichtshof decise di sospendere il procedimento e di chiedere pregiudizialmente alla Corte di Giustizia, se l'articolo 8, paragrafo 2, lettera a), della Direttiva 2004/48[303] dovesse essere interpretato nel senso che la nozione di "indirizzo" si riferisce, per quanto riguarda un utente che abbia caricato file lesivi di un diritto di proprietà intellettuale, al suo indirizzo di posta elettronica, al suo numero di telefono nonché all'indirizzo IP utilizzato per caricare tali file o all'indirizzo IP utilizzato in occasione del suo ultimo accesso all'account utente.

La Corte risolse facilmente la questione pregiudiziale, di scarso interesse ai nostri fini, ossia giunse da affermare che il diritto comunitario deve essere interpretato nel senso che la nozione di "indirizzo" non si riferisce a tutti gli elementi di cui veniva richiesta l'ostensione. Infatti, nel linguaggio corrente, esso riguarda unicamente l'indirizzo postale, vale a dire il luogo di domicilio o di residenza di una determinata persona. Ne consegue che tale termine, qualora, come all'articolo 8, paragrafo 2, lettera a), della Direttiva 2004/48, sia utilizzato senza

---

[303] In particolare, l'articolo 8 così come citato dispone: "*1. Gli Stati membri assicurano che, nel contesto dei procedimenti riguardanti la violazione di un diritto di proprietà intellettuale e in risposta a una richiesta giustificata e proporzionata del richiedente, l'autorità giudiziaria competente possa ordinare che le informazioni sull'origine e sulle reti di distribuzione di merci o di prestazione di servizi che violano un diritto di proprietà intellettuale siano fornite dall'autore della violazione e/o da ogni altra persona che:*

a)sia stata trovata in possesso di merci oggetto di violazione di un diritto, su scala commerciale;

b)sia stata sorpresa a utilizzare servizi oggetto di violazione di un diritto, su scala commerciale;

c)sia stata sorpresa a fornire su scala commerciale servizi utilizzati in attività di violazione di un diritto; oppure

d)sia stata indicata dai soggetti di cui alle lettere a), b) o c) come persona implicata nella produzione, fabbricazione o distribuzione di tali prodotti o nella fornitura di tali servizi.

2. Le informazioni di cui al paragrafo 1 comprendono, ove opportuno, quanto segue:

a)nome e indirizzo dei produttori, dei fabbricanti, dei distributori, dei fornitori e degli altri precedenti detentori dei prodotti o dei servizi, nonché dei grossisti e dei dettaglianti;

b)informazioni sulle quantità prodotte, fabbricate, consegnate, ricevute o ordinate, nonché sul prezzo spuntato per i prodotti o i servizi in questione.

3. I paragrafi 1 e 2 si applicano fatte salve le altre disposizioni regolamentari che:

a)accordano al titolare diritti d'informazione più ampi;

b)disciplinano l'uso in sede civile o penale delle informazioni comunicate in virtù del presente articolo;

c)disciplinano la responsabilità per abuso del diritto d'informazione;

d)accordano la possibilità di rifiutarsi di fornire informazioni che costringerebbero i soggetti di cui al paragrafo 1 ad ammettere la sua partecipazione personale o quella di parenti stretti ad una violazione di un diritto di proprietà intellettuale;

oppure

e)disciplinano la protezione o la riservatezza delle fonti informative o il trattamento di dati personali."

ulteriori precisazioni, non si riferisce all'indirizzo di posta elettronica, al numero di telefono o all'indirizzo IP.

Quello che a noi interessa è che, sebbene i riferimenti siano stati minimi, vi sono anche in questo caso importanti ragionamenti circa la tutela dei dati personali. Infatti, la Corte afferma che essa aveva già avuto occasione di dichiarare che il diritto comunitario mira a conciliare il rispetto di diversi diritti, in particolare il diritto d'informazione dei titolari del diritto d'autore e il diritto alla tutela dei dati personali degli utenti. La Corte non nega che il legislatore europeo avesse previsto per gli Stati membri la possibilità di concedere ai titolari di diritti di proprietà intellettuale il diritto di ricevere un'informazione più ampia, purché, tuttavia, fosse garantito un giusto equilibrio tra i diversi diritti fondamentali coinvolti e fossero rispettati gli altri principi generali del diritto dell'Unione, quali il principio di proporzionalità.

Sebbene la Corte non porti a maggiori conseguenze il ragionamento nel caso di specie, fra le righe deve essere letto anche il fatto che proprio la considerazione del bilanciamento fra interessi di proprietà intellettuale e l'interesse alla privacy ha condotto alla decisione di cui trattasi.

Il riferimento alla precedente giurisprudenza citata può essere illuminante. Nel Caso Coty Germany[304], seppur pervenendo a risultati diversi, essendo coinvolta una fattispecie riguardante il segreto bancario, la Corte si concentra sulla necessaria conciliazione tra le esigenze connesse alla tutela di diversi diritti fondamentali: da una parte, il diritto ad un ricorso effettivo e il diritto di proprietà intellettuale e, dall'altra, il diritto alla tutela dei dati personali.

Secondo la Corte infatti, in questo caso, il diritto d'informazione di cui dovrebbe beneficiare il ricorrente, nell'ambito di un procedimento relativo ad una violazione del suo diritto di proprietà, mira a rendere applicabile e a concretizzare il diritto fondamentale ad un ricorso effettivo garantito dall'articolo 47 della Carta e ad assicurare in tal modo l'esercizio effettivo del diritto fondamentale di proprietà, in cui rientra il diritto di proprietà intellettuale tutelato dall'articolo 17, paragrafo 2, di tale Carta. Il diritto alla tutela dei dati personali, del quale godono le persone di cui all'articolo 8, paragrafo 1, della Direttiva 2004/48, fa parte del diritto fondamentale di ogni persona di ricevere tutela dei dati personali che la riguardano, garantito dall'articolo 8 della Carta e dalla Direttiva 95/46.

Nello specifico, dunque, si deve affermare che, come risulta dall'articolo 2, paragrafo 3, lettera a), della Direttiva 2004/48 e dai suoi considerando 2 e 15, la tutela della proprietà intellettuale non dovrebbe ostacolare, in particolare, la tutela dei dati personali e, quindi, la Direttiva 2004/48 non può, segnatamente, porsi in contrasto con la Direttiva 95/46.

Strumentalizzando le parole della Corte, anche nel caso concreto, l'eventuale ostensione dei nominativi e numeri di telefono degli utenti avrebbe pesantemente violato il diritto alla protezione dei dati personali degli utenti, sebbene la Corte nel caso Costantin non abbia avuto la prontezza o la forza di affermarlo.

7.3.7. CASO STICHTING BREIN: The Pirate Bay

[304] CGUE 16 luglio 2015, C-580/13, *Coty Germany GmbH v. Stadtsparkasse Magdeburg*, (Quarta Sezione), liberamente accessibile presso: «https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:62013CJ0580&from=IT» (Ultimo accesso: 10 maggio 2022).

Famoso caso che negli ultimi anni ha colpito con rinnovato vigore la pirateria è il "Stichting Brein", meglio conosciuto come "Pirate Bay"[305]. Con questo episodio assistiamo ad una rinnovata ferocia nell'attaccare i sistemi di condivisione *peer-to-peer*. Infatti, i titolari dei diritti d'autore, scottati dalle sconfitte ottenute nei precedenti tentativi, come visto, hanno deciso di cambiare strategia e puntare, con un'azione legale, a far rientrare l'operato di tali piattaforme nel concetto di "comunicazione al pubblico"[306].

Il rinvio pregiudiziale era originato nell'ambito di una controversia tra la Stichting Brein, una fondazione che protegge gli interessi dei titolari del diritto d'autore, e la Ziggo BV nonché la XS4ALL Internet BV, Internet Service Providers, relativamente ad alcune domande presentate dalla Stichting Brein e dirette a far ingiungere alle due società di bloccare i nomi di dominio e gli indirizzi IP della piattaforma di condivisione online "The Pirate Bay" (TPB).

Una parte rilevante degli utenti dei *Service Providers* utilizzava la piattaforma di condivisione Pirate Bay, un sistema di scambio di file *peer-to-peer* basato su un indice BitTorrent. La caratteristica essenziale di BitTorrent consiste nel fatto che i file da condividere sono divisi in piccole parti, per cui non è necessario disporre di un *server* centrale per la memorizzazione dei medesimi, circostanza che alleggerisce l'onere dei *server* individuali durante il processo di condivisione. Per poter condividere i file, gli utenti devono prima scaricare un software specifico, denominato "client-BitTorrent", che non viene fornito dalla piattaforma di condivisione online TPB.

Gli utenti (denominati *seeders*) che intendono mettere un file, presente sul loro computer, a disposizione di altri utenti (denominati *leechers*) devono creare un file torrent con l'ausilio del loro client-BitTorrent. I file torrent rinviano a un server centrale (denominato *tracker*) che identifica gli utenti disponibili a condividere un determinato file. Tali file torrent sono caricati (mediante *upload*) dai *seeders* su una piattaforma di condivisione online, quale TPB, che provvede quindi a indicizzarli, affinché possano essere reperiti dagli utenti della piattaforma di condivisione online e affinché le opere cui tali file rinviano possano essere scaricate (mediante *download*) in diversi frammenti sui computer degli utenti, con l'ausilio del loro client-BitTorrent.

Nell'ambito del procedimento a quo, la Stichting Brein chiedeva anzitutto che venisse ingiunto alla Ziggo e alla XS4ALL di bloccare i nomi di dominio e gli indirizzi IP della piattaforma di condivisione online TPB, al fine di evitare che i servizi di tali *Service Provider*

---

[305] CGUE 14 giugno 2017, C-610/15*, Stichting Brein contro Ziggo BV e XS4ALL Internet BV* (Seconda Sezione), liberamente consultabile presso: «https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:62015CJ0610&from=IT» (Ultimo accesso: 10 maggio 2022).

[306] Tale diritto è introduzione della Direttiva c.d. InfoSoc, ossia la Direttiva 2001/29/CE del Parlamento europeo e del Consiglio, del 22 maggio 2001, sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione. L'art. 3 dispone in merito*: "1. Gli Stati membri riconoscono agli autori il diritto esclusivo di autorizzare o vietare qualsiasi comunicazione al pubblico, su filo o senza filo, delle loro opere, compresa la messa a disposizione del pubblico delle loro opere in maniera tale che ciascuno possa avervi accesso dal luogo e nel momento scelti individualmente.*

2. Gli Stati membri riconoscono ai soggetti sottoelencati il diritto esclusivo di autorizzare o vietare la messa a disposizione del pubblico, su filo o senza filo, in maniera tale che ciascuno possa avervi accesso dal luogo e nel momento scelti individualmente:

a) gli artisti interpreti o esecutori, per quanto riguarda le fissazioni delle loro prestazioni artistiche;

b) ai produttori di fonogrammi, per quanto riguarda le loro riproduzioni fonografiche;

c) ai produttori delle prime fissazioni di una pellicola, per quanto riguarda l'originale e le copie delle loro pellicole;

d) agli organismi di diffusione radiotelevisiva, per quanto riguarda le fissazioni delle loro trasmissioni, siano esse effettuate su filo o via etere, comprese le trasmissioni via cavo o via satellite.

3. I diritti di cui ai paragrafi 1 e 2 non si esauriscono con alcun atto di comunicazione al pubblico o con la loro messa a disposizione del pubblico, come indicato nel presente articolo".

potessero essere utilizzati per violare il diritto d'autore e i diritti connessi dei titolari dei diritti di cui la Stichting Brein proteggeva gli interessi.

Il giudice di primo grado accoglieva le domande della Stichting Brein. Tuttavia, esse furono respinte in appello. Lo Hoge Raad der Nederlanden (Corte suprema dei Paesi Bassi) rilevava che, in tale causa, era accertato che, mediante la piattaforma di condivisione online TPB, opere protette venivano messe a disposizione del pubblico senza l'autorizzazione dei titolari dei diritti. Era parimenti accertato che, mediante tale piattaforma, gli abbonati della Ziggo e della XS4ALL rendevano accessibili, senza l'autorizzazione dei titolari dei diritti, opere protette, violando così il diritto d'autore e i diritti connessi di tali titolari.

Con la sua prima questione, il giudice del rinvio chiedeva sostanzialmente se la nozione di comunicazione al pubblico, ai sensi dell'articolo 3, paragrafo 1, della Direttiva 2001/29, dovesse essere interpretata nel senso che comprende, in circostanze come quelle di cui al procedimento principale, la messa a disposizione e la gestione, su Internet, di una piattaforma di condivisione che, mediante l'indicizzazione di metadati relativi ad opere protette e la fornitura di un motore di ricerca, consente agli utenti di tale piattaforma di localizzare tali opere e di condividerle nell'ambito di una rete tra utenti.

Dall'articolo 3, paragrafo 1, della Direttiva 2001/29 risulta che "*gli Stati membri sono tenuti a provvedere affinché gli autori godano del diritto esclusivo di autorizzare o vietare qualsiasi comunicazione al pubblico, su filo o senza filo, delle loro opere, compresa la messa a disposizione del pubblico delle loro opere in maniera tale che ciascuno possa avervi accesso dal luogo e nel momento scelti individualmente*". In forza di tale disposizione, gli autori dispongono pertanto di un diritto di natura precauzionale che consente loro di frapporsi tra eventuali utenti della loro opera e la comunicazione al pubblico che detti utenti potrebbero voler effettuare, e ciò al fine di vietare quest'ultima[307].

Dalla giurisprudenza della Corte di Giustizia si può pertanto evincere che, in linea di principio, ogni atto con cui un utente dà, con piena cognizione di causa, accesso ai suoi clienti ad opere protette può costituire un atto di comunicazione, ai sensi dell'articolo 3, paragrafo 1, della Direttiva 2001/29.

Nel caso di specie occorre constatare, anzitutto, che è pacifico che opere protette dal diritto d'autore erano messe, mediante la piattaforma di condivisione online TPB, a disposizione degli utenti di tale piattaforma, di modo che questi potessero accedervi dal luogo e nel momento che sceglievano individualmente.

Inoltre, è vero che, come sottolineato dal giudice del rinvio, le opere così messe a disposizione degli utenti erano state fornite non già dagli amministratori di quest'ultima, bensì dai suoi utenti. Tuttavia, detti amministratori, mediante la messa a disposizione e la gestione di una piattaforma di condivisione online, intervenivano con piena cognizione delle conseguenze del proprio comportamento, al fine di dare accesso alle opere protette, indicizzando ed elencando su tale piattaforma i file torrent che consentivano agli utenti della medesima di localizzare le opere e di condividerle nell'ambito di una rete *peer-to-peer*. A tale riguardo, è infatti da notare che senza la messa a disposizione e la gestione da parte dei

[307] In merito si veda CGUE 26 aprile 2017, C-527/15, *Stichting Brein*, liberamente accessibile presso: «https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:62015CA0527&from=ES» (Ultimo accesso: 10 maggio 2022); CGUE 31 maggio 2016, C-117/15, *Reha Training*, liberamente accessibile presso: «https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:62015CJ0117&from=IT» (Ultimo accesso: 10 maggio 2022).

suddetti amministratori, le opere in questione non avrebbero potuto essere condivise dagli utenti o, quantomeno, la loro condivisione su Internet sarebbe stata più complessa.

La Corte di Giustizia inoltre nota anche come gli stessi amministratori avessero manifestato espressamente, sui blog e sui forum disponibili su detta piattaforma, il loro obiettivo di mettere a disposizione degli utenti opere protette, incitando questi ultimi a realizzare copie di tali opere. In ogni caso, dalla decisione di rinvio risulta che gli amministratori della piattaforma di condivisione online TPB non potevano ignorare che fornissero accesso ad opere pubblicate senza l'autorizzazione dei titolari di diritti, dato il fatto, espressamente sottolineato dal giudice del rinvio, che gran parte dei file torrent che comparivano sulla piattaforma di condivisione online TPB rinviava ad opere pubblicate senza l'autorizzazione dei titolari di diritti. Inoltre, non si poteva contestare che la messa a disposizione e la gestione della piattaforma di condivisione online erano realizzate allo scopo di trarne profitto, dal momento che tale piattaforma generava considerevoli introiti pubblicitari.

La Corte, quindi, decide statuendo che la nozione di comunicazione al pubblico, ai sensi dell'articolo 3, paragrafo 1, della Direttiva 2001/29, deve essere interpretata nel senso che comprende la messa a disposizione e la gestione, su Internet, di una piattaforma di condivisione che consente agli utenti di tale piattaforma di localizzare tali opere e di condividerle nell'ambito di una rete peer-to-peer.

Pare che il ragionamento in grado di superare le previgenti sentenze in merito al delicato bilanciamento fra diritto d'autore e tutela dei dati personali, possa essere superato con riferimento al "diritto di comunicazione al pubblico", un diritto che pare essere più forte, nelle parole della giurisprudenza, della tutela dei dati personali, come recentemente è stato confermato dalla giurisprudenza della Corte di Giustizia.

7.3.8. CASO MIRCOM INTERNATIONAL CONTENT MANAGEMENT & CONSULTING (M.I.C.M.) LIMITED CONTRO TELENET BVBA

Molto recentemente, il 17 giugno 2021, la Corte di Giustizia si è pronunciata su una nuova importante causa ai fini del presente elaborato, sul caso Mircom[308]. Essa rappresenta il punto di connessione nei bilanciamenti in una linea evolutiva tracciata dalla giurisprudenza di questo capitolo e durata più di un decennio. Infatti, le somiglianze nei fatti di causa fra le prime sentenze analizzate e quest'ultima sono molte, eppure gli esiti diversi da quelli che ci si aspettava di rinvenire.

Tale domanda di rinvio pregiudiziale era stata presentata nell'ambito di una controversia tra la Mircom International Content Management & Consulting (M.I.C.M.) Limited – società di diritto cipriota, titolare di determinati diritti su un gran numero di film pornografici prodotti da otto imprese stabilite negli Stati Uniti e in Canada – e la Telenet BVBA – società stabilita in Belgio, che forniva, segnatamente, servizi di accesso a Internet.

---

[308] CGUE 17 giugno 2021, C-597/19, *Mircom International Content Management & Consulting (M.I.C.M.) Limited contro Telenet BVBA*, (Quinta Sezione), liberamente consultabile presso: «https://eur-lex.europa.eu/legal-content/IT/TXT/ HTML/?uri=CELEX:62019CJ0597&from=IT» (Ultimo accesso: 10 maggio 2022); per un esaustivo commento in merito si veda l'articolo di L. DAFFARRA, *Copyright, come identificare gli autori delle violazioni nel file-sharing secondo la Corte di Giustizia UE*, in *Agenda Digitale.EU,* liberamente accessibile presso: «https://www.agendadigitale.eu/mercati-digitali/*copyright*-la-Corte-di-giustizia-fa-chiarezza-sullidentificazione-degli-autori-delle-violazioni-nel-file-sharing/» (Ultimo accesso: 10 maggio 2022).

Il 6 giugno 2019, la Mircom aveva investito l'Ondernemingsrechtbank Antwerpen (Tribunale delle imprese di Anversa, Belgio) di un'azione diretta a far ingiungere alla Telenet di produrre in giudizio i dati identificativi dei suoi utenti, le cui connessioni Internet erano state utilizzate per condividere, su una rete *peer-to-peer* con l'ausilio del protocollo BitTorrent, film facenti parte del catalogo della Mircom.

La Mircom affermava, infatti, di possedere migliaia di indirizzi IP dinamici, registrati per suo conto, grazie al software *FileWatchBT*, dalla Media Protector GmbH, una società stabilita in Germania, al momento della connessione dei suddetti clienti della Telenet mediante il software di condivisione client-BitTorrent. Una logica molto simile allora a quella che aveva investito il caso Peppermint, che si avvalse dell'operato della Logistep. Parliamo anche in questo caso di una massiccia attività di monitoraggio degli utenti ed un trattamento dei dati personali, gli indirizzi IP appunto, in via di autotutela. Segnaliamo poi che proprio la qualità pornografica dei contenuti illecitamente scambiati sulla rete pone un ulteriore interrogativo circa la sensibilità delle informazioni richieste.

Tralasciando questioni puramente tecniche relative al funzionamento del sistema di scambio tramite file BitTorrent, il giudice di Anversa si trovava dinnanzi ad almeno due questioni di complessa risoluzione. In primo luogo, il giudice del rinvio nutriva dubbi sul fatto che un'impresa, quale la Mircom, potesse godere della protezione conferita dalla Direttiva 2004/48 *sull'enforcement* del diritto d'autore nella misura in cui essa non sfruttava effettivamente i diritti ceduti dagli autori dei film in questione, ma si limitava a chiedere un risarcimento del danno a presunti autori di violazioni. Infatti, la società Mircom, di fatto, ricopriva il ruolo di titolare di limitati diritti connessi sulle opere oggetto di violazione dei diritti, in quanto essa li acquisiva al solo scopo di agire giudizialmente verso i pirati della rete e di conseguenza chiedere un risarcimento dei danni per violazione del *copyright*. Chiaramente, attraverso queste azioni avrebbe trattenuto per contratto parte del ricavo spettante agli effettivi proprietari dei beni immateriali. In gergo, una simile funzione viene definita "*copyright troll*". Per questa ragione, la Corte si interroga anche sul "se" questa impresa potesse godere del diritto di *discovery* che la Direttiva Enforcement assicura.

In secondo luogo, poi, il giudice del rinvio si poneva la questione della liceità del modo in cui gli indirizzi IP erano stati raccolti dalla Mircom, alla luce dell'articolo 6, paragrafo 1, primo comma, lettera f), del Regolamento 2016/679[309]. Questa questione è evidentemente

[309] L'art. 6 del GDPR infatti dispone che "*1. Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:*
a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;
d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.
La lettera f) del primo comma non si applica al trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti.
2. Gli Stati membri possono mantenere o introdurre disposizioni più specifiche per adeguare l'applicazione delle norme del presente regolamento con riguardo al trattamento, in conformità del paragrafo 1, lettere c) ed e), determinando con maggiore precisione requisiti specifici per il trattamento e altre misure atte a garantire un trattamento lecito e corretto anche per le altre specifiche situazioni di trattamento di cui al capo IX.
3. La base su cui si fonda il trattamento dei dati di cui al paragrafo 1, lettere c) ed e), deve essere stabilita:

quella che ci interessa più da vicino, essendo su questo punto che il bilanciamento fra *l'enforcement* del diritto d'autore e la tutela della vita privata vive il maggior punto di frizione. Essendo infatti richiesto che il trattamento sia necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato, la questione si risolve nel bilanciamento fra interesse *all'enforcement* del diritto d'autore, attuato per il tramite di una corposa sorveglianza sul web, oppure quello al corretto trattamento dei dati personali degli utenti.

Stanti tali circostanze, il Tribunale delle imprese di Anversa decise di sospendere il procedimento e di sottoporre alla Corte numerose questioni pregiudiziali.

In particolare, con la sua prima questione, il giudice del rinvio chiedeva alla Corte se la nozione di comunicazione al pubblico, di cui all'articolo 3, paragrafo 1, nonché l'articolo 3, paragrafo 2, lettera c), della Direttiva 2001/29, come visto, comprendeva la condivisione, su una rete tra utenti *peer-to-peer*, di segmenti, talvolta molto frammentari, di un file multimediale contenente un'opera protetta.

Con la sua seconda questione, il giudice del rinvio chiedeva, in sostanza, se la Direttiva 2004/48 dovesse essere interpretata nel senso che un soggetto contrattualmente titolare di taluni diritti di proprietà intellettuale, che tuttavia non li sfruttava esso stesso, ma si limitava a chiedere il risarcimento del danno ai presunti autori di violazioni, potesse beneficiare delle misure, delle procedure e dei mezzi di ricorso di cui al capo II di tale Direttiva.

Con la terza e la quarta questione inoltre, il giudice del rinvio chiedeva, in sostanza, se l'articolo 6, paragrafo 1, primo comma, lettera f), del Regolamento 2016/679 dovesse essere interpretato nel senso che esso osta, da un lato, alla registrazione sistematica, da parte del titolare dei diritti di proprietà intellettuale, nonché da parte di un terzo per suo conto, di indirizzi IP di utenti di reti *peer-to-peer* le cui connessioni Internet sono state asseritamente utilizzate nelle attività di violazione. Dall'altro lato, se esso osti alla comunicazione dei nomi e degli indirizzi postali di tali utenti a detto titolare oppure a un terzo al fine di consentirgli di proporre un ricorso per risarcimento dinanzi a un giudice civile.

---

a) dal diritto dell'Unione; o

b) dal diritto dello Stato membro cui è soggetto il titolare del trattamento.

La finalità del trattamento è determinata in tale base giuridica o, per quanto riguarda il trattamento di cui al paragrafo 1, lettera e), è necessaria per l'esecuzione di un compito svolto nel pubblico interesse o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento. Tale base giuridica potrebbe contenere disposizioni specifiche per adeguare l'applicazione delle norme del presente regolamento, tra cui: le condizioni generali relative alla liceità del trattamento da parte del titolare del trattamento; le tipologie di dati oggetto del trattamento; gli interessati; i soggetti cui possono essere comunicati i dati personali e le finalità per cui sono comunicati; le limitazioni della finalità, i periodi di conservazione e le operazioni e procedure di trattamento, comprese le misure atte a garantire un trattamento lecito e corretto, quali quelle per altre specifiche situazioni di trattamento di cui al capo IX. Il diritto dell'Unione o degli Stati membri persegue un obiettivo di interesse pubblico ed è proporzionato all'obiettivo legittimo perseguito.

4. Laddove il trattamento per una finalità diversa da quella per la quale i dati personali sono stati raccolti non sia basato sul consenso dell'interessato o su un atto legislativo dell'Unione o degli Stati membri che costituisca una misura necessaria e proporzionata in una società democratica per la salvaguardia degli obiettivi di cui all'articolo 23, paragrafo 1, al fine di verificare se il trattamento per un'altra finalità sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti, il titolare del trattamento tiene conto, tra l'altro:

a) di ogni nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto;

b) del contesto in cui i dati personali sono stati raccolti, in particolare relativamente alla relazione tra l'interessato e il titolare del trattamento;

c) della natura dei dati personali, specialmente se siano trattate categorie particolari di dati personali ai sensi dell'articolo 9, oppure se siano trattati dati relativi a condanne penali e a reati ai sensi dell'articolo 10;

d) delle possibili conseguenze dell'ulteriore trattamento previsto per gli interessati;

e) dell'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione."

Se il caso fosse stato proposto al Tribunale di Roma, grazie alle osservazioni del Garante della privacy, la riposta a tali questioni sarebbe consistita in una forte censura all'attività di monitoraggio della Mircom. Tuttavia, la questione venne proposta in sede europea ed il bilanciamento prese una piega diversa.

Analizzando le risposte della Corte in merito a queste domande, ma concentrandoci sulle ultime due, possiamo affermare che la prima questione venne dalla Corte risolta affermando che costituisce una messa a disposizione del pubblico anche il caricamento di meri segmenti di un file multimediale contenente un'opera protetta. Nel caso di specie infatti qualsiasi utente della rete *peer-to-peer* poteva facilmente ricostituire il file originario a partire da segmenti disponibili sui computer degli utenti che partecipavano al medesimo sistema.

Per quanto invece riguarda la seconda domanda, la Corte afferma che tale questione doveva essere intesa come comprensiva di tre parti, vale a dire, in primo luogo, quella relativa alla legittimazione ad agire di un soggetto come la Mircom per chiedere l'applicazione delle misure, delle procedure e dei mezzi di ricorso di cui al capo II della Direttiva 2004/48; in secondo luogo, quella inerente alla questione di stabilire se un soggetto del genere può aver subito un pregiudizio; in terzo luogo, quella concernente la ricevibilità della sua richiesta di informazioni.

La Corte di Giustizia in merito a questo secondo punto non ha dubbi. Infatti, afferma che un soggetto contrattualmente titolare di taluni diritti di proprietà intellettuale, che tuttavia non li sfrutta esso stesso, ma si limita a chiedere il risarcimento del danno a presunti autori di violazioni, può beneficiare, in linea di principio, delle misure, delle procedure e dei mezzi di ricorso previsti dal diritto comunitario.

Il punto che desta maggior interesse ai nostri fini è quello riguardante le risposte date dalla Corte di Giustizia sulle domande terza e quarta in quanto strettamente concernenti il profilo di bilanciamento fra *enforcement* del diritto d'autore e la tutela dei dati personali, alla luce, questa volta, del GDPR.

La Corte nota preliminarmente come "*nel procedimento principale, si discute di due diversi trattamenti di dati personali, ossia un primo trattamento che è già stato effettuato, a monte, dalla Media Protector e per conto della Mircom, nell'ambito di reti tra pari (peer-to-peer) – consistente nella registrazione degli indirizzi IP di utenti le cui connessioni Internet sono state asseritamente utilizzate, in un dato momento, per il caricamento di opere protette su tali reti – e un secondo trattamento che, ad avviso della Mircom, deve essere effettuato a valle dalla Telenet, consistente, da un lato, nell'identificazione di tali utenti attraverso un'attività di collegamento tra tali indirizzi IP e quelli che, in quel medesimo momento, la Telenet aveva attribuito a tali utenti per effettuare detto caricamento e, dall'altro, nella comunicazione alla Mircom dei nomi e degli indirizzi dei medesimi utenti*".

La Corte non ha dubbi nel ricordare che un indirizzo IP dinamico registrato da un fornitore costituisce un dato personale, ai sensi dell'articolo 4 GDPR, ove disponga di mezzi giuridici che gli consentano di far identificare l'interessato grazie ad informazioni aggiuntive in suo possesso. Di conseguenza, la registrazione di tali indirizzi ai fini del loro successivo utilizzo nell'ambito di azioni giudiziarie costituisce un trattamento dei dati personali.

La Corte ricorda poi che ai sensi dell'articolo 6, paragrafo 1, primo comma, lettera f) del GDPR, il trattamento di dati personali è lecito solo se, e nella misura in cui, tale trattamento sia necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali.

Il GDPR, infatti, richiede in merito che siano rispettate almeno tre condizioni: in primo luogo, il perseguimento del legittimo interesse del titolare del trattamento o di terzi, in secondo luogo, la necessità del trattamento dei dati personali per il perseguimento del legittimo interesse e, in terzo luogo, la condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato[310].

Al riguardo, la Corte ritiene che il valido recupero dei crediti possa costituire un legittimo interesse che giustifica il trattamento dei dati personali; che la condizione della necessarietà potrebbe, nel caso di specie, essere soddisfatta dal momento che l'individuazione del titolare della connessione è spesso possibile solo sulla base dell'indirizzo IP e delle informazioni messe a disposizione dal fornitore di accesso a Internet. Infine, per quanto concerne la condizione relativa alla ponderazione dei diritti e degli interessi contrapposti in questione, essa dipende, in linea di principio, dalle circostanze specifiche del caso concreto per cui, secondo la Corte, spetterebbe al giudice del rinvio valutare tali specifiche circostanze. Sorprendentemente invece, il fatto che i contenuti avessero natura pornografica e che le informazioni fossero particolarmente sensibili non venne preso sufficientemente in considerazione. Il tracciamento degli utenti in questo caso ineriva allo scambio di contenuti che, ove ricondotti all'identità degli utenti, avrebbe rivelato informazioni sui gusti e sulle abitudini sessuali degli stessi. Ove questo elemento fosse stato correttamente soppesato, il trattamento avrebbe dovuto essere dichiaro illecito sin dal principio, non esistendo alcun "legittimo interesse del titolare" che possa giustificarne un simile trattamento ai sensi dell'art. 9 GDPR.

Dato che i fatti di causa, come nota la Corte, sembrano rientrare sia nell'ambito di applicazione del Regolamento 2016/679 che in quello della Direttiva 2002/58, atteso che gli indirizzi IP trattati costituiscono tanto dati personali quanto dati relativi al traffico, occorreva verificare se la valutazione della liceità di un trattamento del genere dovesse tener conto delle condizioni previste da tale Direttiva.

Al riguardo, occorre rilevare che, ai sensi dell'articolo 5, paragrafo 1, della Direttiva 2002/58, gli Stati membri vietano l'ascolto, la captazione, la memorizzazione e altre forme di intercettazione o di sorveglianza delle ¢comunicazioni, e dei relativi dati sul traffico, ad opera di persone diverse dagli utenti, senza consenso di questi ultimi, eccetto quando queste ultime siano legalmente autorizzate a norma dell'articolo 15, paragrafo 1, di tale Direttiva.

Detto articolo 15, paragrafo 1, consente, in sostanza, tanto al diritto dell'Unione quanto al diritto dello Stato membro cui è soggetto il titolare del trattamento di limitare, mediante misure legislative, la portata dell'obbligo di riservatezza dei dati personali nel settore della comunicazione elettronica qualora tale limitazione rispetti l'essenza dei diritti e delle libertà fondamentali e costituisca una misura necessaria e proporzionata in una società democratica per garantire, segnatamente, la protezione dei diritti e delle libertà altrui nonché l'esecuzione delle azioni civili.

La Corte non si ritiene in grado di fornire al giudice del rinvio indicazioni utili quanto alla questione di stabilire se un trattamento come quello effettuato a monte, consistente nella registrazione di detti indirizzi IP, rechi pregiudizio ai diritti fondamentali. Per queste ragioni, la Corte ritiene che se dalle verifiche effettuate dal giudice del rinvio dovesse risultare l'esistenza di misure legislative nazionali che potrebbero essere utilmente applicate al caso di

[310] In tal senso la Corte di Giustizia cita anche altra propria giurisprudenza su cui si basa in tale indagine e segnatamente il caso CGUE 4 maggio 2017, C-13/16, *Rīgas satiksme*, liberamente accessibile presso: «https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:62016CJ0013&from=IT» (Ultimo accesso: 10 maggio 2022).

specie, e ammesso che risulti altresì, sulla base degli elementi di interpretazione forniti dalla Corte, che la Mircom è legittimata ad agire e che la sua richiesta di informazioni è giustificata, proporzionata e non abusiva, i summenzionati trattamenti devono essere considerati leciti, ai sensi del Regolamento 2016/679.

Non è intenzione di questo elaborato sostituirsi al giudice ed al suo prudente apprezzamento dei diritti e degli interessi in gioco; tuttavia, desta quantomeno stupore che la Corte di Giustizia, tante volte intenta a fortificare con la sua giurisprudenza le disposizioni del GDPR, in questo campo sia più permissiva. Un trattamento dei dati personali era avvenuto già nel momento del rastrellamento degli indirizzi IP degli utenti compiuto dalla Mircom per tramite della società Media Protector GmbH. Si consideri altresì che tale monitoraggio è avvenuto in un contesto, quale quello dello scambio su reti *peer-to-peer* di materiale pornografico, che è tema particolarmente sensibile, con rischio quindi non solo di sciogliere le garanzie di anonimato degli utenti del web, ma di disvelare anche le preferenze più intime degli utenti.

Chiaramente, questo caso richiama alla mente quanto già analizzato, all'inizio di questa sottosezione, in merito alla vicenda Peppermint. Una storia che si ripete allora, anche se con tecnologie in parte diverse e con ragionamenti solo parzialmente dissimili. È chiaro a questo punto che la Corte sia oscillante nelle sue pronunce e non voglia, o non possa, stabilire un bilanciamento durevole fra i due diritti oggetto della nostra analisi.

Appare forse ora il caso di richiamare l'attenzione anche ad un altro dato utile a costruire un più corretto bilanciamento fra diritti che abbiamo voluto intendere come fondamentali. Caterina Sganga ricorda infatti come l'essenza del diritto d'autore potrebbe essere individuata sulla base della sua funzione sociale essenziale definita dalle Direttive e adattata al particolare settore o opera protetta interessata. Entro tale nucleo essenziale, secondo l'autrice, rientrerebbero solo gli atti che garantiscono i ricavi necessari al raggiungimento di tali obiettivi. In questo senso, dato che anche gli obiettivi socio-culturali farebbero parte della funzione essenziale del diritto d'autore dell'UE, qualsiasi comportamento contrario al loro raggiungimento sarebbe e dovrebbe anche essere inteso come estraneo all'ambito di protezione dell'articolo 17 della Carta di Nizza[311].

Non è dato sapere quale direzione la giurisprudenza europea prenderà in futuro e come il bilanciamento verrà gestito nelle successive pronunce. Tuttavia, un aspetto già risulta chiaro, ossia che nell'evoluzione giurisprudenziale dovranno svolgere un ruolo di primaria importanza le regole ora disposte dall'art. 17 della Direttiva 2019/790 che riguarda nello specifico proprio le piattaforme di condivisione dei contenuti online protetti da diritti d'autore. Presumibilmente sarà proprio su questa disposizione, come vedremo nel quarto

---

311 C. SGANGA, *A Decade of Fair Balance Doctrine, and How to Fix It: Copyright Versus Fundamental Rights Before the CJEU from Promusicae to Funke Medien, Pelham and Spiegel Online,* cit. In particolare l'autrice sostiene: "*the specific subject matter of each exclusive right, could be identified on the basis of its essential social function as defined by the Directives and tailored to the particular sector or protected work involved, specifying the principle now just hinted in the recent Grand Chamber's triad. Only those acts which ensure revenues that are necessary to reach those incentivizing goals would belong to such core. And since socio-cultural objectives are also part of the essential function of EU copyright, any conduct that runs counter to their fulfillment would and should also be understood as falling outside the scope of protection. This would constitute a foreseeable benchmark against which the CJEU could conduct its essence check and the strict proportionality assessment, ensuring legal certainty while providing fact-specific balancing solutions, in line with its early case law, where the notion of essential function (or specific subject matter) was used to identify the core of exclusive rights to be preserved in the balance between copyright, fundamental freedoms and competition law principles*". Si veda inoltre C. SGANGA, *A New Era for EU Copyright Exceptions and Limitations? Judicial Flexibility and Legislative Discretion in the Aftermath of the CDSM Directive and the Trio of the Grand Chamber of the CJEU,* in *ERA Forum*, vol.21, 2020, pp.311-339, 2020, liberamente accessibile presso: «https://ssrn.com/abstract=3804228». (Ultimo accesso: 10 maggio 2022)

capitolo, che si verificheranno le maggiori tensioni fra privacy ed *enforcement* del diritto d'autore.

8. Considerazioni conclusive

In questo capitolo si è tentato di dimostrare la complessità del bilanciamento fra *l'enforcement* del diritto d'autore e la tutela dei dati personali. Concentrando primariamente la nostra attenzione sul contrasto generato dalle reti *peer-to-peer*, abbiamo fornito contezza di come, per tutelare il diritto d'autore nella dimensione dell'Internet, i *copyright holders* abbiano attuato svariate strategie in grado, come effetto collaterale, di incidere pesantemente sulla riservatezza degli utenti in rete.

Il necessario punto fermo che abbiamo dovuto tracciare è stato dato dalla constatazione che, sia negli Stati Uniti che nel contesto europeo ed italiano, sia il diritto d'autore che il diritto alla privacy devono essere considerati come diritti fondamentali e come costituzionalmente garantiti, motivo per cui abbiamo potuto affermare che, quantomeno in linea di principio, tale bilanciamento avviene fra diritti che, sulla carta, posseggono almeno il medesimo valore e riconoscimento.

Si è quindi voluto mettere in luce come si possano rinvenire quattro strategie di *enforcement* del diritto d'autore: campagne pubblicitarie, sistemi di *Digital Rights Management*, azioni volte a colpire le architetture *peer-to-peer* ed infine azioni volte a colpire gli utenti delle reti *peer-to-peer*[312].

Mentre la seconda di queste quattro strategie troverà luogo deputato alla sua analisi nel successivo capitolo, nel presente sono state affrontate sia la terza che la quarta delle strategie, ossia le azioni giudiziarie.

Per compiere ciò abbiamo necessariamente dovuto premettere una opportuna trattazione della legislazione in materia di *enforcement* del diritto d'autore e di responsabilità dei *Service Provider*. Gli strumenti analizzati sono stati quelli del DMCA "*subpoena*", dei "*John Doe proceedings*" e dell'art. 156-bis della Legge 633/1941. Da tale analisi è emerso che sia il sistema statunitense che quello euro-italiano si dimostrano particolarmente attenti agli strumenti di *enforcement* del diritto d'autore. La legislazione, tanto statunitense quanto euro-italiana, pare quasi incoraggiare, se non con apodittici richiami ad un rispetto della riservatezza, una vasta attività di monitoraggio e di sorveglianza degli utenti sulla rete, sostenendo le attività di investigazione privata da parte dei titolari del *copyright*. Esempio emblematico di ciò, come visto, è il caso Peppermint che, avvalendosi della Logistep aveva posto in essere una massiva campagna di sorveglianza di massa per scovare i "pirati" entrando, digitalmente, nei computer degli utenti. Ma non solo, gli stessi istituti di *discovery* incentivano la privatizzazione della tutela, offrendo *subpoena* o azioni cautelari volte a svelare ciò che è celato. La legislazione statunitense sembra sicuramente anteporre il *copyright* alla privacy, come confermato poi dalla giurisprudenza, mentre il sistema italiano, godendo di una forte protezione dei dati personali, porta a bilanciamenti in parte diversi.

Abbiamo quindi proceduto ad analizzare la giurisprudenza sia statunitense che euro-italiana in ambito di entrambe le strategie di *enforcement* del diritto. Punto di partenza obbligato sono state le azioni volte a colpire le reti *peer-to-peer,* prima con il caso Napser, poi Aimster e Grokster. Da questa analisi è emerso che le Corti americane sono solite affidare una

[312] R. CASO, *Il conflitto tra copyright e privacy nelle reti Peer to Peer: il caso Peppermint – Profili di diritto comparato*, cit. 5 e ss.

protezione molto intensa agli interessi dei titolari del diritto d'autore, ai limiti forse dell'esasperazione. Nell'ottica di questo elaborato, tuttavia, tale protezione rimaneva ancora nell'ambito della comprensibilità in quanto erano azioni non volte, direttamente quantomeno, a ledere la privacy degli utenti.

Con l'analisi invece delle sentenze in merito alla quarta delle strategie così delineate, si è avuto modo di dimostrare che gli utenti "pirata" delle reti *peer-to-peer* iniziarono ad essere oggetto di numerose azioni legali. Si delineava una strategia che, come abbiamo più volte ricordato, consisteva in un ricorso, da parte dei titolari del diritto d'autore, a società esterne cui era affidato il compito di scavare nella rete e nei software *peer-to-peer* alla ricerca di indirizzi IP di utenti che si supponeva avessero violato il loro monopolio. In questo senso, è tornata utile l'affermazione compiuta all'origine del presente elaborato, ossia quella per cui gli indirizzi IP degli utenti costituiscono dati personali e come tali meritano di essere protetti nel contesto digitale. Infatti, l'affidarsi alla tecnologia, la dimensione privatistica dell'autotutela, l'alleanza con il mondo degli affari, sono tutti *topoi* ricorrenti della storia dell'*enforcement* del diritto d'autore. Inoltre, non sarebbe stato possibile per i *copyright holders*, come più volte affermato, associare l'indirizzo IP dell'utente alla sua reale identità, necessaria invece per citarlo in giudizio, con conseguente bisogno della collaborazione dei *Service Provider*.

Lo strumento del §512 *subpoena*, con il caso Verizon, non ebbe molto successo per i *copyright holders*, ma per motivazioni che, come visto, erano meramente tecniche. Questo però non impedì ai titolari dei diritti d'autore di rivolgersi allo strumento del *John Doe* ed ottenere invece così piene vittorie. I "*Doe*" non potevano nemmeno sognarsi di avere una aspettativa di privacy nelle reti *peer-to-peer* secondo la giurisprudenza americana. Un'argomentazione tanto retorica quanto criticabile.

Diverso è stato l'esito del bilanciamento nel caso Peppermint: la privacy degli utenti aveva avuto la meglio. Comparativamente, infatti, emerge che solo in Italia il bilanciamento pare essere avvenuto fra diritti di pari rango. La stessa presenza dell'Autorità Garante dei dati personali in Italia dimostra l'attenzione del nostro Stato per la protezione della riservatezza e della vita privata. Il nostro ordinamento costituzionale non pareva lasciare spazio alla sorveglianza degli utenti online, quantomeno non nelle controversie civili. Si esigeva un superiore interesse pubblico, in sostanza, per ottenere le identità degli utenti.

La giurisprudenza europea, solitamente feroce quando si tratta di protezione dei dati personali o di tutela della proprietà intellettuale, si dimostra invece, in un primo tempo, abbastanza remissiva. I Casi Promusicae e Bonnier Audio, per quanto utili nell'affermare la qualità di diritti fondamentali per entrambi quelli di cui il presente elaborato si occupa, e sebbene riconoscano l'imprescindibilità di un serio bilanciamento che tenga veramente in conto tutte le esigenze del caso, rimettono la questione all'apprezzamento del giudice nazionale, senza fornire un serio criterio di risoluzione delle controversie se non quello dell'attenzione al caso concreto. Più di recente invece, con i casi Pirate Bay e Mircom, la Corte arriva, secondo l'analisi qui proposta, a dimenticarsi progressivamente delle tutele che devono essere fornite agli utenti alla luce delle normative europee in tema di trattamento dei dati personali, arrivando a conclusioni che, sebbene non in aperto contrasto con quelle nazionali emergenti dalla vicenda Peppermint, nei fatti si oppongono a tali conclusioni.

Lo spettro della sorveglianza non accenna ad arrestarsi, tanto che con le sentenze Scarlet Extended v. Sabam e Sabam v. Netlog, l'intento del ricorrente era proprio quello di imporre un regime di perenne e costante monitoraggio delle attività online di tutti gli utenti e, sebbene dichiarato contrario al diritto europeo, la posizione non appare immutabile. Le regole ora disposte dall'art. 17 della *Direttiva Copyright*, che dice più di quanto non vi sia scritto,

e l'intensificarsi delle tecnologie di DRM, come vedremo nei due capitoli successivi al presente, portano l'interprete a ragionare nel senso opposto rispetto a quello della Corte.

Senza voler proporre previsioni aleatorie di come il bilanciamento si evolverà nel prossimo futuro e non volendo usurpare né il ruolo del legislatore, né quello del giudice del caso concreto, l'intento del presente capitolo può dirsi compiuto nell'aver dimostrato la sicura difficoltà ma anche l'imprevedibilità dei bilanciamenti compiuti dalle Corti nazionali e sovranazionali. I ragionamenti fin ora apprestati dalla giurisprudenza sono forse poco soddisfacenti ed ancor meno coraggiosi, le disposizioni di legge contraddittorie in molti aspetti e non pare che da alcuna parte giunga un criterio effettivo di soluzione di questo secolare conflitto fra autori e pirati, fra il pugno di ferro *dell'enforcement* dei diritti d'autore ed il grido di tutela degli utenti. Una prospettiva sinceramente desolante.

CAPITOLO TERZO

I SISTEMI DI DIGITAL RIGHTS MANAGEMENT: TRA IL TECNOLOGICO ED IL GIURIDICO

1. Il Digital Rights Management: un'introduzione

La terza parte di questo elaborato prosegue nell'analisi del delicato bilanciamento fra *l'enforcement* del diritto d'autore e la tutela della privacy in un punto in cui massimamente si percepisce la frizione fra i due: nei sistemi di *Digital Rights Management* (DRM). Ricordando quando affermato in principio del capitolo precedente, delle quattro strategie che i titolari dei diritti d'autore possono attuare per la tutela delle proprie opere nel web, quelle riguardanti le azioni giudiziarie volte a colpire i sistemi di *file-sharing* e quelle volte a colpire gli utenti sono già state oggetto di precedente analisi. Ora invece preme dare enfasi a quella strategia consistente nella "*produzione di sistemi di Digital Rights Management (DRM) che abilitano la gestione ed il commercio di file associati a misure tecnologiche di protezione che, tra l'altro, possono impedire la copia e la distribuzione non autorizzate*[313]"

Nel passaggio dall'analogico al digitale, la carta si trasforma in *bit* e le opere dell'ingegno diventano idonee ad essere rappresentate in una somma di 0 e di 1, ossia in codice binario. Il *corpus mechanicum* ed il *corpus mysticum* si fondono inesorabilmente in un panorama connotato da una costante dematerializzazione[314]. Tale trasformazione, come ricorda Roberto Caso, si associa alla comparsa di *software* ed *hardware* in grado di gestire la produzione e la distribuzione dell'informazione [315] in funzione di protezione della proprietà intellettuale e quindi di *enforcement* dei diritti dei *copyright holders*.

In questa sezione, dunque, dopo una prima notazione sulla qualificazione dei sistemi di *Digital Rights Management* come metodi di *enforcement* del diritto d'autore, angolo di visuale privilegiata nel presente elaborato, si passerà all'analisi della disciplina legale in materia, sia nel panorama statunitense che in quello nazionale. In ultima battuta verranno proposte considerazioni in chiave di bilanciamento con il diritto alla privacy degli utenti, tentando di mostrare quali soluzioni gli Stati possano adottare per frenare le derive tecnologiche più evidenti.

In chiusura del precedente capitolo, infatti, abbiamo affermato che lo spettro della sorveglianza non accenna ad arrestarsi ed esempio di questo è sicuramente offerto dalle tecnologie di gestione dei contenuti digitali protetti dal diritto d'autore. Come avremo modo di spiegare maggiormente, i sistemi di DRM solitamente comprendono flussi di dati personali in uscita dai supporti digitali degli utenti, in particolare con riferimento a tutte quelle informazioni sull'uso dei contenuti offerti digitalmente[316]. Questi sistemi, infatti, consentono un costante monitoraggio dei consumi intellettuali degli utenti, principalmente a scopi di profilazione. Tale monitoraggio, oltre a costituire un trattamento dei dati personali sulla cui liceità si possono sollevare dubbi, comporta anche una compressione della libertà e

---

313 R. CASO, *Il conflitto tra copyright e privacy nelle reti Peer to Peer: il caso Peppermint – Profili di diritto comparato,* cit. 5 e ss.

314 Per riferimenti al fenomeno della dematerializzazione si veda G. PASCUZZI (a cura di*), Il diritto nell'era digitale,* cit., 341 e ss.; R. ROMANO, *L'opera e l'esemplare nel diritto della proprietà intellettuale*, Padova, 2001; nonché P. SPADA, *Copia privata ed opere sotto chiave*, in *Riv. dir. ind.*, 2002, I, 591, 600.

315 R. CASO, *Digital rights management: il commercio delle informazioni digitali tra contratto e diritto d'autore,* Padova, 2004, 1, liberamente accessibile presso: «http://eprints.biblio.unitn.it/4375/» (Ultimo accesso: 10 maggio 2022).

316 R. CASO, *Digital rights management: il commercio delle informazioni digitali tra contratto e diritto d'autore,* cit., 66 e ss.

dell'autodeterminazione nel consumo intellettuale degli utenti con conseguenze sulla riservatezza e sulla libertà di estrinsecazione della personalità degli stessi.

2. Quid est? Chiarimenti terminologici

Sin dalle prime battute di questa dissertazione, una delle linee direttrici che abbiamo avuto modo di tracciare, partendo dall'analisi storica degli istituti di proprietà intellettuale, è sicuramente quella della stretta alleanza degli interessi protetti dal diritto d'autore con il mondo degli affari. Nel contesto del *Digital Rights Management* questa connessione si mostra all'evidenza: i titolari dei diritti d'autore si rivolgono alle industrie tecnologiche ed informatiche per creare un nuovo sistema di *enforcement* dei loro diritti, procedendo ad attuare modelli di controllo e di gestione dell'uso e del consumo delle opere dell'ingegno. A distanza di un secolo dall'introduzione dei furgoncini della BBC, capaci di triangolare la posizione degli ascoltatori pirata, la strategia si è raffinata ma nei fatti rimane la stessa: affidarsi alla tecnologia per combattere la pirateria.

Prima di profondersi in considerazioni giuridiche sulla problematicità di questa alleanza, è bene partire da alcune definizioni di base. Come ricordano Rosenblatt e Dykstra[317], il termine "*Digital Rights Management*" iniziò ad essere usato negli anni '90 in connessione alla diffusione di Internet. In senso lato, con tale nome, si fa riferimento a quei "*sistemi tecnologici in grado di definire, gestire, tutelare ed accompagnare le regole di accesso e di utilizzo su contenuti digitali*"[318]

Il punto cruciale di questi sistemi di gestione dei diritti è il fatto che essi agiscono in via automatica, senza richiedere, nel loro funzionamento, un intervento umano al di fuori di quello iniziale di ideazione. Infatti, tali sistemi sono in grado di eseguire contratti e di sanzionarne eventuali violazioni in automatico, in via, diremmo, di "autotutela". La finalità primaria di queste tecnologie, nel campo del *copyright*, è quella che viene chiamata di "*persistent protection*". Infatti, i processi di controllo e gestione dell'accesso ai contenuti sono volti ad ottenere una forma di protezione permanente delle opere protette da diritto d'autore[319]. In tal modo il prodotto dell'ingegno potrà essere schermato da attività illecite che sullo stesso possano andare ad incidere dal momento della sua creazione e per un tempo non definito.

Ma quali sono le ragioni che spingono un titolare dei diritti d'autore a implementare i prodotti da esso distribuiti con sistemi e tecnologie di *Digital Rights Management*? Sicuramente si deve concordare con quella dottrina che afferma che "*il diritto d'autore è la risposta normativa ad un fallimento del mercato, ovvero ad una situazione in cui i normali meccanismi di mercato non riescono a garantire una efficiente allocazione delle risorse. Nel caso di beni oggetto di proprietà intellettuale tale situazione si verifica per la loro particolare natura di beni pubblici, ovvero di beni connotati dalle caratteristiche della non-rivalità e della non-escludibilità*"[320].

---

[317] B. ROSENBLATT, G. DYKSTRA, *Integrating Content Management with Digital Rights Management: Imperatives and Opportunities for Digital Content Lifecycles,* 2003, liberamente accessibile presso: «https://robertoigarza.files.wordpress.com/2010/03/art.-integrating-content-management-with-digital-rights-management-vvaa-2003.pdf» (Ultimo accesso: 10 maggio 2022).

[318] Così riportato in R. CASO, *Digital rights management: il commercio delle informazioni digitali tra contratto e diritto d'autore*, cit., 5, con riferimento a B. ROSENBLATT, G. DYKSTRA, *Integrating Content Management with Digital Rights Management: Imperatives and Opportunities for Digital Content Lifecycles,* cit. 4-5; viene definito come "*a content management system is one that stores digital content for search, browsing, access, and retrieval by users in a workgroup or enterprise*"

[319] Per maggiori informazioni si veda R. CASO*, Digital rights management: il commercio delle informazioni digitali tra contratto e diritto d'autore*, cit., 6.

[320] G. SPEDICATO, *Le misure tecnologiche di protezione del diritto d'autore nella normativa italiana e comunitaria* in *Ciberspazio e diritto*, 2006, fasc. 4., 535 - 580. In riferimento si veda anche A. FLORIO, *I sistemi di Digital Rights*

In prospettiva di analisi economica del diritto, infatti, tale natura dei beni intellettuali comporta che i costi fissi per la produzione dell'informazione originale siano molto elevati mentre i costi marginali di distribuzione siano bassi. Questa peculiare posizione incentiva una prassi definibile in termini di "*free riding*", la quale produce un fallimento del mercato. Per arginare tale fallimento allora gli Stati hanno proposto la costruzione artificiale di un monopolio sull'informazione.

Nel mondo digitale, tuttavia, la facilità di duplicazione dei file comporta, fra i monopolisti del diritto d'autore, una preoccupazione per le possibilità offerte dal web in termini di pirateria. Infatti, come nota un'attenta dottrina, "*gli straordinari traguardi raggiunti nel corso degli ultimi decenni nell'ambito delle tecnologie dell'informazione e della comunicazione hanno prima contribuito al sorgere ed allo sviluppo della società dell'informazione e dell'economia della conoscenza, infondendo nuova linfa al ruolo dei diritti di proprietà intellettuale, poi hanno messo a disposizione di tutti strumenti sempre più semplici ed economici per violare proprio quei diritti a cui avevano restituito centralità*"[321].

Infatti, come ricordano Rosenblatt e Dykstra[322], "*la pirateria, che si tratti di software, musica, film, immagini o testo, costa miliardi di dollari ogni anno. Oltre a drenare le entrate aziendali, la pirateria spreca tempo e risorse preziose delle aziende richiedendo sforzi costosi per rilevare e scoraggiare i furti. Inoltre, la pirateria diffusa crea un'atmosfera di sfiducia che può diventare controproducente per lo sviluppo di nuovi modelli di business per i contenuti digitali; si traduce in prodotti che sono meno intuitivi (*user-friendly*) di quanto potrebbero essere altrimenti*[323]". La reazione a questa preoccupazione è stata quindi, fra le altre già analizzate nel precedente capitolo, l'introduzione di misure tecnologiche di protezione dei diritti d'autore.

In chiave economica e tecnologica, il DRM è innanzitutto definibile in termini di "*business model*" che "*delinea una serie di regole, alle quali ciascun soggetto della catena di produzione e distribuzione del contenuto digitale deve attenersi per avere accesso e per ottenere determinate forme di fruizione del contenuto stesso*[324]". I sistemi di DRM sono quindi estrinsecazione del potere tecnologico che si lega a filo doppio con le strategie di *enforcement* del *copyright* sulla rete. Infatti, tramite i sistemi di DRM i titolari dei contenuti digitali traducono direttamente nei fatti le clausole stabilite nelle licenze d'uso, imponendo quindi contrattualmente regole di accesso e di utilizzo dei contenuti, ma al contempo anche prevedendo meccanismi sanzionatori direttamente attuati dalle tecnologie stesse.

In via generale possiamo affermare, come nota Tripaldi, che "*nella pratica un sistema DRM consente: (1) di definire un set di regole (il business model) in accordo alle quali le diverse componenti del sistema opereranno per consentire ai soli utenti autorizzati l'accesso ai contenuti; (2) di gestire l'intermediazione distributiva qualora vi siano soggetti terzi tra il titolare di contenuti e l'utente finale; (3) di*

Management (DRM) in *dirittodellinformatica.it,* 2009, disponibile sul sito: «https://www.dirittodellinformatica.it/diritto-autore/*copyright*-focus/i-sistemi-di-digital-rights-management-drm.html» (Ultimo accesso: 10 maggio 2022).

321 G. SPEDICATO, *Le misure tecnologiche di protezione del diritto d'autore nella normativa italiana e comunitaria,* cit., 535 - 580.

322 Cfr. B. ROSENBLATT, G. DYKSTRA, *Integrating Content Management with Digital Rights Management: Imperatives and Opportunities for Digital Content Lifecycles*, 2003, cit., 8.

323 Nella versione originale il testo dispone: "*Piracy, whether of software, music, film, images, or text, costs billions of dollars each year. Besides draining corporate revenues, piracy squanders valuable company time and resources by requiring costly efforts to detect and deter theft . Further, widespread piracy creates an atmosphere of distrust that can become counterproductive to developing new business models for digital content; it results in content-based products that are less user- friendly than they might otherwise be*"

324 G. TRIPALDI, *Digital Rights Management: come affrontare la salvaguardia del Copyright nell'era digitale*, in *BorsaItaliana.it*, 2002, 8, citato da R. CASO, *Digital rights management: il commercio delle informazioni digitali tra contratto e diritto d'autore*, cit., 6.

contabilizzare gli accessi ai contenuti e le relative spettanze di tutti i soggetti coinvolti lungo la catena; (4) di codificare i contenuti all'origine e decodificarli nell'uso finale in funzione della validità della licenza digitale in possesso dell'utente e con le modalità da questa contemplate; (5) di presidiare la distribuzione delle licenze/certificati digitali a chi, in funzione del pagamento in una qualche forma predefinita di retribuzione desideri accedere ad un contenuto".[325]

Come poi ricorda Roberto Caso, il business model del DRM prevede diritti di utilizzo del contenuto digitale articolati in tre principali gradi di libertà[326]: (1) il trasferimento del contenuto, che contempla anche diritti di duplicazione, cessione e prestito; (2) il suo riutilizzo da parte di soggetti intermedi; (3) le modalità di fruizione finale. Per quanto riguarda queste ultime, si nota come le modalità di fruizione possono essere tanto la creazione di una copia permanente quanto una visione del materiale o una sua esecuzione. In ogni caso, ciascuna di queste fruizioni si articola come una combinazione di tre fattori. In primo luogo, si prende a riferimento l'"estensione" dei diritti in termini temporali e quantitativi, in secondo luogo la "categoria" di utenti finali che possono essere ad esempio paganti o meno, ed infine il "contraccambio" ossia la prestazione richiesta per ottenere la fruizione. Chiaramente, in questo ultimo caso, la prestazione può consistere tanto in una dazione pecuniaria quanto anche nel pagamento attraverso dati personali, ossia tramite registrazione.

Incidenter tantum, è infatti sempre da ricordare che la registrazione presso piattaforme online non è mai gratuita: i dati personali rappresentano una nuova moneta nel mondo digitale. Si ricordi, ad esempio, la recente vicenda che ha coinvolto *Facebook*, condannato per pratica commerciale ingannevole, per aver pubblicizzato la sua nota piattaforma social come gratuita, senza invece considerare che la cessione dei dati integra una controprestazione, atteso che il 98% del fatturato della società derivava dalla pubblicità on line basata proprio sulla profilazione degli utenti[327].

Per ottenere i risultati sperati dai produttori dei sistemi, nonché dai *copyright holders*, le varie componenti, *software* ed *hardware*, che integrano i sistemi di *Digital Rights Management,* devono combinarsi traducendo il linguaggio naturale o giuridico in *bit* e procedere a imporre regole comportamentali agli utenti nella fruizione dei contenuti protetti dal diritto d'autore. Chiaramente questo è il maggior ostacolo al corretto funzionamento di questi sistemi, nonché motivo di principale preoccupazione per un contesto come quello del diritto d'autore, ma forse di tutto il diritto, in cui i diritti e gli interessi raramente si prestano ad essere ridotti ad algoritmo. Un simile tipo di linguaggio è quello conosciuto come *REL* ossia come *Rights Expression Language* che si inserisce nel più ampio panorama del c.d. "*Semantic Web*"[328].

Solitamente i REL sono espressi in formato XML e sono comunemente incorporati sotto forma di metadati entro altri documenti come, ad esempio, i libri digitali (ebook), i file audio MP3 o i video scaricabili. In informatica, l'XML (sigla di *eXtensible Markup Language*, ossia

---

[325] G. TRIPALDI, *Digital Rights Management: come affrontare la salvaguardia del Copyright nell'era digitale*, in *BorsaItaliana.it*, 2002, 8, citato in nota da R. CASO, *Digital rights management: il commercio delle informazioni digitali tra contratto e diritto d'autore*, cit., 6.

[326] R. CASO, *Digital rights management: il commercio delle informazioni digitali tra contratto e diritto d'autore*, cit., 12 e ss.

[327] In tal senso si è infatti espresso il Consiglio di Stato in relazione alla sanzione amministrativa comminata dalla AGCM con sentenza con la sentenza del 29 marzo 2021 n. 2631, liberamente consultabile presso: «https://images.go.wolterskluwer.com/Web/WoltersKluwer/%7B347864f1-da38-428d-b434-12a07cbf5df5%7D_consiglio-di-stato-sentenza-2631-2021.pdf?_gl=1%2Asl2goh%2A_ga%2ANjc4MDM1MTQ0LjE2NDI3NzM2OTI.%2A_ga_B95LYZ7CD4%2AMTY0MzcwMzY3Ni4xMC4xLjE2NDM3MDM3MDIuMA..&_ga=2.158164922.1240605098.1643703677-678035144.1642773692» (Ultimo accesso: 10 maggio 2022).

[328] Per maggiori informazioni si veda R. CASO, *Digital rights management: il commercio delle informazioni digitali tra contratto e diritto d'autore*, cit., 14 e ss., e la bibliografia ivi rinvenibile in merito.

"linguaggio di marcatura estendibile") è un metalinguaggio per la definizione di linguaggi di markup, ovvero basato su un meccanismo sintattico che consente di definire e controllare il significato degli elementi contenuti in un documento o in un testo[329]. *L'XrML*, eXtensible Rights Markup Language basato sui marcatori XML, traduce in una lingua comprensibile alla macchina disposizioni della natura di cui trattiamo. In particolare, Roberto Caso nota che esso è un linguaggio che si basa sull'idea del trusted systems. "*I trusted systems sono, da un punto di vista concettuale, rappresentati da "black boxes" che rendono disponibile un contenuto alle condizioni poste da chi controlla i sistemi stessi. Il problema di fondo è che sistemi di questo genere necessitano di un modo formale e standardizzato per specificare le condizioni alle quali subordinare la disponibilità del contenuto. Tale modo costituisce appunto un REL, cioè un linguaggio in grado di esprimere "diritti"*[330].

Le tecnologie di base, come di seguito vedremo, per il funzionamento dei sistemi di *Digital Rights Management* sono principalmente la crittografia, il *watermarking* ed il *fingerprinting* su cui si tornerà partitamente per analizzarne il funzionamento.

L'applicazione dei sistemi di *Digital Rights Management* che ci interessa più da vicino in questo contesto è sicuramente quella in merito al diritto d'autore, sebbene non sia l'unica area del reale investita da questa forma tecnologica. Le limitazioni, in campo di proprietà intellettuale, che il DRM può comportare riguardano sicuramente, ad esempio, limiti di tempo a disposizione per la fruizione di un contenuto, o le forme di utilizzo o la possibilità di fruizione solo in determinate aree geografiche.

A differenza delle precedenti strategie di *enforcement* del diritto d'autore volte a colpire gli utenti o le piattaforme di *file-sharing*, nel campo dei CD ad esempio, come prima per le videocassette, cercare di colpire i produttori di stereo o di computer era materialmente controproducente. Al tempo stesso, mentre identificare gli utenti sulle reti *peer-to-peer* tramite gli indirizzi IP era tecnologicamente possibile, cercare di colpire gli utenti che si scambiavano CD o DVD fra amici per compierne copie private era materialmente impossibile. Il c.d. "*CD Burning*", ossia la copia di un disco su un altro tramite un software, non poteva essere raggiunto dalle azioni legali dei titolari dei diritti d'autore, motivo per cui si decise di procedere tramite i sistemi di *Digital Rights Management*, creando soluzioni tecniche volte a impedire la copia[331].

Tali misure di *enforcement* del diritto d'autore sollevano numerose preoccupazioni, sia sul versante della protezione del *copyright* che su quello del trattamento dei dati personali. I bilanciamenti che si giocano in questo contesto sono particolarmente precari. Chiaramente, non ogni attività attuabile tecnologicamente è per ciò solo lecita, anche il diritto d'autore infatti, come ben sappiamo, ha i suoi limiti.

Il diritto d'autore, sin dalla sua nascita, ha dovuto confrontarsi con altre esigenze, di natura non meramente economica, come i diritti alla informazione, allo studio, alla ricerca ed in definitiva al libero accesso alle opere dell'ingegno. Ciò ha condotto a creare un bilanciamento fra opposte esigenze, ponendo limiti al diritto monopolistico dell'autore attraverso eccezioni all'utilizzo altrimenti illecito del materiale protetto da *copyright*.

---

[329] Per maggiori informazioni si veda A. CHIARELLI, *XML Schema e Documenti XML*, su *HTML.it,* liberamente accessibile presso il sito: «https://www.html.it/articoli/xml-schema-e-documenti-xml/» (Ultimo accesso: 10 maggio 2022).

[330] R. CASO, *Digital rights management: il commercio delle informazioni digitali tra contratto e diritto d'autore*, cit., 37.

[331] Per maggiori informazioni in merito si veda M.M. LA BELLE, *The 'Rootkit Debacle': The Latest Chapter in the Story of the Recording Industry and the War on Music Piracy* (2006), in *Denver University Law Review*, Vol. 84, No. 1, 2006, 79, CUA Columbus School of Law Legal Studies Research Paper No. 2010-28, liberamente accessibile presso: «https://ssrn.com/abstract=1564903» (Ultimo accesso: 10 maggio 2022).

In primo luogo, come affermato, l'uso dei DRM consente, grazie alla *permanent protection* che offre, di garantire un monopolio duraturo ai titolari del diritto d'autore così ponendosi in aperto conflitto con il principio dell'esaurimento del diritto[332]. In base a tale principio, infatti, il titolare dei diritti d'autore sull'opera, dopo la prima vendita di un esemplare della stessa, perde il diritto di controllare l'ulteriore distribuzione di quell'esemplare.

In merito si può ricordare come l'ordinamento comunitario disponga all'articolo 4 della Direttiva 2001/29 che "*Gli Stati membri riconoscono agli autori il diritto esclusivo di autorizzare o vietare qualsiasi forma di distribuzione al pubblico dell'originale delle loro opere o di loro copie, attraverso la vendita o in altro modo. Il diritto di distribuzione dell'originale o di copie dell'opera non si esaurisce nella Comunità, tranne nel caso in cui la prima vendita o il primo altro trasferimento di proprietà nella Comunità di detto oggetto sia effettuata dal titolare del diritto o con il suo consenso*".

Del pari, la "*first sale doctrine*" statunitense, oggi racchiusa nella Section 17 U.S.C §109 (a) dispone che in deroga alle disposizioni della Section §106(3) (concernente il diritto di distribuzione), il proprietario di una particolare copia o registrazione legalmente realizzata, o qualsiasi persona autorizzata da tale proprietario, ha il diritto, senza l'autorità del titolare del *copyright*, di vendere o altrimenti disporre del possesso di tale copia o registrazione[333].

Ne consegue che, per l'operare di simili principi, un sistema di *Digital Rights Management* che dovesse procedere a mantenere un controllo sulle opere anche in seguito alla loro vendita sarebbe contrario a tale principio.

Tuttavia, tale principio viene tradito dalle stesse parole del legislatore sia comunitario che conseguentemente nazionale in quanto il requisito della materialità, precisato dal Considerando 28 della Direttiva 29/2001, afferisce specificamente al diritto di distribuzione. Il legislatore comunitario distingue infatti fra le copie realizzate a partire dalla messa a disposizione del pubblico dell'opera "*in maniera tale che ciascuno possa avervi accesso dal luogo e nel momento scelti individualmente*", e le copie materiali dell'opera stessa. La differenza comporta un differente regime giuridico tale per cui, nel caso di opere digitali, il titolare dei diritti d'autore mantiene un potere di controllo dei successivi atti di trasferimento. In tal senso, infatti, la realizzazione di tali copie non comporta l'esaurimento del diritto di distribuzione, come sancito espressamente dal terzo comma dell'art. 17 della legge 633/1941.

Il problema relativo all'esaurimento è poi dipendente anche dalla qualificazione dei contratti con cui le copie di una certa opera vengono messe a disposizione. Ove si qualificasse tale accordo di licenza come rientrante nel *genus* della compravendita, ne conseguirebbe una piena applicazione del principio dell'esaurimento. Alternativamente, ove la licenza fosse qualificabile come locazione, allora il principio non avrebbe esplicazione[334].

---

[332] Per maggiori informazioni in merito si veda: A. FLORIO, *I sistemi di Digital Rights Management (DRM)* in *dirittodellinformatica.it*, cit.

[333] Il testo normativo in particolare dispone: "*Notwithstanding the provisions of Section 106(3), the owner of a particular copy or phonorecord lawfully made under this title, or any person authorized by such owner, is entitled, without the authority of the copyright owner, to sell or otherwise dispose of the possession of that copy or phonorecord".*

[334] Per maggiori riferimenti in merito alla qualificazione giuridica delle licenze d'uso si veda P. GUARDA, *Meraviglioso come a volte ciò che sembra non è: la qualificazione giuridica del contratto,* in T. PASQUINO (a cura di), *Antologia di Casi Giurisprudenziali, Materiali per lo studio del diritto privato*, seconda edizione, Torino, 2015. Notazioni in merito rinvenibili presso CGUE 3 luglio 2012, C- 128/11, *UsedSoft GmbH/ Oracle International Corp.*, Grande Sezione, liberamente consultabile presso: «https://curia.europa.eu/juris/document/document.jsf?docid=124564&doclang=IT» (Ultimo accesso: 10 maggio 2022) il cui principio di diritto dispone che "*l'articolo 4, paragrafo 2, della Direttiva 2009/24/CE del Parlamento europeo e del Consiglio, del 23 aprile 2009, relativa alla tutela giuridica dei programmi per elaboratore, deve essere interpretato nel senso che il diritto di distribuzione della copia di un programma per elaboratore è esaurito qualora il titolare del*

In secondo luogo, poi, il controllo permanente esercitato per mezzo dei sistemi di *Digital Rights Management* potrebbe comportare una compressione della portata delle eccezioni e delle limitazioni poste al diritto d'autore[335]. Infatti, alcune attività, che in assenza di previsione normativa apposita sarebbero illecite ai sensi della normativa sui diritti di proprietà intellettuale, sono dal legislatore considerate lecite in ragione di valutazioni di bilanciamento e di equilibrio fra gli interessi economici monopolistici dei titolari dei diritti e altre esigenze quali quelle alla ricerca, alla libertà di pensiero, alla critica. Tuttavia, è critica comune quella per cui gli algoritmi e i codici binari non sarebbero in grado di distinguere fra un uso lecito ed un uso illecito, tanto che, come vedremo, il legislatore è stato disposto a sacrificare i diritti degli utenti in ragione del funzionamento di questi sistemi.

Molti sono i limiti che comprimono l'egemonia del diritto d'autore, basti ricordare che il potere derivante dai diritti autorali è garantito solo ad opere originali, copre solo le forme espressive e non le idee, e ad un certo momento, per quanto lontano, il diritto si estingue e l'opera cade nel pubblico dominio.

In terzo luogo mentre i diritti morali relativi al diritto d'autore non sono soggetti a limitazioni temporali (art. 23 L. 633/41), i diritti di utilizzazione economica dell'opera sono soggetti a precisi limiti di durata. In base alla regola generale contenuta nell'art. 25 L. 633/41 "*i diritti di utilizzazione economica dell'opera durano tutta la vita dell'autore e sino al termine del settantesimo anno solare dopo la sua morte*". Tuttavia, il concetto di protezione permanente non contempla, di per sé, una limitazione temporale al suo funzionamento, sebbene naturalmente la tecnologia sia soggetta ad un invecchiamento molto veloce che non ha ancora condotto a uno scontro frontale fra queste disposizioni.

Roberto Caso, infatti, nota in merito come "*tali protezioni usualmente non vengono programmate con una scadenza temporale. Finora la storia ha dimostrato che la tenuta di questa tecnologia non è effettivamente perpetua. Col tempo, infatti, emergono tecnologie in grado di eludere le protezioni. Tuttavia, il fatto che non sia programmata una scadenza temporale mina alla base la certezza e la prevedibilità della regola tecnologica. Un risultato tanto più devastante nel settore della proprietà intellettuale, che fa della certezza e della prevedibilità dei limiti temporali un proprio cardine*" [336].

In tale ambito il DRM può essere utilizzato per "*provvedere in modo totalmente o parzialmente automatizzato all'identificazione ed alla negoziazione dei diritti sulle opere, al monitoraggio del loro utilizzo ed alla loro protezione contro usi o attività non consentiti dal titolare dei diritti o non previste in via contrattuale*"[337].

Le licenze che servono a commercializzare i prodotti hanno genericamente la pretesa di mantenere il controllo sul prodotto digitalmente immesso nel mercato[338]. In questo senso, generalmente le clausole contrattuali delle licenze d'uso stabiliscono un divieto di eludere le misure di protezione, nonché attribuiscono al fornitore il potere di revocare la possibilità d'uso del contenuto in via di autotutela in presenza di violazioni delle condizioni d'uso.

---

diritto d'autore che abbia autorizzato, foss'anche a titolo gratuito, il download della copia su un supporto informatico via Internet abbia parimenti conferito, a fronte del pagamento di un prezzo diretto a consentirgli l'ottenimento di una remunerazione corrispondente al valore economico della copia dell'opera di cui è proprietario, il diritto di utilizzare la copia stessa, senza limitazioni di durata".

335 Per maggiori informazioni in merito si vedano: A. FLORIO, *I sistemi di Digital Rights Management (DRM)* cit.; R. CASO, *Digital rights management: il commercio delle informazioni digitali tra contratto e diritto d'autore,* cit., 160 e ss.

336 R. CASO, *Digital rights management: il commercio delle informazioni digitali tra contratto e diritto d'autore,* cit., 98.

337 G. SPEDICATO, *I Digital Rights Management System tra produzione e diffusione di opere dell'ingegno. Quale nuovo assetto per il diritto d'autore?,* in *Ciberspazio e diritto*, vol. 5, n. 3, 2004, 273-302.

338 R. CASO, *Digital rights management: il commercio delle informazioni digitali tra contratto e diritto d'autore*, cit., 170 e ss.

Emerge evidentemente come i sistemi di DRM implichino dei flussi di dati non solo in entrata, come ad esempio gli aggiornamenti dei sistemi, ma anche in uscita dai supporti digitali degli utenti. Il riferimento è a tutte quelle informazioni hardware, ma anche informazioni sull'uso del software con potenziale danno alla privacy degli utenti. Questi sistemi infatti consentono un costante monitoraggio dei consumi intellettuali degli utenti, principalmente a scopi di profilazione.

I sistemi di DRM sono quindi estrinsecazione del potere tecnologico che si lega a filo doppio con le strategie di *enforcement* del *copyright* sulla rete. Tramite i sistemi di DRM i titolari dei contenuti digitali traducono direttamente nei fatti le clausole stabilite nelle licenze d'uso, imponendo quindi contrattualmente regole di accesso e di utilizzo dei contenuti ma al contempo anche prevedendo meccanismi sanzionatori direttamente attuati dalle tecnologie stesse. Infatti, grazie ai meccanismi di monitoraggio, il sistema di DRM è in grado di conoscere l'uso che l'utente compie del contenuto e se tale uso non risulta conforme a quanto stabilito dalle clausole, il sistema provvede direttamente a sanzionare l'utente, per esempio, disabilitando l'accesso dello stesso al contenuto.

È quindi evidente che l'ultima notazione problematica riguardi proprio la dimensione della tutela dei dati personali, su cui si avrà modo di tornare approfonditamente. Tali tecnologie, infatti, permettono di monitorare i comportamenti degli utenti e dei consumatori dei prodotti intellettuali, consentendo ai sistemi di DRM di entrare nella loro vita privata e negli spazi destinati al consumo intellettuale che si strutturano come luoghi seclusi al pubblico.

Il diritto comunitario è consapevole di queste possibili ingerenze nella privacy degli utenti tanto che, al Considerando 57 della Direttiva 2001/29/CE, fa riferimento all'allora vigente Direttiva sulla privacy, affermando che le misure tecnologiche in oggetto devono presentare, nelle loro funzioni tecniche, meccanismi di salvaguardia della vita privata, come previsto dalla Direttiva 95/46/CE.

Come vedremo, l'attuale Codice Privacy ed il GDPR consentono una limitata tutela dell'utente verso le forme più invasive di profilazione. Infatti, l'articolo 22 del GDPR dispone che l'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona. Il riferimento, in conclusione al capitolo, verrà anche posto sulle misure tecnologiche idonee ad implementare un sistema di tutela della privacy direttamente a livello di DRM, attraverso le c.d. PETs (*Privacy Enhancing Technologies*).

In definitiva, gli strumenti di *Digital Rights Management* conferiscono ai titolari dei diritti d'autore una nuova strategia di *enforcement* che si struttura come un potere formalmente contrattuale che tuttavia, come nota Roberto Caso, si pone al confine fra contratto e norma[339]. Tramite il DRM si riesce infatti a regolamentare unilateralmente ogni uso che gli utenti fanno dei contenuti, spesso tramite tecniche poco trasparenti per la generalità dei consociati e con modalità automatiche di negoziazione quali l'accettazione di condizioni contrattuali che, spesso, non vengono nemmeno lette da chi accetta. La finalità ultima è la conformazione di ogni tipo di utilizzo del contenuto digitale.

L'ultima frontiera dello sviluppo del *Digital Rights Management* nel panorama online pare essere, come vedremo, l'adozione di misure di riconoscimento dei contenuti nelle piattaforme online. Infatti, la tutela del diritto d'autore si sta combattendo proprio su

[339] R. CASO, *Digital rights management: il commercio delle informazioni digitali tra contratto e diritto d'autore*, cit., 69 e ss.

piattaforme come *YouTube* o come *Facebook*, in cui si vuole impedire l'uso non autorizzato di contenuti protetti dal diritto d'autore da parte degli utenti. La tematica è di stretta attualità, infatti il successivo capitolo, occupandosi specificamente della nuova Direttiva 2019/790, mostrerà come siano proprio queste tecnologie al centro del dibattito in tema di *enforcement* del diritto d'autore. Il Considerando 66 di tale Direttiva è esplicativo quando dispone che "*nel valutare se un prestatore di servizi di condivisione di contenuti online ha compiuto i massimi sforzi nel rispetto di elevati standard di diligenza professionale di settore, occorre considerare se il prestatore di servizi abbia adottato tutte le misure che un operatore diligente adotterebbe per ottenere il risultato di impedire la disponibilità di opere o altri materiali non autorizzati sul suo sito web, tenendo conto delle migliori pratiche del settore e dell'efficacia delle misure adottate alla luce di tutti i fattori e sviluppi pertinenti, nonché del principio di proporzionalità*". Questi massimi sforzi altro non sono, come vedremo, che tecnologie di *Automatic Content Recognition*.

Sebbene quindi la veste sia quella contrattuale, nei fatti tali disposizioni assumono funzioni di norme. Parte della dottrina ha infatti notato come il carattere preventivo del controllo differenzi una regola "rafforzata" tecnologicamente da una normale regola giuridica che, per non essere vuota declamazione, chiede mezzi, *ex post*, per essere fatta valere. Invece, "*la regola tecnologica è rigida ed opera ex ante: è chi costruisce il DRM a decidere la distinzione tra contenuto protetto e contenuto libero, tra usi consentiti e usi non consentiti, e così via*"[340]. Ed è allora in questo limbo fra la norma ed il contratto che la nostra analisi deve proseguire, in particolare verificando come la legislazione, sia statunitense che euro-italiana, affronti le preoccupazioni così emerse.

3. Dimensione normativa

In questa seconda sezione, prima di passare ad analizzare le disposizioni in materia di tutela dei dati personali nel contesto del DRM, si deve fare un veloce riferimento al quadro normativo di riferimento per l'applicazione dei sistemi di *Digital Rights Management*. Nel proporre la normativa si adotterà un approccio comparato, tentando di mettere in luce le differenze fra i sistemi normativi statunitense ed euro-italiano.

Il potere contrattuale-normativo, come definito nel paragrafo precedente, pone quesiti inediti prima dell'avvento di Internet sul fenomeno di *governance* della rete. Roberto Caso nota in merito che una promettente impostazione è quella di Lawrence Lessing[341]. La tesi del giurista statunitense, infatti, passa attraverso uno snodo concettuale svincolato dalla teoria delle fonti. In base a tale snodo concettuale, il comportamento umano sarebbe condizionato, principalmente, da permessi e divieti, e ciò anche nel contesto digitale. Infatti, "*le regole che permettono o vietano sono il frutto di più fattori: il diritto [di origine statale], le norme [consuetudinarie], il mercato e le architetture [il modo in cui le tecnologie disegnano lo spazio del comportamento] . Questo tipo di riflessione mira a mettere in esponente, da una parte, che le tecnologie digitali rivestono un peso decisivo nel condizionare il comportamento degli attori di Internet , dall'altra, che le stesse tecnologie interagiscono in modo complesso con gli altri fattori di condizionamento. […] Sotto il secondo profilo, si rileva che il diritto di origine statale può influire indirettamente, cioè regolando le tecnologie, sul comportamento degli utenti della rete . Per comprendere l'impatto di questa forma di regolamentazione, occorre tener presente che le tecnologie di Internet*

[340] R. CASO, *Digital rights management: il commercio delle informazioni digitali tra contratto e diritto d'autore*, cit., 97.

[341] L. LESSIG, *Code and Other Laws of Cyberspace,* New York, 1999, 35-36, dello stesso autore si veda anche *The Future of Ideas. The Fate of the Commons in a Connected World*, New York, 2001.

si basano su un'architettura complessa che è fatta di standard tecnologici , e che tali standard possono essere di pubblico dominio (aperti) o soggetti a proprietà intellettuale"[342].

Lo Stato, nonché le regole nazionali, ci si aspetterebbe che puntassero massimamente a rinvenire un delicato bilanciamento fra l'interesse *all'enforcement* del diritto d'autore, tramite le tecnologie di *Digital Rights Management,* e gli interessi dei consumatori ad avere accesso ai prodotti intellettuali, con attenzione anche alla tutela dei dati personali degli utenti che si vedono incisi da questi strumenti nella riservatezza del loro consumo intellettuale. Le speranze vengono tuttavia presto tradite dalla normativa sia nazionale che internazionale la quale si concentra, ancora una volta, dalla nostra angolazione di interesse privilegiata, sulla tutela dei *copyrights holders*, profondendosi precipuamente sulle conseguenze dell'elusione di tali tecnologie.

3.1. I trattati internazionali

La primaria fonte internazionale da cui si possono trarre osservazioni in materia di *Digital Rights Management* è costituita dai trattati WIPO del 1996.

Tali testi normativi sono stati adottati dopo numerosi anni di trattative fra gli Stati firmatari per procedere ad un'opera di intensa armonizzazione dei diritti di proprietà intellettuale ponendo un particolare accento, che li rende interessanti, sui rischi connessi *all'enforcement* del *copyright* nella società dell'informazione e quindi nel contesto digitale.

Chiaramente, essendo Internet uno strumento che consente di abbattere definitivamente ogni confine nazionale, lo strumento del trattato internazionale è apparso in grado di poter superare il limite legale delle leggi sul diritto d'autore legato al principio di territorialità nella sua applicazione, chiedendo agli Stati firmatari di conformarsi alle disposizioni internazionali così giungendo ad una tutela minima, ma diffusa, del diritto d'autore su Internet.

L'obiettivo dei trattati è, nei fatti, quello di una revisione della già citata Convenzione di Berna, adottata nel lontano 1886. Sebbene la Convenzione di Berna ebbe numerose revisioni[343], solo dal 1967 essa è coerentemente amministrata dalla WIPO (Organizzazione Mondiale per la Proprietà Intellettuale). I trattati WIPO del 1996 quindi si inseriscono nel contesto normativo della Convenzione e costituiscono la prima massiccia risposta all'avvento di Internet con un tentativo di normare lo spazio anarchico del web, quantomeno in tema di diritto d'autore.

Il WIPO Copyright Treaty (WCT) introduce alcune novità di rilievo per le tematiche che scuotono il diritto d'autore odierno, in particolare estendendo la protezione della proprietà intellettuale sui software e programmi per elaboratori, nonché sulle compilazioni di dati o altro materiale che costituiscano creazioni intellettuali. Inoltre, rispetto alla Convenzione di Berna, aggiunge ai vari diritti economici di sfruttamento dell'opera anche il c.d. "*diritto di comunicazione al pubblico*" intendendolo, all'articolo 8, come il diritto di autorizzare ogni forma di comunicazione, via filo o via etere, in modo tale che "*chiunque possa liberamente accedervi da un luogo o in un momento di sua scelta*".

L'innovazione più interessante, tuttavia, è disposta dall'art. 11 del WCT il quale dispone che le Parti contraenti debbano prevedere un'adeguata tutela giuridica e precostituire mezzi

---

[342] R. CASO, *Digital rights management: il commercio delle informazioni digitali tra contratto e diritto d'autore*, cit., 127-128.

[343] Berlino (1908), Roma (1928), Bruxelles (1948), Stoccolma (1967) e Parigi (1971).

di ricorso efficaci contro l'elusione delle misure tecnologiche utilizzate dagli autori nell'esercizio dei diritti contemplati dal trattato o dalla Convenzione di Berna, allo scopo di impedire che vengano commessi, nei confronti delle loro opere, atti non autorizzati dagli autori stessi o vietati per legge[344].

Questo articolo dimostra l'attenzione del legislatore internazionale per i fenomeni di *Digital Rights Management*, segnando nei fatti il primo riferimento normativo alla tutela giuridica di tutte quelle misure apposte tecnologicamente ad un'opera protetta da *copyright* che siano atte a impedire usi dell'opera non conformi alla volontà dei titolari dei diritti d'autore. Nel disporre ciò, il trattato richiede agli Stati firmatari di fornire effettivi rimedi contro la violazione di misure tecnologiche di protezione, in particolare richiedendo la predisposizione di mezzi di ricorso in caso di tali illecite elusioni.

Del pari, l'articolo seguente dispone invece che le Parti contraenti debbano prevedere un'adeguata tutela giuridica e debbano precostituire mezzi di ricorso efficaci contro chiunque compia deliberatamente atti di rimozione od alterazione di qualunque informazione elettronica sulla gestione dei diritti senza previo consenso dei titolari dei diritti d'autore.[345] Parimenti, la medesima tutela giuridica, ai sensi dell'articolo 12, deve essere attribuita nel caso di distribuzione, importazione a fini di distribuzione, diffusione o comunicazione al pubblico di opere senza il consenso dei titolari dei diritti, ove vi sia la conoscenza che tali opere sono state ottenute tramite una alterazione delle informazioni elettroniche sulla gestione dei diritti. Il comma secondo specifica poi cosa si debba intendere per "*informazioni sulla gestione dei diritti*", definendole come "*qualunque informazione che identifichi l'opera, l'autore, il titolare di qualsiasi diritto sull'opera, ovvero qualunque informazione circa le condizioni di utilizzazione dell'opera e qualunque numero o codice che racchiuda tali informazioni, qualora anche uno soltanto di questi elementi di informazione figuri su una copia dell'opera o compaia in una qualche comunicazione al pubblico ad essa relativa*".

Nella sostanza, quindi, l'articolo 12 impone agli Stati firmatari di attuare strategie atte a reprimere le condotte finalizzate a indurre, facilitare o dissimulare una violazione dei diritti previsti dal Trattato, ovvero della Convenzione di Berna. Il che è confermato anche dall'art. 14 il cui comma secondo dispone che le Parti contraenti debbano assicurarsi che le loro legislazioni nazionali prevedano adeguate procedure di applicazione, in modo da consentire un'azione efficace contro qualsiasi violazione dei diritti contemplati dal trattato, ivi compresi rapidi mezzi per impedire violazioni e mezzi che costituiscano un deterrente contro ulteriori violazioni.

---

[344] WIPO Copyright Treaty (WCT), liberamente consultabile presso: «https://wipolex.wipo.int/en/text/295166» (Ultimo accesso: 10 maggio 2022), il cui art. 11 dispone: "*Contracting Parties shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention and that restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law*".

[345] WIPO Copyright Treaty (WCT), cit., il cui art. 12 dispone: "*(1) Contracting Parties shall provide adequate and effective legal remedies against any person knowingly performing any of the following acts knowing, or with respect to civil remedies having reasonable grounds to know, that it will induce, enable, facilitate or conceal an infringement of any right covered by this Treaty or the Berne Convention:*

(i) to remove or alter any electronic rights management information without authority;

(ii) to distribute, import for distribution, broadcast or communicate to the public, without authority, works or copies of works knowing that electronic rights management information has been removed or altered without authority.

(2) As used in this Article, "rights management information" means information which identifies the work, the author of the work, the owner of any right in the work, or information about the terms and conditions of use of the work, and any numbers or codes that represent such information, when any of these items of information is attached to a copy of a work or appears in connection with the communication of a work to the public".

La richiesta di una risposta forte da parte degli Stati nei confronti della violazione dei meccanismi di *enforcement* del diritto d'autore tuttavia, è bene sottolineare, non trova alcun articolato normativo dedicato ai bilanciamenti che devono essere compiuti con altri diritti quali la libertà di espressione, la tutela del consumo intellettuale e la protezione dei dati personali. Una normativa in un certo senso monca, o quantomeno fortemente sbilanciata verso gli interessi dei *copyright holders* ed essenzialmente indifferente alle esigenze degli utenti.

Similmente a questo trattato anche il suo gemello, il WTTP (WIPO Performances and Phonograms Treaty), emanato anch'esso in risposta alla crescente distribuzione sul mercato di materiale protetto da *copyright* in formato digitale, tratta brevemente dei sistemi di Digital Rights Management con riferimento ai titolari dei diritti connessi al diritto d'autore quali produttori, artisti interpreti ed esecutori.

L'articolo 18 di questo trattato dispone, similmente a quanto disposto dall'art. 11 del WCT, che le parti contraenti siano tenute a fornire un'adeguata protezione giuridica nonché rimedi legali efficaci contro l'elusione di misure tecnologiche che siano utilizzate da artisti o produttori di fonogrammi in connessione con l'esercizio dei loro diritti ai sensi del trattato e che limitano atti, in relazione alle loro prestazioni o fonogrammi, che non sono autorizzati dagli esecutori o dai produttori o consentiti dalla legge[346].

L'impatto dei trattati internazionali WIPO nell'ambito delle legislazioni nazionali è evidente, in quanto le normative che procederemo ad analizzare costituiscono proprio il recepimento dei trattati. In particolare, come vedremo, disposizioni in materia vennero implementate negli Stati Uniti, con il Digital Millennium Copyright Act del 1998 e in Unione Europea con la Copyright Directive del 2001, trasposta in Italia con D.Lgs. n. 68/2003, inserendo nella Legge 633 del 1941 il Titolo II-ter, denominato "Misure tecnologiche di protezione".

3.2. Normativa italiana ed europea

Il 22 maggio del 2001, anche in forza degli obblighi internazionali nascenti dai trattati WIPO, è stata adottata dall'Unione Europea la Direttiva 29/2001 sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione[347]. Tale Direttiva pone particolare attenzione alle misure tecnologiche di protezione e quindi ai sistemi di *Digital Rights Management*.

Il Considerando 15 della Direttiva mostra evidentemente la relazione con il Trattato della WIPO sul diritto d'autore e il Trattato della WIPO sulle interpretazioni, le esecuzioni e i fonogrammi, relativi rispettivamente alla protezione degli autori e alla protezione degli interpreti o esecutori e dei produttori di riproduzioni fonografiche. Il legislatore comunitario riconosce infatti che detti trattati aggiornano notevolmente la protezione internazionale del diritto d'autore e dei diritti connessi anche per quanto riguarda il piano d'azione nel settore

---

[346] WIPO Performances and Phonograms Treaty (WPPT), art. 18, liberamente consultabile presso: «https://wipolex.wipo.int/en/text/295477» (Ultimo accesso: 10 maggio 2022), il cui testo dispone: "*Contracting Parties shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by performers or producers of phonograms in connection with the exercise of their rights under this Treaty and that restrict acts, in respect of their performances or phonograms, which are not authorized by the performers or the producers of phonograms concerned or permitted by law*".

[347] Direttiva 2001/29/CE del Parlamento europeo e del Consiglio, del 22 maggio 2001, sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione, Gazzetta ufficiale n. L 167 del 22/06/2001 pag. 0010 – 0019, consultabile presso: «https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32001L0029» (Ultimo accesso: 10 maggio 2022).

del digitale (la cosiddetta "*Digital Agenda*") e perfezionano i mezzi per combattere la pirateria a livello mondiale. La Comunità e la maggior parte degli Stati membri avevano già firmato i trattati ed erano già in corso le procedure per la loro ratifica. La Direttiva quindi, nelle parole del legislatore, serve anche ad attuare una serie di questi nuovi obblighi internazionali.

La Direttiva prende in considerazione, al Considerando 13, che le misure tecniche volte a proteggere le opere e ad assicurare la necessaria informazione sui diritti in materia rivestono un'importanza fondamentale in quanto hanno per oggetto, in ultima analisi, l'applicazione dei principi e delle garanzie fissati dalle disposizioni giuridiche.

Nel Considerando 47 il legislatore comunitario nota come lo sviluppo tecnologico nel contesto digitale stava rapidamente consentendo ai titolari dei diritti d'autore di far ricorso a misure tecnologiche ai fini *dell'enforcement* dei loro diritti, in particolare per impedire o limitare atti non autorizzati sulle opere protette dal *copyright*. Del pari, come già i trattati internazionali avevano notato, esisteva il rischio di attività illegali intese a rendere possibile o a facilitare l'elusione della protezione tecnica offerta da tali misure. Per evitare soluzioni legislative frammentarie che avrebbero potuto ostacolare il funzionamento del mercato interno, il legislatore comunitario ha quindi ritenuto necessario prevedere una protezione giuridica armonizzata contro l'elusione delle misure tecnologiche e contro la fornitura di dispositivi, prodotti o servizi a tal fine.

La Direttiva dispone che tale protezione giuridica offerta dalla tecnologia dovrebbe essere accordata alle misure tecnologiche che limitano in modo efficace atti non autorizzati dai titolari del diritto d'autore senza tuttavia impedire il normale funzionamento delle attrezzature elettroniche ed il loro sviluppo tecnico. Tale protezione giuridica dovrebbe rispettare il principio della proporzionalità e non dovrebbe vietare i dispositivi o le attività che hanno una finalità commerciale significativa o un'utilizzazione diversa dall'elusione della protezione tecnica.

In aggiunta, la Direttiva incoraggia l'adozione di sistemi di DRM in quanto sostiene che lo sviluppo tecnologico, agevolando la distribuzione delle opere, in particolare in rete, comporta altresì la necessità per i titolari dei diritti di identificare meglio l'opera o i materiali protetti, l'autore dell'opera o qualunque altro titolare di diritti e di fornire informazioni sui termini e sulle condizioni di utilizzo dell'opera o di altro materiale protetto, così da rendere più facile la gestione dei diritti ad essi connessi. Secondo il legislatore comunitario quindi, come affermato al Considerando 55, si dovrebbero incoraggiare i titolari dei diritti d'autore, quando mettono in rete opere o altri materiali protetti, a usare contrassegni indicanti, tra l'altro, la loro autorizzazione e le informazioni come dette.

Tuttavia, nei "Considerando" della Direttiva, emerge anche un'attenzione, più o meno efficace, in merito al bilanciamento che deve investire questi sistemi di *Digital Rights Management*. Il Considerando 51, in questo senso, afferma che gli Stati membri dovrebbero promuovere l'adozione di misure volontarie da parte dei titolari dei diritti d'autore, comprese la conclusione e l'attuazione di accordi fra i titolari e altre parti interessate, per tener conto della realizzazione degli obiettivi di determinate eccezioni o limitazioni previste nella normativa nazionale e comunitaria. In ogni caso, gli Stati dovrebbero anche prendere provvedimenti adeguati affinché i titolari forniscano ai beneficiari di tali eccezioni o limitazioni i mezzi necessari per fruirne, modificando una misura tecnologica già in atto o in altro modo.

Inoltre, il Considerando 60, per quanto laconico, dispone in chiave di bilanciamento quanto maggiormente interessa ai fini del presente elaborato, ossia che la protezione prevista dalla Direttiva 2001/29 non dovrebbe ostare all'applicazione delle disposizioni di diritto

nazionale o comunitario in altri settori, tra cui quelli della tutela della privacy e dei dati personali. Declamazione che spesso purtroppo rimane sulla carta in quanto la forza dei *copyright holders* non viene sufficientemente controbilanciata da una attenta tutela degli interessi degli utenti, come vedremo in chiusura di questo capitolo. Conferma dell'importanza del corretto trattamento dei dati personali viene anche dal Considerando 57 il quale dispone che, a seconda della loro configurazione, tali misure tecnologiche di protezione potrebbero rendere possibile il trattamento di dati personali riguardanti i modelli di consumo di materiale protetto da parte di singoli consumatori e pertanto consentire di registrarne il comportamento online. Per queste ragioni allora il legislatore comunitario chiede che le misure tecnologiche in oggetto debbano presentare, nelle loro funzioni tecniche, meccanismi di salvaguardia della vita privata, come previsto dalla Direttiva 95/46/CE, e quindi, oggi, dal GDPR.

Stanti queste considerazioni preliminari, il legislatore comunitario tratta delle misure tecnologiche di protezione in particolare nell'art. 6 della Direttiva. Tale norma definisce, al comma terzo, che per "misure tecnologiche" si intendono tutte le tecnologie, i dispositivi o componenti che, nel normale corso del loro funzionamento, sono destinati a impedire o limitare atti, su opere o altri materiali protetti, non autorizzati dal titolare del diritto d'autore o del diritto connesso al diritto d'autore. Le misure tecnologiche sono altresì considerate "efficaci" nel caso in cui l'uso dell'opera o di altro materiale protetto sia controllato dai titolari tramite l'applicazione di un controllo di accesso o di un procedimento di protezione, quale la cifratura, la distorsione o qualsiasi altra trasformazione dell'opera che realizzi l'obiettivo di protezione.

Il legislatore, di conseguenza, concentra la sua disciplina nel richiedere agli Stati membri di prevedere un'adeguata protezione giuridica contro simili elusioni. In aggiunta, la Direttiva richiede che gli Stati membri forniscano un'adeguata protezione giuridica anche contro la fabbricazione, l'importazione, la distribuzione, la vendita, il noleggio, o la detenzione a scopi commerciali di attrezzature, prodotti o componenti che: (a) siano oggetto di una promozione, di una pubblicità o di una commercializzazione, con la finalità di eludere, o (b) non abbiano, se non in misura limitata, altra finalità o uso commercialmente rilevante, oltre quello elusivo, o (c) siano principalmente progettate, prodotte, adattate o realizzate con la finalità di rendere possibile o di facilitare l'elusione di efficaci misure tecnologiche.

Sorprende invece il comma quarto. Se nei Considerando il legislatore sembrava fiducioso nella possibilità di attuare un rispettoso bilanciamento delle istanze dei titolari dei diritti d'autore con i diritti degli utenti compendiati nelle eccezioni e limitazioni, questa fiducia viene tradita dall'articolato normativo il quale contempla solo alcune eccezioni, segnatamente quelle previste dall'art. 5, paragrafo 2, lettere a), c), d), e), o dell'articolo 5, paragrafo 3, lettere a), b) o e)[348]. A questo si aggiunga che l'art.6 è chiaro nel disporre che gli

[348] Si riporta di seguito l'articolato normativo per ragioni di chiarezza nell'esposizione: "Eccezioni e limitazioni […] *2. Gli Stati membri hanno la facoltà di disporre eccezioni o limitazioni al diritto di riproduzione di cui all'articolo 2 per quanto riguarda:*
a) le riproduzioni su carta o supporto simile, mediante uso di qualsiasi tipo di tecnica fotografica o di altro procedimento avente effetti analoghi, fatta eccezione per gli spartiti sciolti, a condizione che i titolari dei diritti ricevano un equo compenso;
b) le riproduzioni su qualsiasi supporto effettuate da una persona fisica per uso privato e per fini né direttamente, né indirettamente commerciali a condizione che i titolari dei diritti ricevano un equo compenso che tenga conto dell'applicazione o meno delle misure tecnologiche di cui all'articolo 6 all'opera o agli altri materiali interessati;
c) gli atti di riproduzione specifici effettuati da biblioteche accessibili al pubblico, istituti di istruzione, musei o archivi che non tendono ad alcun vantaggio economico o commerciale, diretto o indiretto;

Stati membri sono chiamati a imporre la tutela delle eccezioni solo in mancanza di misure volontarie prese dai titolari, compresi accordi fra titolari e altre parti interessate. Roberto Caso sottolinea la gravità della disposizione: pare infatti che sulla rete "*l'interazione tra protezioni tecnologiche e contratto è "premiata" con la neutralizzazione delle "eccezioni e limitazioni" ai diritti sulle opere e sui materiali protetti*[349]". In aggiunta si potrebbe sostenere che "*sia la formulazione della norma del comma 4 dell'art. 6.4, sia quella del "considerando" n. 53, se interpretate alla lettera, non richiedono nemmeno un'esplicita deroga contrattuale alle eccezioni e limitazioni applicabili alle misure tecnologiche. Qualora ci si attenesse a questa interpretazione letterale, la norma suonerebbe davvero come un premio immotivato alle imprese che distribuiscono contenuti digitale in forma on demand*[350]".

Parimenti a quanto richiesto dai Trattati WIPO, anche l'art. 7 della Direttiva richiede poi il rispetto di determinati obblighi relativi alle "informazioni sui regimi dei diritti", intendendo per queste *"qualunque informazione fornita dai titolari dei diritti che identifichi l'opera o i materiali protetti, l'autore o qualsiasi altro titolare dei diritti, o qualunque informazione circa i termini e le condizioni di uso dell'opera o di altri materiali nonché qualunque numero o codice che rappresenti tali*

---

d) le registrazioni effimere di opere realizzate da organismi di diffusione radiotelevisiva con i loro propri mezzi e per le loro proprie emissioni; la conservazione di queste registrazioni in archivi ufficiali può essere autorizzata, se hanno un eccezionale carattere documentario;

e) le riproduzioni di emissioni radiotelevisive effettuate da istituzioni sociali pubbliche che perseguano uno scopo non commerciale, quali ospedali o prigioni, purché i titolari dei diritti ricevano un equo compenso.

3. Gli Stati membri hanno la facoltà di disporre eccezioni o limitazioni ai diritti di cui agli articoli 2 e 3 nei casi seguenti:

a) allorché l'utilizzo ha esclusivamente finalità illustrativa per uso didattico o di ricerca scientifica, sempreché, salvo in caso di impossibilità, si indichi la fonte, compreso il nome dell'autore, nei limiti di quanto giustificato dallo scopo non commerciale perseguito;

b) quando si tratti di un utilizzo a favore di portatori di handicap, sempreché l'utilizzo sia collegato all'handicap, non abbia carattere commerciale e si limiti a quanto richiesto dal particolare handicap;

c) nel caso di riproduzione a mezzo stampa, comunicazione al pubblico o messa a disposizione di articoli pubblicati su argomenti di attualità economica politica o religiosa o di opere radiotelevisive o di altri materiali dello stesso carattere, se tale utilizzo non è espressamente riservato, sempreché si indichi la fonte, incluso il nome dell'autore, o nel caso di utilizzo delle opere o di altri materiali in occasione del resoconto di un avvenimento attuale nei limiti di quanto giustificato dallo scopo informativo e sempreché si indichi, salvo in caso di impossibilità, la fonte, incluso il nome dell'autore;

d) quando si tratti di citazioni, per esempio a fini di critica o di rassegna, sempreché siano relative a un'opera o altri materiali protetti già messi legalmente a disposizione del pubblico, che si indichi, salvo in caso di impossibilità, la fonte, incluso il nome dell'autore e che le citazioni siano fatte conformemente ai buoni usi e si limitino a quanto giustificato dallo scopo specifico;

e) allorché si tratti di impieghi per fini di pubblica sicurezza o per assicurare il corretto svolgimento di un procedimento amministrativo, parlamentare o giudiziario;

f) quando si tratti di allocuzioni politiche o di estratti di conferenze aperte al pubblico o di opere simili o materiali protetti, nei limiti di quanto giustificato dallo scopo informativo e sempreché si indichi, salvo in caso di impossibilità, la fonte, incluso il nome dell'autore;

g) quando si tratti di un utilizzo durante cerimonie religiose o cerimonie ufficiali organizzate da un'autorità pubblica;

h) quando si utilizzino opere, quali opere di architettura o di scultura, realizzate per essere collocate stabilmente in luoghi pubblici;

i) in caso di inclusione occasionale di opere o materiali di altro tipo in altri materiali;

j) quando l'utilizzo avvenga per pubblicizzare un'esposizione al pubblico o una vendita di opere d'arte, nella misura in cui ciò sia necessario alla promozione dell'avvenimento, escludendo qualsiasi altro uso commerciale;

k) quando l'utilizzo avvenga a scopo di caricatura, parodia o pastiche;

l) quando si tratti di utilizzo collegato a dimostrazioni o riparazioni di attrezzature;

m) quando si utilizzi un'opera d'arte consistente in un edificio o un disegno o il progetto di un edificio con lo scopo di ricostruire quest'ultimo;

n) quando l'utilizzo abbia come scopo la comunicazione o la messa a disposizione, a singoli individui, a scopo di ricerca o di attività privata di studio, su terminali dedicati situati nei locali delle istituzioni di cui al paragrafo 2, lettera c), di opere o altri materiali contenuti nella loro collezione e non soggetti a vincoli di vendita o di licenza;

o) quando l'utilizzo avvenga in taluni altri casi di scarsa rilevanza in cui la legislazione nazionale già prevede eccezioni o limitazione, purché esse riguardino solo utilizzi analogici e non incidano sulla libera circolazione delle merci e dei servizi all'interno della Comunità, fatte salve le altre eccezioni e limitazioni contenute nel presente articolo. […]"

[349] R. CASO, *Digital rights management: il commercio delle informazioni digitali tra contratto e diritto d'autore*, cit., 161 e ss.

[350] In nota n.75 pagina 161, in R. CASO, *Digital rights management: il commercio delle informazioni digitali tra contratto e diritto d'autore*, cit., 161.

informazioni". In particolare, il legislatore chiede agli Stati membri di prevedere un'adeguata protezione giuridica contro chiunque compia consapevolmente atti volti a: (a) rimuovere o alterare qualsiasi informazione elettronica sul regime dei diritti; (b) distribuire, importare a fini di distribuzione, diffondere per radio o televisione, comunicare o mettere a disposizione del pubblico opere o altri materiali protetti ai sensi della presente Direttiva, dalle quali siano state rimosse o alterate senza averne diritto le informazioni elettroniche sul regime dei diritti.

La recezione della Direttiva nell'ordinamento italiano è avvenuta con il D.Lgs. n. 68/2003, inserendo nella legge 633/1941 il Titolo II-ter, denominato "Misure tecnologiche di protezione. Informazioni sul regime dei diritti"[351]. Il titolo si compone di due soli articoli di cui il primo è l'art.102-quater. Esso dispone che i titolari di diritti d'autore e di diritti connessi possono apporre sulle opere o sui materiali protetti misure tecnologiche di protezione efficaci che comprendano tutte le tecnologie, i dispositivi o i componenti che, nel normale corso del loro funzionamento, sono destinati a impedire o limitare atti non autorizzati dai titolari dei diritti d'autore.

Il successivo art. 102-quinquies poi, ricalcando le disposizioni comunitarie, afferma che possono essere previste anche informazioni elettroniche sul regime dei diritti affinché identifichino l'opera o il materiale protetto, nonché l'autore o qualsiasi altro titolare dei diritti. Tali informazioni possono altresì contenere indicazioni circa i termini o le condizioni d'uso dell'opera o dei materiali, nonché qualunque numero o codice che rappresenti le informazioni stesse o altri elementi di identificazione.

Le conseguenze dell'elusione delle misure tecnologiche non emergono chiaramente dall'analisi della legislazione in materia, essendo l'unica disposizione quella dell'art. 171-ter che prevede una fattispecie penale per le condotte elusive[352].

Il legislatore italiano, come quello comunitario si è poi interrogato sulla delicatezza dell'assicurare una tutela sconfinata *all'enforcement* del diritto d'autore per mezzo dei sistemi di *Digital Rights Management,* ritenendo necessario compiere un bilanciamento con le eccezioni e limitazioni. Risultato è l'art. 71-quinquies che oggi dispone che i titolari di diritti, che abbiano apposto le misure tecnologiche di cui all'articolo 102-quater, sono tenuti ad adottare idonee soluzioni, anche mediante la stipula di appositi accordi con le associazioni di categoria rappresentative dei beneficiari, per consentire l'esercizio delle eccezioni disposte dalle norme della Legge 633/1941. In mancanza di accordo, ciascuna delle parti può, nel nostro ordinamento, rivolgersi al Comitato consultivo permanente per il diritto d'autore di cui

---

[351] Per commenti al d. lgs. n. 68 del 2003 si vedano, fra i molti: R. CASO*, Digital rights management: il commercio delle informazioni digitali tra contratto e diritto d'autore*, cit.; G. SENA, P. A. E. FRASSI, G. D'AMMASSA, S. GIUDICI, D. MINTOTI, F. MORRI, *Diritto d'autore e diritti connessi nella società dell'informazione*, Milano, 2003; M. S. SPOLIDORO, *Una nuova riforma per il diritto d'autore nella società dell'informazione*, in *Corriere giur.*, 2003, 845; M. FABIANI, *L'attuazione della Direttiva CE su diritto di autore nella società dell'informazione. Un'analisi comparativa*, in *Dir. autore*, 2003, 331; A. M. CASELLATI, *Protezione legale delle misure tecnologiche ed usi legittimi. L'art. 6.4 della Direttiva europea e sua attuazione in Italia*, in *Dir. autore*, 2003, 360. Per alcuni rilievi in margine alla disciplina delle misure tecnologiche contenuta nel disegno poi tradotto nel d. lgs. n. 68 del 2003 si faccia altresì riferimento a P. SPADA, *Copia privata ed opere sotto chiave*, in *Riv. dir. ind.*, 2002, I, 591; M. DE SANCTIS, *Misure tecniche di protezione e libere utilizzazioni*, in *Dir. Autore*, 2003, 1.

[352] Roberto Caso, in R. CASO, D*igital rights management: il commercio delle informazioni digitali tra contratto e diritto d'autore*, cit., 121 e ss., segnala anche le prime pronunce giurisprudenziali in applicazione di tale articolo, criticato dalla più parte della dottrina: Trib. Bolzano, ord. 31 dicembre 2003, la quale ha dichiarato illegittimo un sequestro di una console playstation e di alcuni chip, nell'ambito di un'indagine relativa al reato previsto dall'art. 173-ter della l. n. 633 del 1941, liberamente accessibile presso: «http://www.interlex.it/testi/giurisprudenza/bz031231.htm» (Ultimo accesso: 10 maggio 2022).

all'articolo 190 perché esperisca un tentativo obbligatorio di conciliazione, secondo le modalità di cui all'articolo 194-bis.

Infine, l'articolo 71-sexies, ultimo comma, anch'esso introdotto dalla novella del 2003, dispone che "*i titolari dei diritti sono tenuti a consentire che, nonostante l'applicazione delle misure tecnologiche di cui all'articolo 102- quater, la persona fisica che abbia acquisito il possesso legittimo di esemplari dell'opera o del materiale protetto, ovvero vi abbia avuto accesso legittimo, possa effettuare una copia privata, anche solo analogica, per uso personale*".

3.3. Normativa statunitense

La normativa statunitense in merito ai sistemi di *Digital Rights Management* è primariamente rinvenibile nel DMCA il quale ratifica gli obblighi internazionali imposti dai Trattati WIPO procedendo a prevedere in ambito nazionale una intensa protezione del *copyright* nella sua peculiare estrinsecazione costituita dai sistemi di *Digital Rights Management.* In particolare, nel maggio 1998, il Digital Millennium Copyright Act (DMCA) venne approvato come emendamento alla legge statunitense sul *copyright*, il quale ha criminalizzato la produzione e la diffusione di tecnologie che consentono agli utenti di aggirare i sistemi di DRM.

In particolare, nel Title 17 dell'USC, la §1201(A) prevede icasticamente che nessuno possa eludere una misura tecnologica che controlli efficacemente l'accesso a un'opera protetta dal diritto d'autore[353]. L'eludere una misura tecnologica di protezione, ai sensi del DMCA, significa "*decodificare un'opera codificata, decriptare un'opera criptata o altrimenti evitare, aggirare, rimuovere, disattivare o compromettere una misura tecnologica, senza l'autorizzazione del titolare del diritto d'autore*"[354]

Tale sezione distingue le misure di elusione a seconda che si tratti di c.d. "misure anti-accesso" ovvero "misure anti-copia".

Nel primo caso la disposizione prevede che nessuno possa produrre, importare, offrire al pubblico, fornire o altrimenti trafficare in qualsiasi tecnologia, prodotto, servizio, dispositivo, componente o parte di esso, che: (A) è concepito o prodotto principalmente allo scopo di aggirare una misura tecnologica che controlli efficacemente l'accesso a un'opera protetta ai sensi del presente titolo; (B) ha uno scopo solo limitatamente commercialmente significativo o un uso diverso dall'elusione di una misura tecnologica che controlli efficacemente l'accesso a un'opera protetta; o (C) è commercializzato per l'elusione di una misura tecnologica che controlli efficacemente l'accesso a un'opera protetta ai sensi del presente titolo[355].

---

353 Si riporta il testo della 17 U.S.C §1201 (A): "*No person shall circumvent a technological measure that effectively controls access to a work protected under this title. The prohibition contained in the preceding sentence shall take effect at the end of the 2-year period beginning on the date of the enactment of this chapter*".

354 *A) to "circumvent a technological measure" means to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner;*
(A) to "circumvent protection afforded by a technological measure" means avoiding, bypassing, removing, deactivating, or otherwise impairing a technological measure;

355 *No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that—*
(A) is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under this title;
(B) has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a work protected under this title; or

Nel secondo caso, per le tecnologie genericamente, quanto imprecisamente, dette "anti-copia", si dispone, similmente, che nessuno possa produrre, importare, offrire al pubblico, fornire o altrimenti trafficare in qualsiasi tecnologia, prodotto, servizio, dispositivo, componente o parte di esso, che (A) è progettato o prodotto principalmente allo scopo di eludere la protezione offerta da una misura tecnologica che tutela effettivamente un diritto di un titolare del diritto d'autore ai sensi del presente titolo su un'opera o parte di essa; (B) ha solo uno scopo commercialmente significativo o un uso diverso da quello di eludere la protezione offerta da una misura tecnologica che protegga effettivamente un diritto di un titolare del diritto d'autore ai sensi del presente titolo su un'opera o parte di essa; o (C) è commercializzato da quella persona o da un altro che agisce di concerto e con la conoscenza di quel soggetto per l'uso nell'elusione della protezione offerta da una misura tecnologica che protegge effettivamente un diritto di un titolare del diritto d'autore ai sensi del presente titolo in un'opera o parte di essa. [356]

Il DMCA assicura alla §1201 (c) (1) che "*nulla in questa sezione pregiudica i diritti, i rimedi, le limitazioni o le difese contro la violazione del copyright, incluso il fair use, ai sensi del presente titolo.*[357]". Anche il legislatore statunitense, infatti, ritiene che il rispetto delle eccezioni e limitazioni al diritto d'autore debba essere assicurato, prevedendo ipotesi oltre le quali le misure tecnologiche non possono spingersi. Fra le molte, si possono ricordare quelle attinenti alle biblioteche, attività giudiziarie, protezione dei minori, ma anche la tutela della privacy e dell'identità personale.

Proprio in questo ultimo caso la legislazione statunitense si mostra particolarmente interessante in quanto dispone al 17 U.S.C §1201 (i)(1) che non costituisce violazione della presente normativa l'elusione di una misura tecnologica che controlli efficacemente l'accesso a un'opera protetta ai sensi del presente titolo, se: (A) la misura tecnologica, o l'opera che protegge, contiene la capacità di raccogliere o diffondere informazioni di identificazione personale che riflettono le attività online di una persona fisica che cerca di accedere all'opera protetta; (B) la misura tecnologica, o l'opera che protegge, nel normale corso del suo funzionamento, raccoglie o diffonde informazioni di identificazione personale sulla persona che cerca di accedere all'opera protetta, senza dare cospicuo avviso di tale raccolta o diffusione a tale persona e senza fornire a tale persona la capacità di prevenire o limitare tale raccolta o diffusione; (C) l'atto di elusione ha il solo effetto di identificare e disabilitare la capacità di monitoraggio di cui alla lettera A, e non ha altro effetto sulla capacità di qualsiasi persona di accedere a qualsiasi lavoro; e (D) l'atto di elusione è compiuto al solo fine di impedire la raccolta o la diffusione di informazioni di identificazione personale su una persona fisica che cerca di accedere al lavoro tutelato, e non viola qualsiasi altra legge"[358].

(C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing a technological measure that effectively controls access to a work protected under this title.

[356] *No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that—*

(A) is primarily designed or produced for the purpose of circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof;

(B) has only limited commercially significant purpose or use other than to circumvent protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof; or

(C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof.

[357] *nothing in this Section shall affect rights, remedies, limitations, or defenses to copyright infringement, including fair use, under this title.*

[358] *Notwithstanding the provisions of subsection (a)(1)(A), it is not a violation of that subsection for a person to circumvent a technological measure that effectively controls access to a work protected under this title, if—*

La regolamentazione della materia attuata dal legislatore statunitense ha comportato numerose critiche da parte della dottrina d'oltreoceano [359], nonché ha prodotto esiti giurisprudenziali di non facile inquadramento[360]. Roberto Caso ne segnala una natura quasi paradossale, affermando che *"molti dei soggetti colpiti dai primi giudizi non sono i c.d. pirati della rete, ma persone che operano nel mondo della scienza, della tecnologia e dell'editoria. Il sospetto è che alcuni settori imprenditoriali, che hanno premuto per l'emanazione della legge, abbiano mostrato un bersaglio (i c.d. "utenti-pirati"), volendo colpirne (almeno anche) un altro (coloro che sono in grado di sviluppare nuove e competitive tecnologie). Più in generale, in un ambiente già sovraffollato di diritti di proprietà intellettuale (sempre più restrittivi), la comunità scientifica teme che la tutela delle misure antielusione possa infliggere un vulnus definitivo al pubblico dominio, ai diritti di proprietà informali, alla libera circolazione delle informazioni, ed alla libera manifestazione del pensiero*[361]". Una sorta di logica censoria.

La disciplina statunitense si dimostra, del pari di quella italiana ed europea, come fortemente sbilanciata in favore dei titolari dei diritti d'autore. Le disposizioni, infatti, garantiscono un controllo nei fatti superiore a quello concesso dalle normali regole sul *copyright*, permettendo una tutela rafforzata *dell'enforcement* del diritto d'autore, minacciando invece la libertà di manifestazione del pensiero, la libertà nel consumo dei prodotti intellettuali ed in definitiva della privacy degli utenti, senza che il legislatore preveda serie strategie di riequilibrio al di fuori di vuote declamazioni normative.

4. Uno sguardo alla tecnologia

L'avvento di Internet ha consentito la condivisione delle informazioni a un livello senza precedenti nella storia umana. Questa incredibile facilità di diffusione ha consentito la condivisione e l'uso di file su vasta scala che hanno messo a dura prova le interpretazioni tradizionali della legge sul diritto d'autore e hanno spinto le grandi società di media a investire nelle tecnologie digitali per controllare l'uso dei file elettronici. Queste tecnologie si basano

---

(A) the technological measure, or the work it protects, contains the capability of collecting or disseminating personally identifying information reflecting the online activities of a natural person who seeks to gain access to the work protected;
(B) in the normal course of its operation, the technological measure, or the work it protects, collects or disseminates personally identifying information about the person who seeks to gain access to the work protected, without providing conspicuous notice of such collection or dissemination to such person, and without providing such person with the capability to prevent or restrict such collection or dissemination;
(C) the act of circumvention has the sole effect of identifying and disabling the capability described in subparagraph (A), and has no other effect on the ability of any person to gain access to any work; and
(D) the act of circumvention is carried out solely for the purpose of preventing the collection or dissemination of personally identifying information about a natural person who seeks to gain access to the work protected, and is not in violation of any other law

[359] Per una completa ricostruzione delle posizioni critiche della dottrina si veda R. CASO, *Digital rights management: il commercio delle informazioni digitali tra contratto e diritto d'autore*, cit., 131-152; J. LITMAN, *Digital Copyright*, New York, 2001; J. E. COHEN *Lochner in Cyberspace: the New Economic Orthodoxy of "Rights Management"*, 97 *Mich. L. Rev.* 462 (1998), liberamente accessibile presso: «https://scholarship.law.georgetown.edu/facpub/811/» (Ultimo accesso: 10 maggio 2022).

[360] Roberto Caso, in R. CASO, *Digital rights management: il commercio delle informazioni digitali tra contratto e diritto d'autore, cit., 141-143,* segnala, fra molti, i seguenti casi: Pearl Invs. LLC v. Std I/O Inc., Civ. No. 02-50-P-H, 2003 U.S. Dist. LEXIS 5376 (D. Me. Apr. 2, 2003); Lexmark Int'l, Inc. v. Static Control Components, Inc., No. 02-571-KSF, 2003 U.S. Dist. LEXIS 3734 (E.D. Ky. Feb. 27, 2003); Portionpac Chem. Corp. v. Sanitech Sys., Inc., 210 F. Supp. 2d 1302 (M.D. Fla. 2002); CSC Holdings, Inc. v. Greenleaf Elecs, Inc., No. 99 C 7249, 2000 U.S. Dist. LEXIS 7675 (N.D. Ill. June 1, 2000); Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 317-18 (S.D.N.Y. 2000), aff'd sub nom., Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir. 2001); RealNetworks, Inc. v. Streambox, 2000 WL 127311 (W.D. Wash. 2000); Sony Computer Entertainment of America, Inc. v. GameMasters, 87 F. Supp. 2d 976 (N. D. Cal. 1999).

[361] R. CASO, *Digital rights management: il commercio delle informazioni digitali tra contratto e diritto d'autore*, cit., 143.

su sistemi informatici per imporre restrizioni all'uso di contenuti digitali che aderiscono ai desideri dei titolari dei diritti d'autore[362].

I sistemi di *Digital Rights Management*, come segnalato, consentono ai titolari dei contenuti digitali di tradurre direttamente nei fatti le clausole stabilite nelle licenze d'uso, imponendo quindi contrattualmente regole di accesso e di utilizzo dei contenuti ma al contempo anche prevedendo meccanismi sanzionatori direttamente attuati dalle tecnologie stesse. Infatti, grazie ai meccanismi di monitoraggio, il sistema di DRM è in grado di conoscere l'uso che l'utente compie del contenuto e se tale uso non risulta conforme a quanto stabilito dalle clausole.

Più nello specifico, l'utilizzo dei sistemi di *Rights Management* ha almeno due finalità: in primo luogo può essere usato per proteggere l'opera da illecite riproduzioni, controllando l'accesso alla stessa. Tale finalità si raggiunge solitamente attraverso la crittografia, che scrive il contenuto digitale in un codice che può essere letto solo da dispositivi o software in possesso della chiave per decodificarlo. Questo approccio è talvolta indicato anche come *scrambling*. Altri esempi di protezione dalla copia includono filigrane digitali, impronte digitali e limitazioni delle funzionalità di copia. In secondo luogo, i sistemi di DRM possono essere usati per gestire le autorizzazioni d'uso di una certa opera. Esempi di queste strategie DRM includono licenze, autenticazioni utente e protocolli di autenticazione IP, server proxy, reti private virtuali (VPN), restrizioni regionali o blocchi geografici e progettazioni di prodotti per funzionare solo su hardware o software specializzati[363].

Spostandoci sul piano pratico, si possono tracciare alcune comuni applicazioni dei sistemi di DRM. Fra le molteplici funzionalità possiamo per esempio ricordare che tali tecnologie consentono di limitare l'accesso ai file audio. Ad esempio, l'Apple iTunes Music Store utilizza la tecnologia DRM per limitare il numero di dispositivi che possono essere utilizzati per riprodurre i file audio acquistati[364].

Un sistema di gestione del diritto d'autore, quindi, prevede solitamente due moduli di base, uno per l'identificazione del contenuto e uno per la concessione di licenze o altri diritti di transazione. Tuttavia, ai fini del proseguo del presente elaborato, le tecnologie che maggiormente devono essere analizzate sono quelle che consentono il riconoscimento automatico dei contenuti online su Internet. L'*Automatic Content Recognition* (ACR) è una tecnologia, variamente inquadrabile all'interno del vasto termine di *Digital Rights Management*, usata per identificare il contenuto riprodotto su un dispositivo multimediale o presente all'interno di un file multimediale. Queste tecnologie stanno rapidamente diventando sempre più fondamentali non solo per la tutela della proprietà intellettuale sul web, ma anche per

---

362 E. A. ROBINSON, *Digital Rights Management, Fair Use, and Privacy: Problems for Copyright Enforcement through Technology* (2009), in *Other Topics*, 12, liberamente accessibile presso: «https://soar.usa.edu/other/12» (Ultimo accesso: 10 maggio 2022), citando testualmente esso afferma: "*The advent of the Internet has enabled the sharing of information on a level unprecedented in human history. Simple and speedy transferral of digital content has created widely available educational opportunities and the possibility for broader dissemination of vast libraries of cultural content like music, art., and film in electronic forms. This incredible ease of dissemination has enabled file sharing and use on vast scales that have strained traditional interpretations of copyright law and spurred larger media firms to invest in digital technologies for controlling use of electronic files. These technologies, referred to as Digital Rights Management (DRM) systems rely upon computer systems to impose restrictions on the use of digital content that adhere to the wishes of the copyright holders*"

363 M. HAMM, *What is Digital Rights Management*, in *WIDEN*, 2021, liberamente accessibile presso: «https://www.widen.com/blog/digital-rights-management» (Ultimo accesso: 10 maggio 2022).

364 M. HAMM, *ibidem*

una serie di applicazioni aziendali e di sicurezza e per affrontare le principali sfide della società, come la diffusione online di contenuti terroristici o abusi sui minori[365].

L'attenzione privilegiata per il funzionamento tecnologico dei sistemi di *Digital Rights Management* sotto l'angolatura dell'*Automatic Content Recognition* si spiega in particolare per l'intervento dell'articolo 17 della Direttiva 2019/790, sulle cui disposizioni ci si concentrerà nel capitolo successivo[366].

Gli strumenti di riconoscimento consentiranno alle piattaforme di impegnarsi al meglio per bloccare e rimuovere i contenuti non autorizzati, condizione per la loro assenza di responsabilità. Sebbene l'articolo 17 della Direttiva di per sé non renda obbligatoria alcuna tecnologia particolare, nel definire i migliori sforzi che tali piattaforme devono attuare per andare esenti da responsabilità, fa riferimento ad "*elevati standard di diligenza professionale di settore, volti ad assicurare che non siano disponibili opere e altri materiali specifici per i quali abbiano ricevuto le informazioni pertinenti e necessarie dai titolari dei diritti*".

Nel campo dell'audio e del video è ora, nei fatti, indispensabile che gli interessati facciano riferimento a questi sistemi di *Automatic Content Recognition* per dimostrare di aver compiuto i massimi sforzi per andare esenti da responsabilità. Tutte le piattaforme di condivisione contemplate dalla Direttiva dovranno, in tal senso, compiere uno sforzo di aggiornamento dei propri sistemi di gestione dei contenuti sulla rete, comprendendo nei loro sistemi anche meccanismi di riconoscimento automatico dei contenuti.

La capacità dei computer di riconoscere i contenuti è fondamentale per alcuni dei nuovi sviluppi nei settori dei media digitali, dell'e-commerce o del cloud computing. I computer sono sempre più utilizzati per riconoscere e moderare contenuti online illegali o dannosi, per classificare automaticamente i contenuti archiviati nel cloud, riconoscendo le immagini dei prodotti pubblicati sui social media.

Proprio come la maggior parte degli altri sviluppi tecnologici, l'ACR ha un impatto sulla proprietà intellettuale, attuando diverse tecnologie già in uso per proteggere o gestire meglio il *copyright*. Questo è particolarmente il caso delle soluzioni ACR utilizzate per identificare elenchi di prodotti contraffatti nei mercati di e-commerce o per monetizzare l'uso di contenuti protetti da *copyright* su piattaforme di condivisione video.

Tuttavia, è bene notare che, nella sostanza, le basi tecnologiche su cui strutturarli sono le medesime dei tipici sistemi di *Digital Rights Management* ossia la crittografia, il *watermarking* ed il *fingerprinting*. A questi, recentemente, si è aggiunto il sistema di riconoscimento digitale dei contenuti basato sull'intelligenza artificiale.

4.1. Crittografia: l'Hashing

---

[365] Ufficio dell'Unione europea per la proprietà intellettuale, *Automated content recognition: discussion paper. Phase 1, Existing technologies and their impact on IP*, in European Union Intellectual Property Office, 2020, liberamente accessibile presso: «https://data.europa.eu/doi/10.2814/52085» (Ultimo accesso: 10 maggio 2022).

[366] Maggiori riferimenti rinvenibili presso: Mission Report, *Towards more effectiveness of copyright law on online content sharing platforms: overview of content recognition tools and possible ways forward*, Report sottoposto al CSPLA il 28 November 2019, Ministero della Cultura Francese, liberamente accessibile presso: «https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiH8P6bzeX1AhWWQvEDHa6fDX0QFnoECAoQAQ&url=https%3A%2F%2Fwww.culture.gouv.fr%2Fcontent%2Fdownload%2F265045%2Ffile%2FMission%2520Report%2520Content%2520Recognition%2520Tools%2520ENG%2520V.pdf%3FinLanguage%3Dfre-FR&usg=AOvVaw2P9rxPn_MDDsQtYmdnYMZR» (Ultimo accesso: 10 maggio 2022).

La crittografia consiste in uno strumento idoneo ad alterare il contenuto originale di un certo file in modo da renderlo incomprensibile od inutilizzabile da parte di chiunque non sia in possesso del codice necessario a decifrare il messaggio. È lo stesso sistema che è alla base, per esempio delle firme digitali[367].

In assenza di crittografia, infatti, chiunque potrebbe accedere ad un file e copiarne il contenuto, manipolarlo o trasmetterlo digitalmente a chiunque altro. A questo scopo quindi la crittografia consente di controllare l'accesso al contenuto digitale ed ogni possibile utilizzo dello stesso[368].

Una crittografia basata su chiavi asimmetriche, simile a quella usata per la firma digitale, consente di verificare al contempo l'integrità del contenuto e le identità del fornitore e del consumatore dello stesso[369]. Le chiavi sono asimmetriche in quanto il sistema si basa su due chiavi, una pubblica ed una privata, e per rivelare il contenuto criptato è necessario congiungere le due chiavi[370].

All'interno dell'ampio genere della crittografia, la tecnologia oggi più interessante è quella conosciuta con il termine "*hashing*"[371]. Esso descrive il processo di esecuzione di un file digitale attraverso una funzione di *hashing* (cioè un algoritmo) per generare un identificatore univoco per un certo file sotto forma di una breve stringa di caratteri (un *hash*). Questo processo non può essere compiuto a ritroso, evitando rischi di *reverse engineering*, non essendo, in teoria, possibile recuperare il file originale da un *hash*. La stringa di caratteri appena generata viene assegnata al file, come suo identificatore univoco. Il fatto che tale identificatore sia univoco significa che ove lo stesso identico file dovesse venire sottoposto allo stesso procedimento di generazione di *hash*, il risultato che si otterrebbe sarebbe la stessa identica stringa di caratteri.

L'hashing viene utilizzato per molteplici scopi, tra cui l'indicizzazione del contenuto o la protezione delle password. Un esempio potrebbe essere anche quello della moderazione dei contenuti online, come la tecnologia *PhotoDNA*, originariamente sviluppata da *Microsoft* e ora disponibile sul servizio *cloud* di *Microsoft Azure*, che sfrutta la tecnologia di *hashing* per aiutare a fermare la condivisione di immagini di sfruttamento minorile[372].

Nel campo del riconoscimento dei contenuti, esistono diversi tipi di funzioni di *hashing*, tuttavia quello crittografico è il più utilizzato. *L'hashing* crittografico può essere utilizzato per rilevare tutti i tipi di file, inclusi i file contenenti testo, immagini, contenuti audio o video. Viene spesso utilizzato dalle piattaforme di condivisione dei contenuti. Il limite *dell'hashing*

---

[367] Per approfondimenti in merito si veda G. PASCUZZI, P. GUARDA, *L'evoluzione del concetto di documento e di sottoscrizione*, in G. PASCUZZI (a cura di*), Il diritto nell'era digitale*, Bologna, 2016, 77-87.

[368] R. CASO, *Digital rights management: il commercio delle informazioni digitali tra contratto e diritto d'autore*, cit., 17 e ss.

[369] R. CASO, *ibidem*, 17 e ss.

[370] Per maggiori informazioni sul funzionamento tecnologico delle chiavi si veda G. PASCUZZI, P. GUARDA, *L'evoluzione del concetto di documento e di sottoscrizione*, in G. PASCUZZI (a cura di*), Il diritto nell'era digitale*, Bologna, 2016, 77-87.

[371] Maggiori informazioni sono rinvenibili presso: Ufficio dell'Unione europea per la proprietà intellettuale, *Automated content recognition: discussion paper. Phase 1, Existing technologies and their impact on IP*, in *European Union Intellectual Property Office*, 2020, liberamente accessisibile presso: «https://data.europa.eu/doi/10.2814/52085» (Ultimo accesso: 10 maggio 2022).

[372] Per ulteriori informazioni si veda il sito di Microsoft dedicato a PhotoDNA «https://www.microsoft.com/en-us/photodna» (Ultimo accesso: 10 maggio 2022).

per il riconoscimento del contenuto è che individua solo un file invece del suo contenuto effettivo[373].

Nell'ambito del *Content Recognition* per ipotesi di violazione del *copyright*, il sistema della crittografia consente, ad esempio, di garantire che un file che sia stato notificato ad una piattaforma online come in violazione dei diritti d'autore, non sia condiviso nei servizi di archiviazione *cloud*: alcuni servizi di archiviazione *cloud* utilizzano infatti *l'hashing* per identificare e impedire la condivisione di file che sono stati rimossi per violazione del *copyright*. Questo è in particolare il caso di *Dropbox* o *Google Drive*.

Con l'esempio di *Dropbox*[374] si può notare che ove un utente carichi un file sulla piattaforma, accadono due cose: viene generato un *hash* e quindi il file viene crittografato per impedire a qualsiasi utente non autorizzato di poterlo aprire. Ove un reclamo di violazione del diritto d'autore sia notificato al sistema di *Dropbox*, esso aggiunge *l'hash* del file che si suppone essere stato illecitamente condiviso ad una "lista nera" di stringhe rappresentanti file la cui condivisione è vietata. Ove, quindi, un utente proceda a condividere un determinato file, trasformato in un *hash* da Dropbox, e ai server risulti che *l'hash* di tal file corrisponde ad uno inserito nella "lista nera", procederà a bloccare tale condivisione.

In secondo luogo, la crittografia mediante *hashing* è altresì utilizzata affinché un file rimosso da una piattaforma, per violazione dei diritti d'autore, non venga ricaricato sulla stessa[375]. L'esempio è quello di *YouTube* che utilizza, assieme ad altre misure tecnologiche, anche *l'hashing* per impedire il caricamento ripetuto di file che sono stati oggetto di una notifica di violazione del *copyright*. Tale sistema è solitamente offerto in alternativa o in congiunzione al più noto sistema del "*Content ID*", su cui *infra*.

Il sistema crittografico basato *sull'hashing* ha notevoli vantaggi dal punto di vista tecnologico. In particolare, mentre diverse tecniche e algoritmi richiedono quantità diverse di potenza di calcolo, *l'hashing* richiede capacità di calcolo e di archiviazione dati relativamente inferiori rispetto ad altre tecnologie ACR. Un database di riferimento *hash* memorizza solo una breve stringa di caratteri anziché l'intero file. Al contempo, tuttavia, è altresì vero che *l'hashing* può identificare con precisione solo i duplicati esatti di un file digitale. Infatti, la minima modifica del file ne rende impossibile il riconoscimento in quanto tale tecnologia non resiste a qualsiasi cambio di formato, compressione o alterazione di un file. Chiaramente esistono sistemi di riconoscimento più o meno forti, essendo alcuni capaci di riconoscere il file nonostante alcune modificazioni che tuttavia devono essere minimali[376].

---

[373] Per maggiori informazioni si veda: Ufficio dell'Unione europea per la proprietà intellettuale, *Automated content recognition : discussion paper. Phase 1, Existing technologies and their impact on IP'*, cit. 7 e ss. In particolare, il testo citato dispone: "*Cryptographic hashing can be used to detect all types of files, including files containing text, image, audio or video content. It appears to be well-suited when analysing hosted content rather than 'on the fly' content. It is often used by content-sharing platforms, where content is openly accessible and not individually encrypted. If it can be used in end-to-end encrypted communication environments, cryptographic hashing techniques are mostly successful in recognising content that is not encrypted. Cryptographic hashing techniques also support the recognition of compressed content, when the original format of the compressed content is known. The limitation of hashing for content recognition is that it only recognises a file as opposed to its actual content".*

[374] In merito si veda G. KUMPARAK, *How Dropbox Knows When You're Sharing Copyrighted Stuff (Without Actually Looking At Your Stuff)*, in *Techcrunch*, 2013, liberamente accessibile presso: «https://techcrunch.com/2014/03/30/how-dropbox-knows-when-youre-sharing-*copyright*ed-stuff-without-actually-looking-at-your-stuff/» (Ultimo accesso: 10 maggio 2022).

[375] Per maggiori informazioni si veda: Ufficio dell'Unione europea per la proprietà intellettuale, *Automated content recognition: discussion paper. Phase 1, Existing technologies and their impact on IP,* cit., 7 e ss.

[376] Notazioni in merito a vantaggi e svantaggi della tecnologia di crittografia sono rinvenibili presso: Ufficio dell'Unione europea per la proprietà intellettuale, *Automated content recognition: discussion paper. Phase 1, Existing technologies and their impact on IP*, cit., 8-10

Un sicuro punto di forza *dell'hashing* è la capacità di essere utilizzato in combinazione con altre tecnologie: poiché richiede risorse limitate, *l'hashing* crittografico viene utilizzato per integrare tecnologie ACR ad alta intensità di risorse e, in particolare il *fingerprinting*.

È infatti il caso di *YouTube* che utilizza la tecnologia di *fingerprinting* (c.d. *Content ID*) per identificare i contenuti sulla sua piattaforma. Una volta che un file specifico è stato identificato dal *Content ID* e rimosso, *l'hashing* viene utilizzato per impedire che lo stesso identico file venga caricato ripetutamente. In questo caso *l'hashing* crittografico viene utilizzato come prima linea di difesa per limitare l'uso della tecnologia di *fingerprinting*, che richiede invece più risorse.

4.2. Watermarking

La seconda possibile soluzione tecnica di *Digital Rights Management* che merita di essere considerata è il *Watermarking*, ossia una tecnologia finalizzata all'inserzione di una filigrana in un contenuto digitale[377]. Esso può essere definito come un procedimento "*steganografico*" volto a incorporare un codice di riconoscimento od una filigrana che sia solitamente invisibile o comunque impercettibile da parte dei fruitori dei servizi.

La tecnologia di *watermarking* deve rispondere a specifici requisiti. In particolare, deve essere connotata dall'impercettibilità, nel senso che la filigrana non deve essere visibile nella normale fruizione del contributo, inoltre deve essere robusta, ossia non eliminabile dalla mera compressione del file o manipolazione dello stesso. La filigrana altresì deve cercare di contenere i maggiori dati identificativi dell'opera possibili in modo indelebile, consentendo efficientemente la rilevazione della stessa ove si rendesse necessario[378].

In generale, dunque, il *watermarking* serve ad inserire permanentemente in un determinato file un insieme di metadati riguardanti, in particolare, il contenuto del file, il titolare dei diritti sull'opera o un insieme di condizioni generali di contratto legate al contenuto offerto.

Nell'ambito *dell'Automatic Content Recognition*, il *watermarking* viene utilizzato per identificare supporti o file digitali, con modifiche percettibili o impercettibili applicate al contenuto o al file. Il processo di *watermarking* ha in genere due fasi separate: una di marcatura e una di identificazione della filigrana.

La fase di marcatura avviene quando si applica la filigrana al contenuto. Può essere una filigrana generica applicata a tutte le copie digitali di un contenuto o una individuale e specifica per ciascuna copia. La fase di identificazione della filigrana può avvenire tramite lettura di una filigrana visiva che appare su un contenuto, o richiedere l'uso di un software di rilevamento della filigrana per identificare quelle digitali od addirittura crittografate.

La filigrana si applica a contenuti di testo, immagini, video e audio. Tuttavia, essa può supportare solo il rilevamento di contenuti che sono stati effettivamente contrassegnati in precedenza. L'inserimento di singole filigrane in ogni copia digitale di un'opera, nonché la

---

377 R. CASO, *Digital rights management: il commercio delle informazioni digitali tra contratto e diritto d'autore*, cit., 23 e ss.

378 Notazioni riprese da B. ROSENBLATT, B. TRIPPE, S. MOONEY, *Digital Rights Management, Business and Technology*, così come citato da R. CASO, *Digital rights management: il commercio delle informazioni digitali tra contratto e diritto d'autore*, cit., 23 e ss.

gestione della distribuzione di queste copie contrassegnate individualmente, possono richiedere risorse significative[379].

Esistono diversi tipi di *watermarking*, potendosi ad esempio distinguere fra una "filigrana visibile" in contrapposizione a "filigrana invisibile" che solitamente codifica le informazioni nel contenuto digitale, senza distorcere il contenuto stesso. Queste informazioni possono essere rilevate e decodificate solitamente solo tramite algoritmi specifici.[380]

È altresì possibile distinguere, ad esempio, tra una "filigrana statica" ed una "filigrana dinamica": la prima include informazioni predeterminate, solitamente un logo o un insieme di caratteri, fissate sul contenuto una volta pubblicato. Con la "filigrana digitale" invece, possono essere aggiunte componenti ulteriori, le quali possono essere aggiornate in tempo reale, rendendo il file digitale filigranato unico e facilmente identificabile[381].

Ulteriore distinzione riguarda la contrapposizione fra il c.d "*software watermarking*" e l' "*hardware watermarking*". La prima è una tecnica sviluppata per minare la pirateria del software incorporando un segnale digitale nello stesso. Il secondo è il processo di incorporazione di segni nascosti come caratteristiche o attributi di progettazione all'interno di un hardware e richiede meccanismi altamente sofisticati per impiantare un marchio all'interno del progetto senza alterare la funzionalità del dispositivo. Ad esempio, alcuni *chip* possono essere integrati in una fotocamera digitale o in qualsiasi altro dispositivo multimediale, in modo tale che i suoni o le immagini da questi registrati vengano filigranati direttamente quando vengono catturati[382].

Appare quindi evidente che l'uso più diffuso di questa tecnologia sia proprio quello dell'aggiunta di informazioni relative a diritti o titolari di diritti: le filigrane vengono utilizzate per proteggere i diritti di proprietà intellettuale includendo informazioni relative ai diritti e ai loro titolari direttamente nel contenuto (ad es. un logo, il nome del titolare dei diritti o un indirizzo e-mail).

---

[379] Per maggiori informazioni si veda: Ufficio dell'Unione europea per la proprietà intellettuale, *Automated content recognition: discussion paper. Phase 1, Existing technologies and their impact on IP*, cit., 10 e ss.

[380] Si veda a titolo di esempio il sito *DigitalWatermarkingAlliance*, presso: «http://digitalwatermarkingalliance.org/digital-watermarking-works/» (Ultimo accesso: 10 maggio 2022) in cui si afferma che: "*Una filigrana digitale è un dato digitale che può essere incorporato in tutte le forme di contenuto multimediale, comprese immagini digitali, audio, video e persino determinati oggetti. È disponibile un software speciale per incorporare informazioni impercettibili tramite sottili modifiche ai dati del contenuto digitale originale. Le filigrane digitali possono essere facilmente rilevate e lette da computer, reti e una varietà di dispositivi digitali, convalidando il contenuto originale e/o avviando azioni. La filigrana digitale si riferisce a una tecnologia nota come steganografia, che letteralmente significa "scrittura coperta". È una tecnica progettata per proteggere un messaggio nascondendolo all'interno di un altro oggetto in modo che possa essere tenuto segreto a tutti tranne che al destinatario previsto. Questo è abbastanza diverso dalla crittografia che rende il messaggio (che è generalmente visibile o udibile) incomprensibile a spettatori non autorizzati per impedirne l'accesso. I messaggi steganografici possono o meno essere crittografati. Grazie a molti progressi nella tecnologia, la steganografia è ora utilizzata con successo in una varietà di settori. Le filigrane digitali forniscono i mezzi per nascondere i messaggi steganografici per molti scopi diversi*".

[381] Si veda ad esempio il sito *SmartFrame*, presso «https://smartframe.io/features/dynamic-watermarking/» (Ultimo accesso: 10 maggio 2022) ove sono fornite maggiori informazioni sul funzionamento dei sistemi di filigrana dinamica.

[382] In merito si veda ad esempio il contributo S. P. MOHANTY, A. SENGUPTA ET. AL., *Everything You Want to Know About Watermarking: From Paper Marks to Hardware Protection* (2016), in *IEEE Consumer Electronics Magazine*. 6. 10.1109/MCE.2017.2684980, liberamente accessibile presso: «https://www.researchgate.net/publication/309179925_Everything_you_Wanted_to_Know_About_Watermarking_From_Paper_Marks_to_Hardware_Protection» (Ultimo accesso: 10 maggio 2022).

Esistono numerosi servizi in questo campo, come EditionGuard[383], Logaster[384] o SnapRetail[385].

Allo stesso tempo, la filigrana può essere utilizzata per identificare la rete che distribuisce o trasmette il contenuto. Un "ID di rete" viene aggiunto al contenuto per ogni emittente/distributore. Anche in merito agli e-book, per esempio, sono state immaginate filigrane volte ad incorporare dati nascosti nelle illustrazioni, alterare algoritmicamente contenuti diversi dalla sostanza effettiva del libro, od utilizzare i c.d "*kerning algorithms*", algoritmi usati per calcolare la spaziatura dei caratteri in una riga di testo[386].

Un sicuro beneficio derivante dall'utilizzo di questi sistemi di riconoscimento di contenuti contrassegnati da *watermark* è che esso richiede meno risorse computazionali rispetto al *fingerprinting*, in quanto consiste nel riconoscere le informazioni incorporate nel contenuto stesso del file senza la necessità di un database di riferimento. Tuttavia, i sistemi e le tecniche di marcatura non sono generici o standardizzati e una filigrana generata da una tecnologia non può essere letta da un sistema che utilizza una tecnologia diversa[387].

Nonostante ciò, la tecnologia di *watermarking* digitale raggiunge un elevato livello di accuratezza ai fini dell'identificazione dei contenuti e del tracciamento della fonte. Tuttavia, l'accuratezza nel rilevamento della filigrana e, di conseguenza, nel riconoscimento dei contenuti, può essere compromessa se la protezione della filigrana viene aggirata (ad esempio, mediante rimozione o sfocatura della stessa). Infatti, le filigrane meno forti dal punto di vista tecnologico possono scomparire, in genere, quando si verifica un qualche tipo di elaborazione del file o del supporto, ad esempio quando il contenuto viene compresso. Le filigrane "visibili" sono generalmente più fragili ed è stato dimostrato che possono essere rimosse automaticamente utilizzando algoritmi informatici specifici[388]. Esistono diverse tecniche per aggirare la protezione della filigrana di immagini o video, alcune delle quali utilizzano software o servizi online perfettamente leciti,[389] quali la sfocatura della filigrana o modificazione del formato di *output* di un file.

4.3. Fingerprinting

[383] Si veda in merito il contributo EditionGuard's '*Watermarks for Your Digital Content: The 'How To'*, 2018 presso: «https://www.editionguard.com/learn/watermarks-digital-content/» (Ultimo accesso: 10 maggio 2022).
[384] Si veda in merito quanto affermato da Logaster's *'How to create a logo and use it as a watermark',* 2018, «https://www.logaster.com/blog/create-logo-watermark/» (Ultimo accesso: 10 maggio 2022).
[385] Si veda in merito quanto affermato da Snapretail's '*How to Watermark Your Photos for Pinterest*', 2017, presso: «https://snapretail.com/snapretail-blog/how-to-watermark-your-photos-for-pinterest/» (Ultimo accesso: 10 maggio 2022).
[386] Si veda ad esempio B. ROSENBLATT, *A bounty hunting service for e-books piracy*, in *Blockchain, Copyright Monitoring, Publishing, Watermarking*, in *Copyright and Technology*, 2017, accessibile presso: «https://*copyright*andtechnology.com/2017/01/30/a-bounty-hunting-service-for-e-book-piracy/» (Ultimo accesso: 10 maggio 2022).
[387] Per maggiori informazioni si veda: Ufficio dell'Unione europea per la proprietà intellettuale, *Automated content recognition: discussion paper. Phase 1, Existing technologies and their impact on IP*, cit., 13-15.
[388] T. DEKEL, M. RUBINSTEIN, C. LIU, W. T. FREEMAN, *Google Research, On the Effectiveness of Visible Watermarks,* in *Computer Vision Foundation e IEEE Xplore,* disponibile in open access presso: «https://openaccess.thecvf.com/content_cvpr_2017/papers/Dekel_On_the_Effectiveness_CVPR_2017_paper.pdf» (Ultimo accesso: 10 maggio 2022).
[389] Per maggiori informazioni si veda: Ufficio dell'Unione europea per la proprietà intellettuale, *Automated content recognition: discussion paper. Phase 1, Existing technologies and their impact on IP*, cit., 15 e ss.

Il *fingerprinting*, letteralmente "impronta digitale", consiste in una specifica tecnologia di *Digital Rights Management* che si struttura disponendo un file indissolubilmente legato ad un altro che ne funge da impronta di riferimento[390].

A differenza del *watermarking*, il *fingerprinting* non aggiunge alcuna informazione al contenuto, ma lo analizza per identificare alcune delle sue proprietà intrinseche. L'impronta digitale è molto simile *all'hashing*. La differenza principale è che invece di generare una stringa di caratteri basata sulle caratteristiche di un file digitale, le impronte digitali vengono generate in base alle caratteristiche del *contenuto* effettivo di quel file. Anche il processo di *fingerprinting* ha due fasi separate: una prima di generazione dell'impronta, ed una seconda di "confronto" delle impronte digitali. La generazione delle impronte digitali utilizza un peculiare software per analizzare ed estrarre caratteristiche riconoscibili e altre informazioni dal contenuto, quindi, generare una stringa di valori che descrivono le caratteristiche e le informazioni estratte e memorizzare le impronte generate in un database di riferimento. Il confronto delle impronte digitali, poi, utilizza un software specifico per analizzare ogni singolo contenuto nuovo o sconosciuto dal sistema e generare un'impronta digitale. L'impronta digitale generata viene confrontata con tutte le impronte memorizzate nel database di riferimento per vedere se sovviene una corrispondenza[391].

Proprio come *l'hashing*, il *fingerprinting* limita la quantità di dati che devono essere archiviati nel database di riferimento e che devono essere confrontati. Ciò riduce significativamente l'archiviazione dei dati e la potenza di calcolo necessaria per confrontare due contenuti.

Il *fingerprinting* può essere utilizzato per identificare immagini, contenuti video o audio, con un elevato livello di accuratezza, anche ove il contenuto dovesse essere stato alterato o modificato (ad esempio un'immagine sfocata o la registrazione di un film da uno schermo televisivo). Gli strumenti più avanzati possono persino riconoscere una melodia in una versione *cover* di un altro interprete[392].

Approcci diversi possono essere utilizzati per diversi tipi di contenuto. Nell'ipotesi di applicazione ad un file testuale le parole ivi contenute vengono estratte dall'intero testo per generare un'impronta digitale; ciò può essere ottenuto selezionando parole specifiche, utilizzando algoritmi per ordinare le parole seguendo uno schema specifico o semplicemente assumendo il testo grezzo come impronta digitale del documento. In ipotesi di applicazione ad un file fotografico od una immagine, le caratteristiche spaziali uniche di un'immagine possono essere analizzate per identificare aree o punti specifici di quell'immagine, poiché questi non sono, solitamente, destinati a cambiare anche ove l'immagine dovesse essere ridimensionata, riorientata, distorta o ne fosse cambiata la luminosità. In merito ai file video, ancora, tramite il *fingerprinting* viene solitamente estratto un campione statistico del contenuto per generare un'impronta digitale dell'intero contenuto audiovisivo o solo di una parte di esso[393].

---

390 Per maggiori informazioni si vedano: R. CASO, *Digital rights management: il commercio delle informazioni digitali tra contratto e diritto d'autore*, cit., 24 e ss.; Ufficio dell'Unione europea per la proprietà intellettuale, *Automated content recognition: discussion paper. Phase 1, Existing technologies and their impact on IP*, cit., 15 e ss.

391 Ufficio dell'Unione europea per la proprietà intellettuale, *Automated content recognition: discussion paper. Phase 1, Existing technologies and their impact on IP*, cit., 15 e ss.

392 L'esempio in questo caso è quello della tecnologia di *fingerprinting* offerta da *Shazam*, capace di riconoscere i file audio tramite il microfono del dispositivo da cui viene utilizzato il software. Per maggiori informazioni si rimanda al sito ufficiale: «https://www.shazam.com/it/company» (Ultimo accesso: 10 maggio 2022).

393 In merito all'audio ed al video fingerprinting si veda F. LEFEBVRE, B. CHUPEAU, A. MASSOUDI, E. DIEHL, *Image and video fingerprinting: forensic applications, Proc. SPIE 7254, Media Forensics and Security*, 725405 (February

Gli esempi precedenti hanno lo scopo di illustrare come le tecniche di *fingerprinting* possono applicarsi a diversi tipi di contenuto. Più elementi vengono estratti, più accurata e robusta è l'impronta che ne deriva, ma anche più dati devono essere archiviati nel database di riferimento e maggiore è la potenza di calcolo necessaria per confrontare le impronte digitali.

Similmente a quanto già analizzato per il *watermarking*, le soluzioni di *fingerprinting* vengono utilizzate per "segnalare" e identificare i contenuti illeciti. Tuttavia, ai fini del presente elaborato interessa maggiormente ove venga utilizzato dalle piattaforme di condivisione dei contenuti per rilevare l'uso di contenuti protetti da *copyright*. Esso viene utilizzato, fra le altre cose, per applicare politiche specifiche definite dai titolari dei diritti d'autore, incluso il blocco o la monetizzazione dell'uso dei loro contenuti.

Alcune aziende sono specializzate nell'uso delle tecnologie di *fingerprinting* per monitorare le piattaforme di condivisione video e identificare copie piratate di contenuti video, anche se i contenuti sono stati modificati o degradati. È il caso di Vobile[394] che fornisce anche servizi per l'invio di avvisi di rimozione e per identificare in tempo reale una violazione della proprietà intellettuale.

Come ha recentemente notato anche l'Ufficio statunitense per il Copyright, molti settori utilizzano già un'ampia varietà di strumenti tecnologici per facilitare le operazioni nell'ambito della procedura di notice and take down prevista, come ricordato nel secondo capitolo, dalla §512 del DMCA. Questi strumenti includono una varietà di tecnologie di *fingerprinting*, che sono state adottate e impiegate da ISP e titolari di diritti tra i quali, per importanza, si segnalano *Facebook, SoundCloud, Twitch, Vimeo* e *Verizon Wireless*. Il Copyright Office statunitense in particolare nota come gli ISP ed i titolari dei diritti d'autore possano negoziare una risposta specifica ad un'eventuale corrispondenza carpita dai sistemi di *fingerprinting*, come ad esempio scegliere di bloccare il caricamento del contenuto lesivo o consentirne il caricamento ma monetizzarlo. [395]

In generale, le tecniche di *fingerprinting* offrono un elevato livello di accuratezza[396]. La precisione dipende chiaramente dal numero di caratteristiche riconoscibili che vengono estratte per generare l'impronta digitale. Il livello di accuratezza dipende anche dalla capacità della soluzione di *fingerprinting* di riconoscere brevi estratti e di escludere automaticamente parti irrilevanti del contenuto durante l'esecuzione del riconoscimento. In generale, l'impostazione di una soglia di qualità troppo elevata per il riconoscimento del software comporterebbe un livello elevato di falsi negativi per contenuti leggermente alterati. Al contrario, se la soglia impostata è troppo bassa, lo strumento di riconoscimento potrebbe rilevare in eccesso, determinando un livello elevato di falsi positivi.

Come ricorda anche il Copyright Office statunitense, l'efficacia e l'efficienza di questa tecnologia dipende dal miglioramento dei dati che alimentano i sistemi di *fingerprinting*. La

---

2009), 2, liberamente accessibile presso: «https://www.spiedigitallibrary.org/conference-proceedings-of-spie/7254/1/Image-and-video-fingerprinting-forensic-applications/10.1117/12.806580.short?SSO=1» (Ultimo accesso: 10 maggio 2022); Ufficio dell'Unione europea per la proprietà intellettuale, *Automated content recognition: discussion paper. Phase 1, Existing technologies and their impact on IP*, cit., 15 e ss.

394 Si veda in merito il sito Internet di Vobile, operante per Netflix, presso: «http://www.vobilegroup.com/rightsid/» (Ultimo accesso: 10 maggio 2022).

395 Per maggiori riferimenti in merito all'analisi dei sistemi di *fingerprinting* con riferimento alla dinamica statunitense di veda: United States Copyright Office, *Section 512 of Title 17, A Report Of The Register Of Copyrights*, cit., 42 e ss.

396 Ufficio dell'Unione europea per la proprietà intellettuale, *Automated content recognition: discussion paper. Phase 1, Existing technologies and their impact on IP*, cit., 21 e ss.

qualità dei dati, così come l'accessibilità economica della tecnologia, si basa sul coinvolgimento dei creatori e sulla cooperazione fra le parti interessate durante tutto il processo. Poiché la tecnologia di filtraggio dei contenuti si basa intrinsecamente su file di riferimento e dati forniti dai titolari dei diritti, l'ufficio ricorda che la tecnologia non può sfruttare appieno il suo potenziale a meno che i proprietari dei diritti d'autore non siano disposti a fornire file di riferimento e non siano disposti a gestire attivamente tali dati[397].

4.4. AI-based/enhanced recognition

Diverse società tecnologiche stanno fornendo a terzi servizi di riconoscimento basati sull'intelligenza artificiale. Questo è in particolare il caso della tecnologia AWS Amazon Rekognition[398], Image Search fornita da Alibaba Cloud[399] od ancora la tecnologia Computer Vision di Microsoft Azure[400].

Questa tecnologia di riconoscimento dei contenuti sfrutta le forze computazionali ed algoritmiche dell'intelligenza artificiale ai fini di *enforcement* del diritto d'autore sul web. Tale modello di gestione dei diritti può essere, ad esempio, utilizzato a fini di riconoscimento di immagini quali i loghi o altri segni distintivi dell'impresa, tenendo traccia delle menzioni di questi sul web e del sentimento degli utenti sui social media connesso a tali segni. Questi servizi possono essere utilizzati anche per rilevare i loghi che compaiono negli elenchi di e-commerce per prodotti contraffatti. Alcuni dei principali mercati di e-commerce, come Amazon, stanno sviluppando le proprie soluzioni in questo campo. Un ulteriore esempio di tecnologie basate sull'intelligenza artificiale sono quelle tipicamente impiegate nel campo del riconoscimento ottico dei caratteri (OCR).

Le soluzioni di riconoscimento basate sull'intelligenza artificiale consentono di raggruppare, classificare e contrassegnare i contenuti da esse processate con un elevato grado di accuratezza, migliorando così il livello di gestione dei contenuti. Servizi come il "*tagging automatico delle immagini*", per esempio, analizzano i pixel di fotografie o altre opere digitali ed estraggono funzioni per assegnare automaticamente parole chiave ad un'immagine.

La tecnologia basata sull'intelligenza artificiale trova sicuramente il suo principale *habitat naturale* sul web e nel mondo online. Per esempio, il mercato online GOAT[401], specializzato nel commercio di calzature, utilizza il riconoscimento delle immagini per identificare e autenticare le scarpe nel suo magazzino a fini del rilevamento di eventuali falsi. Tuttavia, anche nel mondo "off-line" si può notare come vi sia sempre un maggiore spazio per soluzioni basate sull'intelligenza artificiale nel riconoscimento dei contenuti. In questo caso, il riferimento è ai prodotti sviluppati da Entrupy[402], che ha sfruttato l'intelligenza artificiale per offrire servizi di rilevamento dell'autenticità di alcuni prodotti di lusso,

---

397 United States Copyright Office, *Section 512 of Title 17, A Report Of The Register Of Copyrights*, cit., 42 e ss.
398 Si veda in merito il sito: «https://aws.amazon.com/it/rekognition/customers/» (Ultimo accesso: 10 maggio 2022).
399 Si veda in merito il sito: «https://www.alibabacloud.com/product/imagesearch» (Ultimo accesso: 10 maggio 2022).
400 Si veda in merito il sito: «https://azure.microsoft.com/en-us/services/cognitive-services/computer-vision/» (Ultimo accesso: 10 maggio 2022).
401 Si veda in merito il sito ufficiale di GOAT presso: «https://www.goat.com/verification» (Ultimo accesso: 10 maggio 2022).
402 Si veda in merito il sito ufficiale di Entrupy presso: «https://www.entrupy.com» (Ultimo accesso: 10 maggio 2022).

commercializzando dispositivi mobili od applicazioni per i rivenditori, utili ad autenticare i prodotti.

Simili tecnologie inoltre possono essere utilizzate anche per il rilevamento delle violazioni online del *copyright*, con servizi di supporto per recuperare denaro in caso di violazione. Poiché l'IA richiede l'archiviazione, l'elaborazione e l'analisi di grandi quantità di dati, necessita di risorse computazionali significative, in particolare nel campo del riconoscimento di immagini e video. Inoltre, l'accuratezza di una determinata tecnologia dipende in gran parte dalla quantità di dati o dei contenuti forniti.[403] Un simile strumento di *enforcement* dei diritti sul web richiede sicuramente anche una notevole mole di lavoro da parte di professionisti tecnici altamente qualificati nel settore, impiegati al fine di trovare il modello di *machine learning* più appropriato in relazione allo scopo, motivo per cui l'utilizzo di simili sistemi è ancora in fase di sperimentazione.

4.5. Applicazioni pratiche:

4.5.1. YouTube: il "Content ID" ed il suo "Matching tool"

Il sistema di *Digital Rights Management* che si basa su queste tecnologie per la gestione del *copyright* sulla sua piattaforma è sicuramente il c.d. *Content ID* di *Youtube*. Esso è un sistema che si basa, principalmente, sul *fingerprinting*, utilizzabile per riconoscere la parte audio o video di un determinato contenuto, verificando se esso violi o meno i diritti dei *copyright holders* che si avvalgono di tale strumento. Il *Content ID* in particolare si occupa della gestione e della monetizzazione dei contenuti, sulla base di una valutazione della corrispondenza tra quelli che sono stati rivendicati e aggiunti al suo database di riferimento e i contenuti appena caricati su *YouTube*[404].

Nello specifico, prendendo a riferimento direttamente quanto Google scrive nelle sue pagine informative in merito[405], si legge che il *Content ID* consente ai titolari del *copyright* di identificare e gestire facilmente i propri contenuti su *YouTube*. I video caricati su *YouTube* vengono esaminati e confrontati con un database di file che *YouTube* stesso riceve dai proprietari dei contenuti. Una volta identificata una violazione del *copyright*, avverte che "*spetta al titolare del copyright decidere cosa fare nel caso in cui i contenuti di un video di YouTube corrispondano a una delle sue opere. Quando viene trovata una corrispondenza, il video riceve una rivendicazione di Content ID*".

In particolare, secondo gli schemi contrattuali disposti da Google, i titolari del *copyright* possono intraprendere diverse azioni nei confronti di contenuti corrispondenti ai propri: (1) bloccare la visione dell'intero video; (2) monetizzare il video pubblicando annunci, talvolta condividendo le entrate con l'utente che ha caricato il video; (3) tracciare le statistiche sulle visualizzazioni del video.

---

[403] Maggiori informazioni rinvenibili presso: Ufficio dell'Unione europea per la proprietà intellettuale, *Automated content recognition: discussion paper. Phase 1, Existing technologies and their impact on IP*, cit., 24 e ss.

[404] Maggiori informazioni rinvenibili presso: Ufficio dell'Unione europea per la proprietà intellettuale, *Automated content recognition: discussion paper. Phase 1, Existing technologies and their impact on IP*, cit., 18 e ss.

[405] Il riferimento è alla pagina di supporto Google: *"Funzionamento di Content ID"* consultabile presso: «https://support.google.com/youtube/answer/2797370?hl=it&ref_topic=9282364» (Ultimo accesso: 10 maggio 2022).

A seguito di una rivendicazione di proprietà da parte dei titolari dei diritti, quindi, *YouTube* può generare le "impronte digitali" necessarie al funzionamento del sistema direttamente dal contenuto protetto da *copyright*[406].

Youtube si avvale in ciò del suo "*Copyright Match Tool*", ossia lo strumento in grado di identificare automaticamente i video che corrispondono, effettivamente o potenzialmente, ad altri video su *YouTube*. Quando viene identificata una corrispondenza, il titolare dei diritti d'autore presuntivamente violati può scegliere l'azione da intraprendere.

Il *Copyright Match Tool*[407] è disponibile per tutti gli utenti di *YouTube* che hanno presentato una richiesta di rimozione per violazione del *copyright* valida. Dopo l'approvazione della richiesta, *Copyright Match Tool* inizia a scansionare i caricamenti sulla piattaforma alla ricerca di potenziali corrispondenze con i video indicati dai titolari dei diritti d'autore.

YouTube avverte altresì: "*Prima di esaminare le corrispondenze rilevate, tieni presente che l'individuazione di un video corrispondente non significa necessariamente che tale video violi il tuo copyright. È tua responsabilità esaminare ogni video corrispondente e verificare che ai contenuti non si applichi fair use, fair dealing o un'analoga eccezione al copyright*".

In merito al sistema di *fingerprinting* adottato da *YouTube*, il Copyright Office statunitense nota altresì come esso sia uno dei sistemi di filtraggio più robusti presenti su Internet. Ricorda infatti come esso esegua una scansione dei video caricati sulla piattaforma sulla base di un database di file inviati dai proprietari di contenuti che partecipano al programma. Sulla base dei dati in possesso dall'Ufficio, si stima che, nel 2020, oltre 9.000 titolari dei diritti partecipavano a *Content ID*, rivendicando oltre 800 milioni di video. Negli ultimi cinque anni, *YouTube* ha versato 2 miliardi di dollari ai partecipanti al sistema che abbiano scelto di monetizzare i file utilizzando *Content ID*. Alla luce di questi dati, il Copyright Office afferma proprio come alcune delle parti interessate abbiano lodato il sistema del *Content ID* proprio per aver automatizzato la gestione dei diritti e per aver creato un flusso di entrate completamente nuovo per l'industria musicale consentendo ai titolari dei diritti d'autore, se lo desiderano, di permettere l'accesso ai video ai propri fan e di guadagnare da essi tramite lo strumento ideato da *YouTube*[408].

4.5.2. Audible Magic: Content Recognition

Audible Magic fornisce la sua soluzione di identificazione audio a diverse piattaforme di condivisione. Anche questa, del pari del *Content ID*, si basa sul *fingerprinting*, che consente l'identificazione di colonne sonore digitali e può essere utilizzata per riconoscere i contenuti audiovisivi.

Le impronte digitali possono essere generate gratuitamente dalla stessa *Audible Magic* e integrate nel suo database di riferimento insieme ai metadati relativi al contenuto. Fornisce inoltre la sua soluzione *AMSigGen*, in modo che i titolari dei diritti possano generare autonomamente le impronte digitali e inviarle per essere aggiunte al database di riferimento.

---

[406] Maggiori informazioni rinvenibili presso: Ufficio dell'Unione europea per la proprietà intellettuale, *Automated content recognition: discussion paper. Phase 1, Existing technologies and their impact on IP*, cit., 18 e ss.

[407] Il riferimento è alla pagina di supporto Google: "*Utilizzare Copyright Match Tool",* consultabile presso: «https://support.google.com/youtube/answer/7648743?hl=it&ref_topic=9282364#» (Ultimo accesso: 10 maggio 2022).

[408] Per maggiori riferimenti in merito all'analisi del *Content ID* di *YouTube* con riferimento al sistema americano si veda: United States Copyright Office, *Section 512 of Title 17, A Report Of The Register Of Copyrights*, cit., 42 e ss.

Queste soluzioni possono essere integrate direttamente nella catena di fornitura digitale di un titolare dei diritti o utilizzate da terze parti che agiscono per loro conto. Le soluzioni di *Audible Magic* consentono ai titolari dei diritti d'autore di bloccare, permettere o monetizzare l'uso dei loro contenuti. Attraverso il servizio *AMLive*, Audible Magic fornisce una soluzione per impedire la ritrasmissione in tempo reale di contenuti da parte degli utenti di piattaforme di live streaming. *Audible Magic* è in ciò utilizzato da diverse piattaforme di condivisione dei contenuti, tra cui *Dailymotion*, *Twitch*, *Soundcloud* o *TikTok*.

Nel sito dedicato al software in merito si legge "*la nostra tecnologia brevettata ACR identifica qualsiasi supporto in base alle caratteristiche percettive dell'audio e del video. Funziona su formati di file, codec, bit rate e algoritmi di compressione. Con tassi di identificazione del 99,99%, la tecnologia di riconoscimento dei contenuti di Audible Magic produce praticamente zero falsi positivi e non richiede alcuna dipendenza da metadati, filigrane o hash di file. Il nostro approccio è inoltre immune da molti tipi di trasformazioni o rumori di fondo*"[409].

Aggiunge inoltre: "*Quando si combina VideoID con i servizi di riconoscimento dei contenuti, è possibile identificare il video senza audio e l'audio senza video. Progettata per soddisfare le esigenze di eventi live internazionali con copertura multimediale in più lingue che viene spesso trasmessa in streaming su piattaforme social, questa solida soluzione gestisce il degrado della qualità video, le modifiche alla frequenza dei fotogrammi, le modifiche alle proporzioni, i ticker e le sovrapposizioni grafiche e altro ancora*[410]"

4.5.3. Facebook Rights Manager

Nel 2016, come ricorda il Copyright Office statunitense, *Facebook* ha sviluppato il proprio strumento di riconoscimento dei contenuti chiamato *Rights Manager*, consistente in una tecnologia di abbinamento video intesa, dichiaratamente, ad aiutare ulteriormente i titolari dei diritti a proteggere i contenuti che possiedono[411]. *Rights Manager* consente agli editori approvati di caricare e mantenere una libreria di riferimento di video; creare regole su come vengono utilizzati i video in base, ad esempio, a quanti contenuti sono stati riutilizzati o quante visualizzazioni sono state ricevute; identificare nuove corrispondenze. Originariamente, il sistema di *Rights Manager* era prevalentemente manuale: una volta che *Rights Manager* avesse individuato le corrispondenze, il sistema stesso non avrebbe potuto inviare notifiche automatiche. Nell'ottobre 2017, *Facebook* ha iniziato a integrare direttamente *Rights Manager* con servizi di fornitori di terze parti per consentire una maggiore automazione

---

[409] Sul sito dedicato al funzionamento di Audible Magic («https://www.audiblemagic.com/technology/» (Ultimo accesso: 10 maggio 2022)) si legge: "*Our patented ACR technology identifies any media based on perceptual characteristics of the audio and video. This works across file formats, codecs, bit rates, and compression algorithms. With identification rates at 99.99%, Audible Magic's content recognition technology produces virtually zero false positives and requires no dependence on metadata, watermarks, or file hashes. Our approach is also immune to many types of transformations or background noise".*

[410] Sul sito dedicato al funzionamento di Audible Magic, cit., si legge: "*When you combine VideoID with content recognition services, you can identify video without audio and audio without video. Designed to meet the needs of international live events with multiple language media coverage that is often streamed on social platforms, this robust solution handles video quality degradation, frame rate changes, aspect ratio changes, tickers and graphic overlays and more.*"

[411] A. T. KEEF & L. BEN-KERETH, *Introducing Rights Manager*, in *FACEBOOK FOR MEDIA* (Apr. 12, 2016), liberamente accessibile presso: «https://www.facebook.com/facebookmedia/blog/introducing-rights-manager» (Ultimo accesso: 10 maggio 2022); si faccia altresì riferimento a FACEBOOK, INC. ("Facebook"), *Comments Submitted in Response to U.S. Copyright Office's Dec. 31, 2015, Notice of Inquiry at 6* (Apr. 1, 2016) ("Facebook Initial Comments") ("[T]he tool flags uploaded videos that match the rights owners' content and allows those rights owners to quickly and efficiently report the videos to Facebook for removal.").

e nel febbraio 2018 ha ampliato il suo strumento per coprire i contenuti video pubblicati su Instagram[412].

Ad oggi, *Facebook Rights Manager* si basa sull'architettura del *fingerprinting*. Le impronte digitali vengono generate direttamente dai titolari dei diritti utilizzando *l'API Rights Manager*[413]. Il titolare dei diritti può impostare la propria politica di gestione dei contenuti, decidendo se preferisce bloccare il contenuto, monetizzarlo o applicare l'attribuzione, in modo che il sistema possa intervenire in caso di corrispondenza[414].

Facebook stesso definisce il suo sistema come "*Uno strumento potente e altamente personalizzabile. [..] È progettato per le persone che vogliono controllare quando, come e dove i propri contenuti vengono condivisi su Facebook e Instagram*[415]" Per avvalersene, un titolare di diritti d'autore, deve aggiungere i contenuti che desidera proteggere in una libreria di riferimento usata da *Rights Manager* per scovare qualsiasi contenuto su *Facebook* e *Instagram* che corrisponda a quello così caricato. Ove il contenuto dovesse essere rilevato su una pagina o un profilo del gruppo *Facebook*, il *copyright holder* può scegliere tra diverse azioni disponibili. Ciò può includere il monitoraggio del contenuto, il blocco o l'attribuzione di crediti tramite un collegamento di proprietà."[416].

Fra le misure che *Facebook* consente di adottare si annoverano il blocco del video, tale per cui un video bloccato non può essere visualizzato da nessuno, ad eccezione della persona che lo ha pubblicato o richiedere il denaro guadagnato da un video che contiene pause pubblicitarie. In aggiunta si può altresì chiedere di inserire un banner di rimando al titolare originario sotto un video, ed infine usare *Rights Manager* per inviare a *Facebook* una segnalazione di violazione del diritto d'autore, che potrebbe comportare la rimozione del video segnalato.

Facebook utilizza altresì, nella gestione dei contenuti online, i software di *Audible Magic* per evitare la pubblicazione di video non autorizzati. I video caricati su *Facebook* vengono infatti sottoposti ad un controllo tramite *Audible Magic* al momento del caricamento. Se viene individuata una corrispondenza, il caricamento viene interrotto e l'utente ne riceve una notifica.

---

412 Per maggiori riferimenti in merito all'analisi dei sistemi di Facebook Rights Manager con riferimento al sistema americano si veda: United States Copyright Office, *Section 512 of Title 17, A Report Of The Register Of Copyrights*, 45 e ss, liberamente accessibile presso: «https://www.copyright.gov/policy/section512/section-512-full-report.pdf» (Ultimo accesso: 10 maggio 2022)

413 Per maggiori informazioni si veda il case study "Facebook Inc.'s Rights Manager" affrontato con dovizia di dettagli in J. P. QUINTAIS, P. MEZEI, I. HARKAI, J. C. MAGALHÃES, C. KATZENBACH, S. F. SCHWEMER, & T. RIIS, *Final Report on mapping of EU legal framework and intermediaries' practices on copyright content moderation and removal*, 2022, 149 e ss, in *Zenodo*, liberamente accessibile presso: «https://doi.org/10.5281/zenodo.6461568» (Ultimo accesso: 10 maggio 2022).

414 Maggiori informazioni rinvenibili presso: Ufficio dell'Unione europea per la proprietà intellettuale, *Automated content recognition: discussion paper. Phase 1, Existing technologies and their impact on IP*, cit., 18 e ss.

415 Sul sito di Facebook («https://rightsmanager.fb.com» (Ultimo accesso: 10 maggio 2022)) si legge, nella versione originale inglese: "*A powerful, highly customizable tool, Rights Manager lives within Facebook's Creator Studio platform. It's built for people who want to control when, how, and where their content is shared across Facebook and Instagram. From creators who post their own unique content to publishing houses that don't post to Facebook at all, Rights Manager can be customized to meet business goals of any size*".

416 Sul sito si legge, nella versione originale inglese "*To get started, you'll add content you've created and want to protect into a reference library. Rights Manager will take it from there, finding any content on Facebook and Instagram that matches yours. You can also adjust the match settings to specify such things as if your ownership should apply worldwide or only in certain locations. When your content is detected on a Page or profile, you can choose from one of the available actions that works best for you. This can include monitoring the content, blocking it or attributing credit via an ownership link. You can even add trusted partners and properties to protect them from matching your reference files.*"

5. DRM e Privacy

Ricordando le strategie di *enforcement* dei diritti d'autore nel contesto digitale [417] che accompagnano il presente elaborato sin dal principio del secondo capitolo, lo strumento qui analizzato del *Digital Rights Management* si dimostra immediatamente in forte tensione con il diritto alla privacy degli utenti e con esso necessita di essere bilanciato[418]. Come abbiamo avuto modo di constatare infatti, il potere tecnologico, contrattuale e normativo connesso all'implementazione di tecnologie di varia natura, volte alla protezione del diritto d'autore, si basa sulla acquisizione di dati personali degli utenti, realizzando un esteso monitoraggio dei comportamenti degli stessi ed in particolare del consumo di prodotti intellettuali da essi compiuto. Tramite un simile monitoraggio, infatti, i sistemi di DRM, rinviando ai titolari dei contenuti digitali numerose informazioni sulle attività dei fruitori, comprimono la privacy degli utenti.

I sistemi più diffusi di *Digital Rights Management*, infatti, contemplano la possibilità di sorvegliare gli utenti nella fruizione dei contenuti o dei servizi con la connessa possibilità di sanzionare gli utenti stessi, ad esempio con la disattivazione di un servizio, nell'ipotesi in cui dal monitoraggio emerga una violazione delle regole contrattuali stabilite dalle licenze.

I problemi sono connessi chiaramente anche alla profilazione dell'utente, volta a definire i gusti ed i comportamenti dei consumatori, spesso a fini di una personalizzazione degli annunci pubblicitari. Testimoni ne sono quell'insieme di tecnologie quali *cookies, spyware ed adware* capaci di tracciare un dettagliato profilo dei comportamenti degli utenti.

Organizzare un controllo ferreo sulle informazioni digitali finisce necessariamente, come nota Palmieri[419], con l'interferire con la sfera privata del fruitore, attuale o potenziale, di tali informazioni. Il monitoraggio delle peculiari modalità con cui ciascun utente si rapporta a un certo prodotto informativo, comporta, infatti, la creazione di repertori di dati personali, i quali, necessariamente devono rispondere ai criteri per il loro trattamento disposti dalla normativa nazionale e sovranazionale in materia di dati personali.

Palmieri inoltre nota che "*diffusa è, invero, la percezione che i sistemi DRM, oltre a scontare le indubbie difficoltà con cui l'utente vi si accosta, creano in quest'ultimo una certa insicurezza, vuoi perché permettono di abusare dei dati personali, vuoi perché non li trattano con le precauzioni che sarebbero da attendersi. Al che si imputa, assieme al ravvisato scollamento tra tecnologie e reali esigenze dell'utente, la frenata dei mercati dei prodotti digitali, nel senso che la loro crescita effettiva appare inferiore rispetto al loro potenziale*"[420].

Il condizionamento del consumo intellettuale, incidendo nella sfera di autodeterminazione degli individui, pone direttamente limiti al comportamento degli utenti. Tali tecnologie delimitano e restringono direttamente lo spazio di libertà legato al consumo intellettuale, riducendo l'autonomia di cui un soggetto gode nell'uso di un prodotto

---

417 R. CASO, *Il conflitto tra copyright e privacy nelle reti Peer to Peer: il caso Peppermint – Profili di diritto comparato*, cit. 5 e ss.

418 Per l'esperienza statunitense, si veda J. COHEN, *DRM and Privacy*, cit.; per la prospettiva europea: L. A. BYGRAVE, *Digital Rights Management and Privacy – Legal Aspects in the European Union*, in E. BECKER et al. (eds.), *Digital Rights Management Technological, Economic, Legal and Political Aspects*, Berlin, 2003, 418.

419 A. PALMIERI, *Drm e Disciplina Europea della Protezione dei Dati Personali* in R. CASO (a cura di), *Digital Rights Management: problemi teorici e prospettive applicative*. Atti del Convegno tenuto presso la Facoltà di Giurisprudenza di Trento il 21 ed il 22 marzo 2007, Università di Trento, Trento, 2008, 197-215, liberamente accessibile presso: «http://eprints.biblio.unitn.it/1336/» (Ultimo accesso: 10 maggio 2022).

420 A. PALMIERI, *ibidem,* 199.

informativo. Come afferma in merito Roberto Caso, simili tecnologie "*dislocano dal fruitore al titolare dei contenuti la scelta relativa al consumo intellettuale*"[421].

Una attenta dottrina d'oltreoceano[422], come vedremo, distingue, in connessione ai sistemi di *Rights Management* ed al loro influsso in termini di riservatezza, fra una privacy "spaziale" ed una "concettuale", ambedue compromesse, se non annullate, dal massiccio uso di simili tecnologie.

Inoltre, i sistemi digitali realizzano un'ulteriore strategia, ossia quella di autotutela. Le funzionalità di sanzione tipiche del DRM, operando in congiunzione a quelle di monitoraggio, possono essere attivate automaticamente dal sistema stesso di *Rights Management*. Nel fare questo, esse identificano un particolare fruitore di contenuti digitali come il bersaglio di una misura di autotutela: tale utente patisce quindi una classificazione perdendo il conseguente anonimato.

Prima di analizzare nello specifico queste concezioni della privacy e quindi i bilanciamenti che devono essere compiuti in merito *all'enforcement* del diritto d'autore in questo contesto, è bene partire da due esempi pratici di come la tecnologia in commento abbia avuto modo di destare preoccupazioni presso gli utenti.

5.1. Celebri Esempi

5.1.1. Sony *Rootkit*

Lo scandalo che ha coinvolto la Sony BMG nel 2005 riguardava l'adozione di sistemi di *Digital Rights Management*, in particolare sotto forma di misure anticopia, su circa 22 milioni di CD distribuiti dalla Sony stessa[423]. I CD, in particolare, istallavano un software che forniva una forma di gestione dei diritti digitali che, modificando il sistema operativo, impediva la copia (c.d "*CD Burning*") dei CD. I componenti software in questione non potevano essere facilmente disinstallati e crearono vulnerabilità sfruttate da *malware* e *virus*. Il software inoltre procedeva ad inviare alla Sony rapporti sulle abitudini di ascolto privato dell'utente, anche se l'utente rifiutava il contratto di licenza allegato.

In particolare, il programma per elaboratori raccoglieva (1) l'indirizzo IP dell'utente, (2) il tipo di sistema operativo utilizzato sul computer, (3) la versione di Internet Explorer installata sul computer dell'utente ed infine (4) i titoli delle canzoni che l'utente aveva caricato sul suo computer[424]. In tutto ciò la licenza affermava "*The Software will not be used at any time to collect any personal information from you, whether stored on your computer or otherwise*[425]". Queste componenti erano altresì strutturate per nascondere l'esistenza del software.

---

421 R. CASO, *Digital rights management: il commercio delle informazioni digitali tra contratto e diritto d'autor*e, cit., 105.

422 Il riferimento è a J. E COHEN, *DRM and Privacy*, 13 *Berkeley Tech.* L.J. 575 (2003), liberamente accessibile presso: «https://scholarship.law.georgetown.edu/facpub/60» (Ultimo accesso: 10 maggio 2022).

423 Per un approfondimento dal punto di vista tecnico e giuridico sul caso rootkit si veda M. M. LABELLE, *The 'Rootkit Debacle': The Latest Chapter in the Story of the Recording Industry and the War on Music Piracy* (2006) in *Denver University Law Review*, Vol. 84, No. 1, p. 79, 2006, CUA Columbus School of Law Legal Studies Research Paper No. 2010-28, liberamente accessibile presso: «https://ssrn.com/abstract=1564903» (Ultimo accesso: 10 maggio 2022); J. A. HALDERMAN, E. W. FELTEN, *Lessons from the Sony DRM Episode*, *Ctr. for Info. Tech., Princeton Univ., Dep't of Computer Sci., Working Paper,* 2006 liberamente accessibile presso: «http://itpolicy.princeton.edu/pub/sonydrm-ext.pdf» (Ultimo accesso: 10 maggio 2022).

424 M. M. LABELLE, *The 'Rootkit Debacle': The Latest Chapter in the Story of the Recording Industry and the War on Music Piracy*, cit., 89-101

425 M. M. LABELLE, *The 'Rootkit Debacle': The Latest Chapter in the Story of the Recording Industry and the War on Music Piracy*, cit., 89-101

Infatti, il problema principale, oltre alla vulnerabilità che ingenerava, era sicuramente legato al fatto che tale istallazione del software, pur se dichiarata *nell'End Users License Agreement* (EULA), difettava sia di un'idonea identificazione che di uno strumento di rimozione. Inoltre, tale programma era in grado di interferire con il normale funzionamento del sistema operativo Microsoft Windows, nonché con la lettura degli stessi CD musicali[426]. A ciò va aggiunto che L'EULA non dichiarava la reale natura del software installato né i rischi di sicurezza e privacy creati.

Sony BMG inizialmente aveva negato che i software così introdotti nei computer degli utenti fossero dannosi. Mossa tuttavia dalla preoccupazione presso il pubblico, decise di rilasciare, per uno dei componenti software, un "programma di disinstallazione" che invece procedeva ad installare un software aggiuntivo che non poteva essere rimosso facilmente. Tale programma, quindi, peggiorava quasi la situazione, infatti raccoglieva altresì gli indirizzi e-mail dell'utente e introduceva ulteriori vulnerabilità di sicurezza.

Tale software, così come delineato nei suoi tratti essenziali, venne definito come "*rootkit*". Nicola Lucchi nota come il termine *rootkit* nasca dall'unione dei due termini *root* e *kit*. "*Il primo indica quello che nei sistemi operativi Unix è l'utente administrator. Il secondo termine indica un insieme di strumenti adibiti allo svolgimento di un determinato scopo. Un rootkit, dunque, è un insieme di strumenti software attraverso i quali è possibile acquisire i privilegi di amministratore del computer infettato. Per raggiungere tale obiettivo, il rootkit è solitamente in grado di nascondere la propria presenza e le proprie tracce anche ai software anti-virus*"[427].

L'installazione di tale software aveva quindi come effetto collaterale quello di aprire delle "falle di sicurezza". In altri termini, esso avrebbe prodotto una breccia nel sistema operativo utilizzabile per accedere al computer e quindi alle informazioni ivi contenute. Il computer dell'utente colpito da tale software, quindi, sarebbe stato estremamente vulnerabile ad attacchi esterni, consentendo l'accesso a qualsiasi informazione contenuta nel dispositivo dell'utente, comprese informazioni finanziarie o sensibili, in ogni caso, quindi, dati personali.

Lo scandalo si fa risalire al 31 ottobre del 2005 quando Mark Russinovich[428] postò nel suo blog una attenta analisi dei componenti tecnici del software anticopia della Sony (*F4I's XCP, Extended Copyright Protection*). Russinovich in tale contesto paragonava il software a un *rootkit* a causa della sua installazione clandestina e dei suoi sforzi per nasconderne l'esistenza. Osservava che l'EULA non menzionava il software e affermava con enfasi che il programma per elaboratore fosse illegittimo e che la gestione dei diritti digitali era "*andata troppo oltre*". Russinovich scoprì infatti numerosi problemi di questa componente software, in particolare, che essa creava falle di sicurezza che potevano essere sfruttate da software dannosi come *worms* o *virus*. Inoltre, rallentava significativamente il computer dell'utente, indipendentemente dalla riproduzione di un CD protetto o meno. Inoltre, Russinovich riconosceva come tale software fosse installato in modo tale che tentativi inesperti di

---

[426] Per maggiori riferimenti si veda N. LUCCHI, *DRM, Contratto e Protezione dei Consumatori,* in R. CASO (a cura di), *Digital Rights Management: problemi teorici e prospettive applicative.* Atti del Convegno tenuto presso la Facoltà di Giurisprudenza di Trento il 21 ed il 22 marzo 2007, Università di Trento, Trento, 2008, 127-167, liberamente accessibile presso: «http://eprints.biblio.unitn.it/1336/» (Ultimo accesso: 10 maggio 2022).

[427] Per maggiori riferimenti si veda N. LUCCHI, *DRM, Contratto e Protezione dei Consumatori,* in R. CASO (a cura di), *Digital Rights Management: problemi teorici e prospettive applicative, cit., 136, nota n.18*.

[428] M. RUSSINOVICH, *Sony, Rootkits and Digital Rights Management Gone Too Far*, 31 ottobre 2005, in *Mark's Blog. Microsoft MSDN*, liberamente accessibile presso: «https://web.archive.org/web/20150317040653/http://blogs.technet.com/b/markrussinovich/archive/2005/10/31/sony-rootkits-and-digital-rights-management-gone-too-far.aspx» (Ultimo accesso: 10 maggio 2022).

disinstallarlo avrebbero potuto portare il sistema operativo a non riconoscere le unità esistenti[429].

In seguito al contributo di Russinovich, Sony BMG rilasciò rapidamente un software per rimuovere il componente *rootkit* di XCP dai computer Microsoft Windows interessati. Russinovich tuttavia, non convinto, analizzò nuovamente il software così fornito per la disinstallazione, notando come tale implementazione avesse solo esacerbato i problemi di sicurezza e sollevato ulteriori preoccupazioni sulla privacy degli utenti[430]. Infatti, il programma di disinstallazione non aveva raggiunto il risultato sperato. Per scaricare il programma di disinstallazione, inoltre, era necessario fornire un indirizzo e-mail e installare un controllo *ActiveX* contenente metodi *backdoor* potenzialmente pericolosi per attacchi virali.

A seguito dello scandalo pubblico, indagini governative e *class action* svoltesi nel 2005 e nel 2006, Sony BMG decise di affrontare parzialmente la questione con accordi con i consumatori, procedendo ad una revoca di circa il 10% dei CD interessati e la sospensione delle misure di protezione dalla copia dei CD all'inizio del 2007. Nonostante la Sony avesse annunciato il ritiro dal mercato dei prodotti contenti questo software anticopia, i risultati non furono abbastanza rapidi o soddisfacenti per gli utenti statunitensi, risultando in un gran numero di azioni legali contro Sony.

La prima azione legale venne intrapresa in Texas[431] il 21 novembre 2005. In particolare, le accuse affermavano che Sony avesse violato le leggi statali sullo *spyware* e avesse proceduto a porre in essere pratiche commerciali ingannevoli, in quanto il software, veniva notato, sarebbe stato installato su un computer anche se l'utente avesse rifiutato il contratto di licenza che autorizzava l'azione. Il procuratore Abbott, che si occupava del caso, in merito dichiarava: "*Continuiamo a scoprire metodi aggiuntivi utilizzati da Sony per ingannare i consumatori del Texas che pensavano di acquistare semplicemente musica*"[432] e "*Migliaia di texani sono ora potenziali vittime di questo gioco ingannevole che Sony ha giocato con i consumatori per i propri scopi*[433]".

Alla Sony, in esito alla vicenda, venne ordinato di pagare $ 750.000 di spese legali al Texas, accettare i resi dei clienti dei CD interessati, inserire un avviso dettagliato e ben visibile sulla loro home page circa le potenzialità dannose del software[434]. Tuttavia, le vicende legali

---

[429] M. RUSSINOVICH, *Sony, Rootkits and Digital Rights Management Gone Too Far*, cit. Si veda inoltre J. E. COHEN, *The Place of the User in Copyright Law*, *74 Fordham L.Rev.*347 (2005); J. P. LIU, *Copyright Law's Theory of the Consumer*, 44 *B.C. L. Rev.* 397 (2003).

[430] Si veda, per esaustivi riferimenti, il post di M. RUSSINOVICH, *More on Sony: Dangerous Decloaking Patch, EULAs and Phoning Home*, in *TechNet*, 4 novembre 2005, liberamente consultabile presso: «https://techcommunity.microsoft.com/t5/windows-blog-archive/more-on-sony-dangerous-decloaking-patch-eulas-and-phoning-home/ba-p/723452» (Ultimo accesso: 10 maggio 2022).

[431] Si veda in merito l'articolo *Texas Attorney General Brings Lawsuit Against Sony BMG For Spyware*, in *Government Technology,* liberamente accessibile presso: «https://www.govtech.com/security/texas-attorney-general-brings-lawsuit-against.html» (Ultimo accesso: 10 maggio 2022).

[432] Si veda in merito l'articolo del Dallas Business Journal intitolato *AG throws more allegations at Sony BMG*, liberamente consultabile presso: «https://www.bizjournals.com/dallas/stories/2005/12/19/daily31.html» (Ultimo accesso: 10 maggio 2022).

[433] Dallas Business Journal intitolato *AG throws more allegations at Sony BMG*, liberamente consultabile presso: «https://www.bizjournals.com/dallas/stories/2005/12/19/daily31.html» (Ultimo accesso: 10 maggio 2022).

[434] Texas v. Sony BMG Music Entm't, Dist. Ct., Travis Co, Texas, liberamente accessibile presso: «http://www.sonysuit.com/classactions/texas/complaint.pdf» (Ultimo accesso: 10 maggio 2022).

connesse a Sony Rootkit non si arrestarono, ed una *class action* venne intentata negli Stati di New York e della California[435] conclusasi tuttavia in via transattiva[436].

Si è scelto di partire da una dimensione casistica per mostrare le interrelazioni fra *l'enforcement* del diritto d'autore e la tutela della privacy nell'ambito delle misure tecnologiche di protezione. In particolare, come verrà approfondito in seguito, il caso *Sony Rootkit* dimostra la rilevanza dell'interferenza nella sfera privata degli utenti. Questo per numerose ragioni. Innanzitutto, il software di Sony, come detto, monitorava le attività di consumo dei prodotti intellettuali degli utenti, provvedendo ad inviare alla società stessa dei *record* dei comportamenti degli utenti.

Questo monitoraggio costituisce, infatti, un trattamento dei dati personali, in particolare concernente le abitudini di consumo degli utenti. In ciò chiaramente l'illecito derivava dalla assenza di trasparenza della tecnologia utilizzata se non addirittura da un occultamento della stessa. Questo comportava un tracciamento automatizzato di cui gli utenti non erano nemmeno consapevoli al momento dell'acquisto dei CD. Il *record* dei comportamenti degli utenti altresì si svolgeva in una dimensione che essi percepivano come eminentemente privata. Infatti, alcuni spazi, come la casa, sono tradizionalmente intesi come seclusi agli occhi del pubblico e privi dalle interferenze di altri soggetti. Nella dimensione digitale emerge sempre più spesso come altri luoghi debbano intendersi eminentemente privati quali ad esempio i *device* tecnologici come i computer e gli *smartphone*[437], come di seguito si avrà modo di affermare.

5.1.2. Amazon Kindle: 1984 e La Fattoria degli Animali

Un secondo scandalo, dopo *Sony Rootkit*, ha colpito invece Amazon, la nota piattaforma di e-commerce. Infatti, nel 2009, essa aveva cancellato da remoto alcune edizioni digitali di alcuni libri dai dispositivi *Kindle* dei lettori che li avevano in precedenza acquistati. Tale azione era intervenuta in quanto gli *e-books* in questione erano stati aggiunti al negozio Kindle da una società che non ne possedeva i diritti d'autore. Per tale motivo Amazon, informato di tale violazione da parte del reale titolare di diritti d'autore, ha proceduto repentinamente a rimuovere le copie illegali dai dispositivi dei clienti e a rimborsare gli utenti del corrispettivo versato[438]. I libri in questione erano "*1984*" e "*La Fattoria degli Animali*" di George Orwell.

Amazon era stata in grado di rimuovere tali titoli perché lo strumento del *Kindle* è configurato per sincronizzarsi automaticamente con lo scaffale dell'utente tramite il servizio wireless *WhisperNet* offerto dalla medesima piattaforma. Quando la società decise di rimuovere i libri non autorizzati dagli account dei clienti, essi, tramite automatica sincronizzazione, sono scomparsi anche dal *Kindle*. Amazon ha quindi inviato un'e-mail

---

[435] Articolo BBC News: *Sony sued over copy-protected CDs; Sony BMG is facing three lawsuits over its controversial anti-piracy software*, in *BBC News*, 10 novembre 2005, liberamente consultabile presso: «http://news.bbc.co.uk/1/hi/technology/4424254.stm» (Ultimo accesso: 10 maggio 2022).

[436] Articolo New York Times, *Sony BMG Tentatively Settles Suits on Spyware*, in *The New York Times. Associated Press*, 30 dicembre 2005, liberamente accessibile presso: «https://www.nytimes.com/2005/12/30/technology/sony-bmg-tentatively-settles-suits-on-spyware.html» (Ultimo accesso: 10 maggio 2022).

[437] Riley v. California, 136 S. Ct. 506 (2015), liberamente accessibile presso: «https://www.law.cornell.edu/supremecourt/text/13-132» (Ultimo accesso: 10 maggio 2022).

[438] Informazioni in merito al caso rinvenibili nell'articolo apparso sul New York Times: B. STONE, *Amazon Erases Orwell Books From Kindle*, in *New York Times*, 17 luglio 2009, liberamente consultabile presso: «https://www.nytimes.com/2009/07/18/technology/companies/18amazon.html» (Ultimo accesso: 10 maggio 2022).

criptica su ciò che era successo, affermando: "*We recently discovered a problem with a Kindle book that you have purchased. We have processed a refund to the payment method used to acquire this book. The next time the wireless is activated on your device, the problematic item will be removed. If you are not in a wireless coverage area, please connect your device to a computer using your USB cable and delete the file from the documents folder.*"[439]

I due libri in questione erano stati pubblicati per Kindle da una società chiamata *Mobile Reference*, che offriva libri di pubblico dominio a circa $ 1. *Mobile Reference*, tuttavia, non aveva il diritto di vendere i romanzi di Orwell perché sia "*1984"* che "*La Fattoria degli Animali"* erano ancora protetti dal diritto d'autore. Tali volumi elettronici, quindi, non erano copie legittime dei libri, ma piuttosto copie illecite che non avrebbero dovuto essere vendute[440].

Bruce Schneier, Chief Security Technology Officer della British Telecom ed esperto di sicurezza informatica affermava, in esito allo scandalo: "*Come proprietario di Kindle, sono frustrato. Non posso prestare libri alle persone e non posso vendere libri che ho già letto, e ora si scopre che non posso nemmeno contare sull'avere ancora i miei libri domani*[441]".

Anche questo esempio mostra le particolari interferenze con la privacy che i sistemi di *Digital Rights Management* possono portare. La potenza della tecnologia in questo caso si dimostra talmente forte da poter unilateralmente entrare nella libreria degli utenti e privare gli stessi di un libro che pensavano di possedere.

Si immagini, infatti, di procedere all'acquisito dello stesso libro da un rivenditore locale, od anche meglio da una bancarella che vende numerosi volumi della cui provenienza non si può essere certi ma nemmeno diffidenti. Una volta compiuto l'acquisto, in buona fede, si riporti il libro nella propria casa e se ne gusti la lettura del primo capitolo per poi riporlo ordinatamente nella libreria domestica, magari fra gli altri libri dello stesso autore. Si immagini poi di svegliarsi la mattina seguente e dirigersi verso la propria libreria alla ricerca del libro la cui lettura si era interrotta il giorno precedente per scoprire che il volume è sparito. Al suo posto si immagini di trovare le monete con cui si era pagato il libro il giorno prima ed un bigliettino scritto dal commerciante affermante "scusi, abbiamo avuto un problema con il suo libro e abbiamo proceduto a rimuoverlo". Il venditore sarebbe quindi entrato nello spazio fisico dell'acquirente, nella dimora dello stesso, avrebbe rovistato nella sua libreria alla ricerca del libro incriminato, e quindi sottratto alla sua disponibilità. Inaccettabile. Se trasposto nel mondo digitale diventa forse più accettabile? Basta chiamare un libro come "digitale", "e-book", per dimenticarsi dell'accaduto? Probabilmente no.

Il diritto alla privacy, infatti, sebbene non si confonda in toto con il diritto di proprietà, dimostra di avere molte sovrapposizioni con lo stesso, come vedremo. La potenza della tutela

---

[439] Informazioni rinvenibili presso l'articolo N. MOOK, *Media goes crazy over Amazon deleting '1984' from Kindle, but 99-cent ebook was illegal copy*, in *Betanews*, liberamente consultabile presso: «https://betanews.com/2009/07/17/media-goes-crazy-over-amazon-deleting-1984-from-kindle-but-99-cent-ebook-was-illegal-copy/» (Ultimo accesso: 10 maggio 2022). Traducendo liberamente il testo citato: "*Di recente abbiamo scoperto un problema con un libro Kindle che hai acquistato. Abbiamo proceduto ad attribuire un rimborso sul metodo di pagamento utilizzato per acquisire questo libro. La prossima volta che il wireless verrà attivato sul tuo dispositivo, l'elemento problematico verrà rimosso. Se non ci si trova in un'area di copertura wireless, collegare il dispositivo a un computer utilizzando il cavo USB ed eliminare il file dalla cartella dei documenti"*

[440] Informazioni rinvenibili presso N. MOOK, *Media goes crazy over Amazon deleting '1984' from Kindle, but 99-cent ebook was illegal copy*, cit.

[441] Informazioni in merito al caso rinvenibili nell'articolo apparso sul New York Times: B. STONE, *Amazon Erases Orwell Books From Kindle*, in *New York Times*, 17 luglio 2009, cit., in tale contesto, letteralmente si legge: "*As a Kindle owner, I'm frustrated. I can't lend people books and I can't sell books that I've already read, and now it turns out that I can't even count on still having my books tomorrow."*

del diritto d'autore nel mondo digitale permette di avere accesso alla proprietà, anch'essa digitale, ed entrare in via di autotutela nella libreria di un utente per ragioni di *enforcement* del diritto d'autore. È chiaro che il processo in corso è quello che porta ad assottigliare progressivamente i limiti di libertà che gli utenti hanno sempre goduto negli spazi privati in relazione alle attività di consumo intellettuale. Stupisce anche la scarsa trasparenza dell'autotutela realizzata, ricordiamo che infatti Amazon, rimuovendo gli *e-book*, informava i suoi utenti meramente che "avevano avuto un problema".

5.2. Le interferenze con la privacy

In materia di *Digital Rights Management* ed il suo scontro con la tutela della riservatezza si segnala sicuramente il contributo di Julie E. Cohen la quale afferma efficacemente che le tecnologie di gestione dei contenuti digitali comprimono le dimensioni sia "spaziali" che "informazionali" della privacy che i consumatori solitamente potevano aver goduto nel consumo dei prodotti intellettuali[442].

L'autrice parte, infatti, dal presupposto secondo il quale le tecnologie di DRM consistono in uno sforzo per dare una nuova forma alle pratiche ed agli spazi dedicati al consumo intellettuale, creando le potenzialità per una vasta raccolta di informazioni circa le abitudini di consumo dei prodotti protetti dal diritto d'autore. Infatti, la dimensione di quei comportamenti definibili in termini di "consumo intellettuale" è essenzialmente privata e si svolge, solitamente, entro spazi anch'essi privati. L'interesse a mantenere la privacy su questi comportamenti viene identificato in termini di interesse ad un "*breathing space*" uno spazio vitale, costantemente minacciato dalle tecnologie che impongono delle dirette limitazioni o regolamentazioni a tali attività[443].

In questo senso l'autrice distingue due "zone" della privacy in relazione ai sistemi di DRM affermando che di essa vengano in rilievo la dimensione tanto "concettuale" o "intellettuale" quanto "spaziale" o "fisica".

In questo senso la privacy concettuale deriverebbe dall'esigenza degli utenti di affermare la propria autonomia personale. È infatti affermazione comune di tutti i sistemi occidentali quella di un diritto dell'uomo sulla sua stessa persona, diritto che include non solo il controllo sulla propria integrità fisica, ma anche sui propri pensieri e sulla propria personalità. In questo contesto, dunque, una sorveglianza continua ed una obbligazione di "*disclosure*" delle informazioni personali, delle preferenze anche circa il consumo dei contenuti protetti dal diritto d'autore, minaccia nel profondo tali diritti.

Ad avviso di Julie E. Cohen, infatti, sebbene non si possa proibire materialmente ad un soggetto di pensare ciò che desidera, una persistente osservazione può sottilmente modellare, dare forma, a comportamenti, espressioni ed in definitiva alla personalità ed alla

---

442 J. E. COHEN, *DRM and Privacy,* 18 *Berkeley Tech*. L.J. 575-617 (2003), Georgetown Law Faculty Publications and Other Work, liberamente accessibile presso: «https://scholarship.law.georgetown.edu/facpub/60» (Ultimo accesso: 10 maggio 2022).

443 J. E. COHEN, *DRM and Privacy*, cit., 577; in particolare essa afferma: "*Properly understood, an individual's interest in intellectual privacy has both spatial and informational aspects. At its core, this interest concerns the extent of "breathing space," both metaphorical and physical, available for intellectual activity. DRM technologies may threaten breathing space by collecting information about intellectual consumption (and therefore exploration) or by imposing direct constraints on these activities".*

identità delle persone[444], in questo modo andando a violare frontalmente il diritto all'autodeterminazione.

In aggiunta, una simile forma di monitoraggio capillare sarebbe altresì in grado di incidere sulla fondamentale dignità dell'essere umano, che riduce la complessità della individualità alla somma di profili generati dalle tecnologie digitali sulla base dei dati raccolti.

La seconda dimensione della privacy che viene toccata, a dire dell'autrice, dalle tecnologie di *Digital Rights Management* è quella che concerne gli "spazi privati". L'autrice, infatti, ricorda come le società occidentali tradizionalmente riservano certi tipi di luoghi all'individuo od alla famiglia ed alla riservatezza delle questioni che ivi si svolgono. Il primo e più importante di questi luoghi è proprio la casa che viene concepito come un luogo di ritiro dagli occhi del mondo esterno[445]. Non è un mistero, infatti, che il diritto alla riservatezza ed alla privacy in genere abbia molti punti di contatto con il diritto di proprietà e spesso vi si sovrapponga. Tuttavia, come nota l'autrice, è una corrispondenza solamente imperfetta, in quanto, afferma che "*Non ogni invasione di un interesse di proprietà è un'invasione della privacy; per esempio, la maggior parte delle persone non pensa che un fastidio, come un rumore eccessivo o fumi nocivi, sia anche un'invasione della privacy. E le persone possono avere aspettative sulla privacy in spazi che non possiedono o non affittano, come bagni pubblici, spogliatoi e cabine telefoniche. Il riconoscimento di queste aspettative suggerisce un consenso abbastanza ampio sul fatto che gli interessi tutelati dalla "privacy" e dalla "proprietà" sono diversi. Le regole e le tradizioni sulla libertà all'interno degli spazi privati riguardano non solo gli interessi di proprietà, ma anche le garanzie di un respiro (*breathing space*) fisico e letterale per il comportamento individuale*[446]"

Fra i comportamenti protetti dalla privacy spaziale rientrano anche quelli inerenti le attività della mente. La privacy spaziale infatti garantisce agli utenti la libertà di esplorare aree dei propri interessi intellettuali che un soggetto potrebbe non sentirsi parimenti libero di intraprendere in pubblico, garantendo quindi la libertà di un consumo intellettuale inosservato e non impedito da altri. Le tecnologie di DRM, entrando di forza in questi luoghi privati, non consentono la piena estrinsecazione di questo diritto.

In sostanza, dunque, le tecnologie di *Digital Rights Management*, grazie al loro potere para-normativo e all'intenso monitoraggio delle attività degli utenti che dei prodotti protetti si avvalgono, comprimono indebitamente altri diritti. *L'enforcement* del diritto d'autore quindi si scontra frontalmente con la privacy degli utenti.

Come visto, molte tecnologie di gestione dei diritti attuano limitazioni agli usi che di un certo contenuto gli utenti possono compiere. Tali tecnologie possono dunque assottigliare i limiti di libertà dei quali gli utenti hanno tradizionalmente potuto godere negli spazi privati

---

444 J. E. COHEN *DRM and Privacy*, cit., 577; in particolare essa afferma: *"Surveillance and compelled disclosure of information about intellectual consumption threaten rights of personal integrity and self-definition in subtle but powerful ways. Although a person cannot be prohibited from thinking as she chooses, persistent, fine-grained observation subtly shapes behavior, expression, and ultimately identity".*

445 J. E. COHEN, *DRM and Privacy*, cit., 578; in particolare essa afferma: "*The second strand of privacy theory that relates to intellectual privacy concerns privacy within physical spaces. Within Western societies, tradition and social practice reserve certain types of "private space" to the individual or the family. Chief among these is the home, which is conceived as a place of retreat from the eyes of the outside world".*

446 J. E. COHEN, *DRM and Privacy*, cit., 578; in particolare essa afferma: "*Not every invasion of a residential property interest is an invasion of privacy; for example, most people do not think that a nuisance, such as excessive noise or noxious fumes, is also a privacy invasion. And individuals can have privacy expectations in spaces that they do not own or rent, such as public restrooms, dressing rooms, and telephone booths. Acknowledgment of these expectations suggests a fairly broad consensus that the interests protected by "privacy" and "property" are different. Rules and traditions about freedom within private spaces concern not only property interests, but also guarantees of literal, physical breathing space for individual behavior."*

in relazione a tutte quelle attività di consumo intellettuale. Nell'imporre ciò al consumatore quindi, i titolari dei diritti d'autore, per il tramite di queste tecnologie, riducono il livello di autonomia nell'uso e nel godimento dei beni offerti[447].

Tali sistemi infatti permettono un controllo, automatico, sulle circostanze temporali e fisiche del consumo intellettuale, su quella dimensione privata di riservatezza e di non interferenza che gli individui si aspettano di avere. Il concetto di privacy, infatti, ha la capacità di sovrapporsi a quello di libertà, sebbene non si confonda con esso. "*L'interesse per la non interferenza con i comportamenti di consumo intellettuale all'interno degli spazi privati non è "semplicemente" una questione di libertà (negativa), ma anche e più fondamentalmente una questione di capacità di esercitare un controllo positivo su un'attività fondamentale per l'autodeterminazione*"[448].

È quindi proprio la connessione fra una simile attività ed il luogo protetto ove si svolge che genera un interesse alla privacy che si sostanzia nel diritto a porre in essere una attività libera da coercizioni dirette da parte di simili sistemi tecnologici. Solitamente tali tecnologie, come visto, operano mediante una sorveglianza capillare dell'uso che gli utenti compiono di tali contenuti, essendo strutturate per riportare al titolare di tali sistemi un insieme di dati sulle attività degli utenti. Solitamente tale monitoraggio avviene a fini di profilazione, cercando di tratteggiare profili degli utenti e dei loro consumi per generare forme di pubblicità più mirata.

Le tecnologie DRM che monitorano il comportamento degli utenti creano dei record del comportamento all'interno di spazi privati, spazi entro i quali ci si potrebbe ragionevolmente aspettare che il proprio comportamento non sia soggetto a osservazione. Queste tecnologie rientrano direttamente nella comprensione convenzionale dell'invasione della privacy. La raccolta di informazioni sul consumo intellettuale rende accessibili le preferenze intellettuali, sia al fornitore delle informazioni che a terzi, che potrebbero acquistarle o invocare procedimenti legali per costringerne la produzione. E nella misura in cui i comportamenti all'interno degli spazi privati diventano accessibili, o potenzialmente accessibili, al mondo esterno, l'individuo ha perso una parte della privacy che la cesura fra pubblico e privato dovrebbe garantire[449].

Anche il Gruppo di Lavoro Art. 29, organo che riunisce i Garanti europei, ha in più occasioni affrontato le preoccupazioni per il trattamento dei dati personali in relazione alle tecnologie di *Digital Rights Management*. In particolare, esso ha notato, in un suo parere del 18 gennaio 2005, che gli utenti spesso sono tenuti ad "*identificarsi prima di poter scaricare un brano da un provider ufficiale e il loro profilo verrà completato con le informazioni raccolte tramite l'identificatore univoco incluso in ogni brano musicale scaricato dall'utente*[450]". Oltre allo scopo dichiarato di

---

447 J. E. COHEN, *DRM and Privacy*, cit. 583.

448 J. E. COHEN, *DRM and Privacy*, cit. 583; in particolare essa afferma: "*The interest in noninterference with behaviors of intellectual consumption within private spaces is not "simply" a matter of (negative) liberty, but also and more fundamentally a matter of the ability to exert positive control over an activity fundamental to self-determination*".

449 J. E. COHEN *ibidem, 585, "DRM technologies that monitor user behavior create records of intellectual consumption. Indirectly, then, they create records of intellectual exploration, one of the most personal and private of activities. They also create records of behavior within private spaces, spaces within which one might reasonably expect that one's behavior is not subject to observation. These technologies fall straightforwardly within conventional understandings of privacy invasion. Gathering information about intellectual consumption renders intellectual preferences accessible, both to the information provider and to third parties that might purchase it or invoke legal process to compel its production. And to the extent that behaviors within private spaces become accessible, or potentially accessible, to the outside world, the individual has lost a portion of the privacy that seclusion ought to guarantee.*

450 Gruppo di Lavoro Articolo 29, (Article 29 – WP) 104 - *Data Protection Issues And Intellectual Property; Working document on data protection issues related to intellectual property rights*, 18 gennaio 2005, 3, liberamente accessibile presso: «https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1497279» (Ultimo accesso: 10 maggio 2022). Nel testo si legge: "*Users will for example, often have to identify themselves before being able to*

controllare l'uso delle informazioni da parte dell'individuo in conformità con il DRM, il Gruppo nota anche come ad esempio, "*il tagging viene spesso utilizzato per profilare e indirizzare annunci pubblicitari agli utenti. Come già affermato dall'International Working Group on Telecommunications, sono in fase di ideazione e offerta sistemi elettronici di gestione del copyright (ECMS) che potrebbero portare a una sorveglianza onnipresente degli utenti da parte di opere digitali. Alcuni ECMS stanno monitorando ogni singolo atto di lettura, ascolto e visualizzazione su Internet da parte dei singoli utenti, raccogliendo così informazioni altamente sensibili sull'interessato*".

Il Gruppo dei Garanti ricorda poi come lo scopo legittimo perseguito dai titolari dei diritti di prevenire l'uso improprio delle informazioni protette si traduce spesso nel tracciamento degli utenti e nel monitoraggio delle loro preferenze. In particolare, rileva come l'utilizzo di identificatori univoci consenta l'interconnessione dei dati relativi a un singolo individuo e ne faciliti la profilazione. Nell'ambito della gestione dei diritti digitali, consentono la profilazione dell'utente in base alla qualità e quantità dei documenti che consulta. Il Gruppo Art. 29 nota infatti come, ad esempio, "*un'azienda che offre contenuti legali online sarà in grado di tracciare la circolazione di tali documenti con watermark (che utilizzano identificatori univoci) su reti peer-to-peer e identificare l'utente all'origine del download legale nonché ulteriori presunti illeciti usi del documento. Anche sul posto di lavoro, l'industria musicale o cinematografica avrebbe la capacità di tracciare l'uso da parte dei propri dipendenti delle informazioni protette messe a loro disposizione. Il Gruppo di lavoro mette seriamente in discussione l'uso di identificatori allo scopo di tracciare "a priori" ogni utente, al fine di risalire a una persona specifica in caso di sospetto abuso del diritto d'autore. L'etichettatura di un documento non deve essere collegata a una persona fisica a meno che tale collegamento sia necessario per l'esecuzione del servizio o se la persona è stata informata e ha acconsentito ad essa".*

In questo si osserva dunque un divario crescente tra la protezione delle persone nel mondo off-line e on-line, soprattutto considerando il tracciamento e la profilazione generalizzata delle persone.

Molta di questa attività di monitoraggio, come nota Julie E. Cohen, è compiuta automaticamente dalla tecnologia stessa, senza il necessario coinvolgimento di un essere umano che ne controlli le risultanze. Ciò non neutralizza tuttavia la minaccia alla privacy, forse invece la fortifica. Non a caso oggi l'art. 22 del GDPR stabilisce proprio che "*l'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.*" Il che è altresì confermato dal considerando 71 del GDPR che dispone segnatamente che "*l'interessato dovrebbe avere il diritto di non essere sottoposto a una decisione, che possa includere una misura, che valuti aspetti personali che lo riguardano, che sia basata unicamente su un trattamento automatizzato […], quali il rifiuto automatico di una domanda di credito online o pratiche di assunzione elettronica senza interventi umani. Tale trattamento comprende la «profilazione», che consiste in una forma di trattamento automatizzato dei dati personali che valuta aspetti personali concernenti una persona fisica, in particolare al fine di analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato, ove ciò produca effetti giuridici che la riguardano o incida in modo analogo significativamente sulla sua persona".*

---

download a song from an official provider, and their profile will be completed with information collected through the unique identifier included in each piece of music downloaded by the user. In addition to the claimed purpose of control of the use of the information by the individual in compliance with DRM, the tagging is often used to profile and target advertisements to the users. As already stated by the International Working Group on Telecommunications, "Electronic Copyright Management Systems (ECMS) are being devised and offered which could lead to ubiquitous surveillance of users by digital works. Some ECMS are monitoring every single act of reading, listening and viewing on the Internet by individual users thereby collecting highly sensitive information about the data subject concerned".

Ove le informazioni così raccolte esistano in una forma accessibile e tale da rendere identificabile l'utente, essa può essere soggetta a "*disclosure*" e ad una produzione forzata. La mancanza di stringenti protezioni della privacy, dunque, può comportare una significativa diminuzione della libertà nel consumo intellettuale e quindi compromettere gli interessi alla privacy intellettuale.

Infine, è chiaro, come visto, che le tecnologie di *Digital Rights Management* possano essere sfruttate come forme di autotutela privata *nell'enforcement* del diritto d'autore. L'estesa sorveglianza realizzata da tali tecnologie potrebbe risultare nel rinvenimento di attività illecite compiute dagli utenti. In tali occasioni le tecnologie potrebbero operare automaticamente per disabilitare, ad esempio, l'accesso al contenuto stesso. La dimensione della privacy che si percepisce in questo caso è connessa alla perdita dell'anonimato dell'utente. Infatti, la identificazione di un particolare utente come bersaglio di misure di autotutela tecnologica rende quell'utente non già uno fra i tanti consumatori, ma un "pirata". Si ripercuotono in questo anche le considerazioni già precedentemente trattate circa l'automatismo di questo sistema sanzionatorio, spesso attuato in assenza di un controllo umano sulla correttezza delle decisioni algoritmiche, in contrasto, nuovamente, con quanto dispone oggi l'art. 22 GDPR.

Inserendo funzioni di *enforcement* automatico dei diritti d'autore negli spazi e nelle attività private, "*queste tecnologie annullano la differenza tra comportamento pubblico/governato da regole e comportamento privato che è molto più vagamente circoscritto dalle regole e dalle norme sociali applicabili*[451]*."*

In tutti gli ordinamenti occidentali è poi da notare che esiste un forte divieto di farsi giustizia da sé, tanto che lo stesso codice penale italiano, ad esempio, sanziona penalmente la "ragion fattasi" disponendo che "*chiunque, al fine di esercitare un preteso diritto, potendo ricorrere al giudice, si fa arbitrariamente ragione da sé medesimo […] è punito a querela della persona offesa*". Il potere di *Digital Rights Management*, tuttavia, consente al titolare dei contenuti protetti dal diritto d'autore di ricorrere unilateralmente *all'enforcement* dei propri diritti. Questo avviene principalmente mediante la negazione dell'accesso, la distruzione di informazioni o la disattivazione di talune funzionalità in modo essenzialmente non violento che tuttavia non ne diminuisce la invasività e la distruttività[452]. A ciò si deve aggiungere altresì la constatazione che le forme digitali di autotutela sono scarsamente trasparenti e visibili tanto che per l'utente potrebbe essere quasi impossibile conoscere l'esistenza di una misura di autotutela. In questo, la dislocazione del potere coercitivo in capo ai privati rende concreto il rischio di un c.d "*autoritarismo decentrato*"[453].

Per combattere le forme più forti di compressione dei diritti degli utenti deve ergersi a baluardo il potere normativo dello Stato[454]. Solo lo Stato, infatti, quale naturale antagonista delle forme di autotutela tecnologica, può dimostrare un potere sufficientemente vasto da contenere le derive più significative in campo di *Digital Rights Management* e contrapporre al potere privato, para-normativo e contrattuale dei privati un potere pubblico di tutela degli utenti, garantendo agli stessi mezzi di ricorso effettivi contro la violazione dei loro diritti. Si

---

451 J. E. COHEN, *DRM and Privacy*, cit. 587, si esprime affermando: "*By inserting automatic enforcement functions into private spaces and activities, these technologies elide the difference between public/rule-governed behavior and private behavior that is far more loosely circumscribed by applicable rules and social norms".*

452 R. CASO, *Digital rights management: il commercio delle informazioni digitali tra contratto e diritto d'autore,* cit., 110 e ss.

453 R. CASO, *Digital rights management: il commercio delle informazioni digitali tra contratto e diritto d'autore,* cit., 11-12, 107, 114; si veda in merito il riferimento a R. STALLMAN, *The Right to Read*, 1997, disponibile sul sito Web: «http://www.gnu.org/philosophy/right-to-read.html» (Ultimo accesso: 10 maggio 2022).

454 Di avviso similare pare essere R. CASO, *Digital rights management: il commercio delle informazioni digitali tra contratto e diritto d'autore*, cit. 180 e ss.

chiede al legislatore, quindi, di ristabilire l'equilibrio fra *enforcement* dei diritti d'autore e la tutela della privacy, equilibrio turbato dalla tecnologia.

5.3. Possibili risoluzioni statunitensi

Nel contesto statunitense, nonostante la feroce difesa della proprietà intellettuale che connatura la dimensione normativa e giurisprudenziale, esistono già nel *Common Law* strumenti efficaci per evitare di incorrere in derive tecnologiche che dimentichino la privacy degli utenti.

Gli strumenti di cui l'ordinamento di Common Law dispone sono stati definiti da Prosser[455] e poi confluiti nel *Restatement of Torts* e sono: (a) *Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs; (b) Public disclosure of embarrassing private facts about the plaintiff; (c) Publicity which places the plaintiff in a false light in the public eye; (d) Appropriation, for the defendant's advantage, of the plaintiff's name or likeness.*

Per il primo fra i *tort*, (sub a) esso si sostanzia in una figura che non necessita che le informazioni siano rese pubbliche, basta una introduzione nella vita privata altrui carpendo informazioni private. L'intrusione nella vita privata altrui può anche non essere fisica, ma solamente visiva o uditiva. In ogni caso deve essere altamente offensiva per una "persona ragionevole". È il solo dei quattro *tort* che non necessita che le informazioni siano rese "pubbliche"; pertanto l'illecito si realizza già nel momento in cui le informazioni sono raccolte. Il secondo (sub b) riguarda ipotesi in cui un individuo rende pubbliche informazioni vere di un altro individuo senza il consenso dello stesso. È composto di quattro elementi: (1) disseminazione di informazioni veritiere (2) offensive per una persona ragionevole, (3) che non siano di interesse pubblico e (4) siano così intime da confliggere con il senso comune di decoro. Il terzo (sub c) mira ad evitare che un soggetto possa avere un ritorno economico derivante dall'utilizzo della immagine o del nome della persona senza il suo consenso, così prevenendo l'ingiusto arricchimento. Si caratterizza chiaramente per lo scopo "commerciale" che il soggetto mira a conseguire con l'utilizzo dell'immagine altrui. L'ultimo dei tort (sub d) è rivolto alla situazione in cui si vada a mettere una persona in cattiva luce pubblicando informazioni che sono false sull'individuo o, per il modo in cui sono esposte, che creano una falsa rappresentazione del soggetto. Deve trattarsi di una condotta altamente offensiva per una "persona ragionevole" e perché vi sia responsabilità, chi pubblica la notizia deve farlo nella consapevolezza della falsità.

Tali strategie sono state efficacemente riprese da Julie E. Cohen,[456] affermando che fra tali *tort*, quelli che possono avere rilievo nel contesto digitale sono: "*intrusion upon seclusion", "appropriation of name or likeness"* e infine *"public disclosure of private facts*".

L'autrice in particolare ritiene che nel prosseriano *tort* "*intrusion upon seclusion*" si possano rinvenire efficaci tutele avverso una indebita ingerenza nella privacy degli utenti.

Nel caso Lake v. Wal-Mart Stores la Corte afferma che "*The right to privacy is an integral part of our humanity; one has a public persona, exposed and active, and a private persona, guarded and*

[455] W.L. PROSSER., *Privacy,* in *California Law Review* 383, 1960 liberamente accessibile presso: «https://lawcat.berkeley.edu/record/1109651» (Ultimo accesso: 10 maggio 2022).
[456] J. E. COHEN, *DRM and Privacy*, cit. 589 e ss.

preserved. The heart of our liberty is choosing which parts of our lives shall become public and which parts we shall hold close" [457].

L'applicabilità di tali strumenti viene confermata anche dalle Corti statunitensi in merito ai ragionamenti circa il quarto emendamento. In linea evolutiva, infatti, le ingerenze nella privacy dei cittadini, vietate dal quarto emendamento nelle attività dello Stato, devono essere riaffermate, *a fortiori*, quando si tratti di liti fra privati. Si può ritenere quindi che congiungendo gli strumenti dei *privacy torts* con i ragionamenti delle Corti statunitensi circa il quarto emendamento ed il suo ambito di protezione, si possa giungere ad affermare una estesa tutela della privacy in campo digitale per il tramite del common law.

Le Corti federali in particolare hanno affermato che il quarto emendamento può proteggere anche le informazioni personali ottenute mediante mezzi tecnologici. Il riferimento è infatti alla sentenza Kyllo vs. US[458]. Sulla base dell'analisi termografica, si voleva verificare che la quantità di calore emessa dalla casa di Kyllo fosse coerente con le lampade ad alta intensità tipicamente utilizzate per la coltivazione di marijuana, fatto di cui era sospettato. Grazie a tali immagini, un magistrato federale emise un mandato per perquisire la casa di Kyllo. Kyllo lamentò che lo strumento utilizzato rientrava nel "search and seizure" del quarto emendamento. La Corte Suprema ritenne che vi fosse una "*reasonable expectation of privacy*" e pertanto il mandato sarebbe stato necessario fin da principio, ovvero anche per utilizzare il termografo.

La Corte Suprema in questo caso parte, infatti, dalla constatazione per cui "*sarebbe sciocco sostenere che il grado di privacy assicurato ai cittadini dal quarto emendamento è stato del tutto inalterato dal progresso della tecnologia*"[459].

La linea di demarcazione che esclude ciò che è pubblico da ciò che è privato secondo la Corte deve essere "*bright*"[460], evidente, il che richiede una chiara specificazione di quei metodi di sorveglianza che richiedono un mandato. Dal caso Kyllo non rimaneva chiaro se tale protezione avverso nuove forme intrusive a livello tecnologico si estendesse solo alla dimensione della casa. Tali dubbi furono tuttavia fugati dalla successiva giurisprudenza.

Con il caso US v. Jones 2012[461], la giurisprudenza modifica il proprio intendimento come risultante dal caso Kyllo proprio riferendosi alla capacità intrusiva della moderna tecnologia. In questa fattispecie concreta, la polizia, agendo oltre i limiti del mandato ottenuto, installò un GPS sulla macchina della moglie di un soggetto sospettato di narcotraffico. Jones, successivamente imputato per narcotraffico anche grazie ai dati ottenuti dal GPS, contestò la raccolta dei dati alla luce del quarto emendamento. La Corte, in questo

---

[457] Lake v. Wal-Mart Stores 528 N.W.2d 231 – Minn. 1998, liberamente accessibile presso: «https://casetext.com/case/lake-v-wal-mart-stores-inc-1» (Ultimo accesso: 10 maggio 2022), traducendo liberamente il testo riportato: "*Il diritto alla privacy è parte integrante della nostra umanità; un soggetto ha una persona pubblica, esposta e attiva, e una persona privata, custodita e preservata. Il cuore della nostra libertà è scegliere quali parti della nostra vita diventeranno pubbliche e quali terremo strette*".

[458] Kyllo v. United States, 533 U.S. 27 (2001), liberamente accessibile presso: «https://supreme.justia.com/cases/federal/us/533/27/» (Ultimo accesso: 10 maggio 2022).

[459] Nelle parole della Corte: "*It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology*".

[460] Nelle parole della Corte: "*We have said that the Fourth Amendment draws "a firm line at the entrance to the house," Payton, 445 U.S., at 590. That line, we think, must be not only firm but also bright–which requires clear specification of those methods of surveillance that require a warrant. While it is certainly possible to conclude from the videotape of the thermal imaging that occurred in this case that no "significant" compromise of the homeowner's privacy has occurred, we must take the long view, from the original meaning of the Fourth Amendment forward*".

[461] U.S. v. Jones, 132 S. Ct. 945 (2012), liberamente accessibile presso: «https://www.law.cornell.edu/supremecourt/text/10-1259» (Ultimo accesso: 10 maggio 2022).

caso, decise che tale utilizzo della tecnologia del GPS costituisse una "*search*" ai sensi del quarto emendamento.

Maggiormente significativo è poi il successivo caso Riley v. California[462]. Nel contesto della common law, infatti, per affermare una proteggibilità della privacy è necessario indagare che l'intrusione sia "offensiva per una persona ragionevole". Julie E. Cohen nota che sia il quarto emendamento che il *Common Law* estendono la protezione contro la perquisizione e il sequestro senza mandato non solo all'abitazione, ma anche ai "documenti ed effetti" degli individui.

In questo caso, l'imputato Riley era stato fermato per una violazione del codice stradale, che tuttavia portò, da una ispezione dell'autovettura al suo arresto con l'accusa di detenzione illecita di armi. Venne ispezionato il telefonino di Riley che era stato trovato nei suoi pantaloni e dall'analisi del traffico telefonico si evinse il collegamento di Riley con una "*street gang*" e con una sparatoria avvenuta poco tempo prima. Si procedette dunque per i reati collegati alla partecipazione di Riley nella *gang*, fra cui un tentato omicidio. Riley chiese che le prove raccolte fossero soppresse perché ottenute in violazione del quarto emendamento, in quanto senza mandato o senza altre giustificazioni[463].

I telefoni cellulari differiscono sia in senso quantitativo che qualitativo da altri oggetti che potrebbero essere trasportati sulla persona di un arrestato. In particolare, i telefoni cellulari moderni hanno un'immensa capacità di archiviazione. Prima dei cellulari, la ricerca di una persona era limitata dalle realtà fisiche e generalmente costituiva solo una stretta intrusione nella privacy. Ma i telefoni cellulari possono memorizzare milioni di pagine di testo, migliaia di immagini o centinaia di video. Ciò ha diverse conseguenze sulla privacy. In primo luogo, un telefono cellulare raccoglie in un unico luogo molti tipi distinti di informazioni che rivelano molto di più in combinazione rispetto a qualsiasi record isolato. In secondo luogo, la capacità del telefono consente anche a un solo tipo di informazioni di trasmettere molto più di quanto fosse possibile in precedenza. Terzo, i dati sul telefono possono risalire ad anni fa. Inoltre, un elemento di pervasività caratterizza i telefoni cellulari ma non le registrazioni fisiche[464].

Pare dunque possibile affermare che, quantomeno evolutivamente, il diritto alla privacy si estenda non solo alla casa ed ai luoghi affini, ma anche ai "luoghi digitali" quali i computer o i telefoni cellulari che contengono la dimensione principale degli interessi alla privacy intellettuale, indipendentemente dal luogo fisico in cui materialmente siano contenuti.

---

462 Riley v. California, 136 S. Ct. 506 (2015), liberamente accessibile presso: «https://www.law.cornell.edu/supremecourt/text/13-132» (Ultimo accesso: 10 maggio 2022).

463 Nel testo della sentenza il caso è così riportato: "*petitioner Riley was stopped for a traffic violation, which eventually led to his arrest on weapons charges. An officer searching Riley incident to the arrest seized a cell phone from Riley's pants pocket. The officer accessed information on the phone and noticed the repeated use of a term associated with a street gang. At the police station two hours later, a detective specializing in gangs further examined the phone's digital contents. Based in part on photographs and videos that the detective found, the State charged Riley in connection with a shooting that had occurred a few weeks earlier and sought an enhanced sentence based on Riley's gang membership. Riley moved to suppress all evidence that the police had obtained from his cell phone. The trial court denied the motion, and Riley was convicted. The California Court of Appeal affirmed*".

464 Nelle parole della Corte: "*Cell phones differ in both a quantitative and a qualitative sense from other objects that might be carried on an arrestee's person. Notably, modern cell phones have an immense storage capacity. Before cell phones, a search of a person was limited by physical realities and generally constituted only a narrow intrusion on privacy. But cell phones can store millions of pages of text, thousands of pictures, or hundreds of videos. This has several interrelated privacy consequences. First, a cell phone collects in one place many distinct types of information that reveal much more in combination than any isolated record. Second, the phone's capacity allows even just one type of information to convey far more than previously possible. Third, data on the phone can date back for years. In addition, an element of pervasiveness characterizes cell phones but not physical records. A decade ago officers might have occasionally stumbled across a highly personal item such as a diary, but today many of the more than 90% of American adults who own cell phones keep on their person a digital record of nearly every aspect of their lives*".

La Corte, nel fare riferimento al tipo di tecnologia utilizzata, richiede quindi che vi siano persino garanzie aggiuntive per non incorrere in una indebita invasione della privacy.

Nel campo del *Digital Rights Management* quindi Julie E. Cohen afferma che l'attività profondamente personale e privata del consumo intellettuale porta a ritenere che sia ragionevole e necessaria una adeguata tutela della privacy intellettuale.

L'applicazione dei *tort* poi di "*appropriation of name or likeness*" e " *public disclosure of private facts*" alle tecnologie di monitoraggio DRM trova parallelismi nella giurisprudenza statunitense che si basa sul primo emendamento e che tocca la privacy intellettuale. I casi che coinvolgono la divulgazione forzata delle abitudini di lettura e visione rinvengono che l'attività intellettuale in discussione è essenzialmente privata a causa del c.d "*chilling effect*" che potrebbe avere sull'attività espressiva e politica privata che potrebbe derivare dalla divulgazione forzata di opinioni e pensieri[465].

Con un ragionamento simile, sia i fatti privati che gli illeciti di appropriazione dovrebbero comprendere la vendita, l'affitto o lo scambio di informazioni sui modelli di consumo intellettuale. "*Probabilmente, i danni risultanti dalla divulgazione di fatti privati relativi ad attività e preferenze intellettuali sono almeno altrettanto gravi di quelli risultanti dalla divulgazione di informazioni sulle attività e preferenze sessuali, poiché è la prima, piuttosto che la seconda, su cui una società democratica fa affidamento per costituire i suoi cittadini*"[466].

Un ulteriore supporto per l'espansione dell'illecito di appropriazione in modo da comprendere l'identità digitale viene, paradossalmente, dal *doppelganger* commerciale della privacy, il diritto alla pubblicità (*right to publicity*) di common law. Come l'illecito-privacy dell'appropriazione non autorizzata, i diritti di pubblicità proteggono dall'appropriazione non autorizzata di nomi e sembianze. I diritti di pubblicità in genere vengono invocati per proteggere somiglianze di valore commerciale, ma entrambe le teorie cercano di riservare il controllo sullo sfruttamento commerciale dell'identità all'individuo a cui tale identità è associata. A differenza dei tribunali che si occupano di casi di privacy, i tribunali nei casi di pubblicità hanno generosamente interpretato il concetto di "somiglianza", estendendo la protezione a qualsiasi attributo della personalità che può essere ragionevolmente identificato come appartenente all'attore.

In definitiva quindi appare che l'ordinamento statunitense possa disporre di sufficienti strumenti per orientare le decisioni giudiziarie a favore degli utenti. Le Corti, quindi, dovrebbero orientarsi verso un'interpretazioni dei *tort* che, in linea con la giurisprudenza statunitense in merito al quarto emendamento ed alla sempre più attenta protezione di luoghi non solo fisici ma anche digitali, sia in grado di arginare le più gravi violazioni dei diritti degli utenti a scopo di *enforcement* del diritto d'autore tramite i sistemi di *Digital Rights Management.*

5.4. Possibili risoluzioni euro-italiane

---

[465] J. E. COHEN, *DRM and Privacy,* ricorda, fra i molti casi, i seguenti: Denver Area Educ. Telecomm. Consortium, Inc. v. FCC, 518 U.S. 727, 751- 66 (1996); Stanley v. Georgia, 394 U.S. 557, 563-66 (1969); Schneider v. Smith, 390 U.S. 17,24-25 (1968); Lamont v. Postmaster Gen., 381 U.S. 301, 307 (1965); Fabulous Assoc., Inc. v. Pa. Pub. UtiI. Comm'n, 896 F.2d 780, 785 (3d Cir. 1990); see also Gibson v. Fla. Legislative Investigation Comm., 372 U.S. 539, 544 (1963).

[466] J. E. COHEN, *DRM and Privacy,* cit., 589 e ss. L'autrice infatti afferma: "*Arguably, the harms resulting from disclosure of private facts relating to intellectual activities and preferences are at least as great as those resulting from disclosure of information about sexual activities and preferences, since it is the former rather than the latter upon which a democratic society relies to constitute its citizens*"

L'ordinamento italiano ed europeo può contare su un forte strumento per rimediare ai casi più eclatanti di violazione dei diritti alla privacy degli utenti, perpetrati dai titolari dei diritti d'autore per mezzo di strategie di *enforcement* che facciano leva sui sistemi di *Digital Rights Management*. Il riferimento è al *corpus* normativo conosciuto come GDPR, ossia il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE.

Si deve infatti affermare che il monitoraggio e le conseguenti decisioni prese in via di autotutela da parte dei titolari dei diritti d'autore costituiscono un trattamento dei dati personali. Come tale, deve rispettare le previsioni normative che disciplinano la privacy a livello comunitario ed italiano.

I cittadini europei, quindi, possono essere sicuri del fatto che, almeno sulla carta, qualsiasi attività di monitoraggio attuata nel territorio dell'Unione da qualunque soggetto rientrerà nell'ambito di applicazione territoriale, ex art. 3 GDPR, del Regolamento, con conseguente applicazione della disciplina ivi prevista. Infatti, ai sensi dell'art. 3 GDPR, tale Regolamento non solo si applica verso quei titolari del trattamento che hanno una sede od uno stabilimento in Unione Europea, ma anche a coloro che tale stabilimento non possiedono ove le attività attuate da tale titolare riguardino la prestazione di beni o servizi nel territorio dell'Unione o comunque il monitoraggio del comportamento degli utenti che ha luogo nel territorio dell'Unione. Tale constatazione è confermata dal Considerando 24 il quale dispone in merito che "*è opportuno che anche il trattamento dei dati personali degli interessati che si trovano nell'Unione ad opera di un titolare del trattamento […] non stabilito nell'Unione sia soggetto al presente regolamento quando è riferito al monitoraggio del comportamento di detti interessati, nella misura in cui tale comportamento ha luogo all'interno dell'Unione. Per stabilire se un'attività di trattamento sia assimilabile al controllo del comportamento dell'interessato, è opportuno verificare se le persone fisiche sono tracciate su Internet, compreso l'eventuale ricorso successivo a tecniche di trattamento dei dati personali che consistono nella profilazione della persona fisica, in particolare per adottare decisioni che la riguardano o analizzarne o prevederne le preferenze, i comportamenti e le posizioni personali*".

Sicuri dunque di tale applicabilità, già il Considerando 4 chiede di ragionare in termini di bilanciamento, un bilanciamento che la tecnologia vuole dimenticare ma che con forza viene riaffermato dal legislatore europeo. Il Regolamento in questo è chiaro: "*il trattamento dei dati personali dovrebbe essere al servizio dell'uomo*". Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità. E tale considerazione vale a maggior ragione nell'ambito del diritto alla proprietà intellettuale che, sebbene vada protetto e riaffermato anche nella dimensione digitale, non va esasperato, con alcune tecniche di *enforcement* che, per il presente elaborato, devono essere sconfessate alla luce della normativa vigente.

Il Regolamento non è cieco dinnanzi al cambiamento tecnologico ed alle potenzialità della tecnologia, ma chiede che venga rinvenuto un equilibrio fra i vari interessi che su Internet si scontrano. Il Considerando 6 riconosce che "*la rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali. La portata della condivisione e della raccolta di dati personali è aumentata in modo significativo. La tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività*". Il legislatore europeo, infatti, non dimentica che la tecnologia ha trasformato l'economia e le relazioni sociali e ciò *"dovrebbe facilitare ancora di più la libera*

circolazione dei dati personali […], garantendo al tempo stesso un elevato livello di protezione dei dati personali".

Per queste ragioni, ad avviso di chi scrive, le soluzioni euro-italiane da rinvenire per arginare le derive orwelliane dell'impiego dei sistemi di *Digital Rights Management* devono essere trovate proprio nelle disposizioni del GDPR, ultimo vallo che permette di proteggere gli utenti.

Innanzitutto, il trattamento dei dati personali compiuto dai titolari dei diritti d'autore nell'applicare le misure tecnologiche di monitoraggio e di autotutela è lecito solo ove si rinvenga una base legale capace di comprenderlo. Stante il disposto dell'art. 6 GDPR[467], le possibili cause giustificative del trattamento possono essere alternativamente rinvenute alla lettera a) od alla lettera f). Di queste, la prima richiede che l'interessato al trattamento dei dati abbia espresso il proprio consenso, la seconda invece legittima la raccolta dei dati alla luce del perseguimento del legittimo interesse del titolare del trattamento o dei terzi, correttamente bilanciato con gli interessi e i diritti degli utenti.

Perché si possa ritenere integrata la condizione del consenso non sono sufficienti quelle disposizioni contrattuali che presumono il consenso alla apertura di un imballaggio o ad un semplice click "accetta tutto". Infatti, l'art. 7 GDPR richiede che la richiesta di consenso sia presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Il Considerando 32 specifica poi che il consenso dovrebbe essere espresso mediante "*un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano*". Non dovrebbe pertanto configurare consenso il silenzio, l'inattività o la preselezione di caselle.

In merito si può richiamare una recente sentenza della Corte di Giustizia nella quale il giudice del rinvio si chiedeva, in sostanza, se l'articolo 6, paragrafo 1, lettera a), del Regolamento 2016/679, dovesse essere interpretato nel senso che il consenso possa essere validamente espresso quando l'archiviazione di informazioni o l'accesso a informazioni già archiviate, mediante cookie, nell'apparecchiatura terminale di un utente, dovessero essere autorizzati mediante una casella preselezionata che l'utente avrebbe dovuto dunque deselezionare al fine di negare il proprio consenso. Secondo la Corte, in virtù della rinnovata disciplina del GDPR, "*il consenso non è validamente espresso quando l'archiviazione di informazioni o l'accesso a informazioni già archiviate nell'apparecchiatura terminale dell'utente di un sito Internet attraverso cookie sono autorizzati mediante una casella di spunta preselezionata che l'utente deve deselezionare al fine di negare il proprio consenso. […] A tal riguardo, risulta praticamente impossibile determinare in modo oggettivo se l'utente […] abbia effettivamente manifestato il proprio consenso al trattamento dei suoi dati*

[467] In particolare, l'art. 6 paragrafo primo afferma: "*Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:*
a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precon- trattuali adottate su richiesta dello stesso;
c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;
d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.
La lettera f) del primo comma non si applica al trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti".

personali, nonché, in ogni caso, se tale consenso sia stato manifestato in modo informato. Non può, infatti, essere escluso che detto utente non abbia letto l'informazione che accompagna la casella preselezionata, o addirittura che lo stesso non abbia visto tale casella, prima di continuare la propria attività[468]".

Emanuele Lucchini Guastalla pone in luce un ulteriore profilo problematico nel momento in cui osserva che può avvenire che l'utente sia "*posto di fronte a un aut aut: o presta il consenso, o non potrà fruire del servizio; […] Questa situazione non è infrequente: basti pensare a quante volte l'accesso a un servizio online è subordinato alla prestazione del consenso non soltanto al trattamento dei dati da parte del gestore, ma anche alla trasmissione dei dati a operatori terzi ai fini, ad es., dell'invio all'utente di comunicazioni commerciali. […] Il legislatore europeo ha dunque previsto che, ove il consenso sia stato prestato in tali condizioni, sia ragionevolmente plausibile che esso non sia stato prestato liberamente. Non si tratta di una presunzione, ma - per così dire - di un invito di fonte legislativa a prestare attenzione, tra le altre circostanze del consenso, a questa peculiare forma di condizionamento, potenziale indice di una menomata libertà decisionale dell'utente*"[469].

L'impostazione fatta propria dal Regolamento è analoga a quella adottata nel 2013 dal nostro Garante per la protezione dei dati personali, secondo cui "*il consenso […] deve intendersi libero quando non è preimpostato e non risulta - anche solo implicitamente in via di fatto - obbligatorio per poter fruire del prodotto o servizio fornito dal titolare del trattamento*"[470]. Peraltro, già nel 2010, il Garante si era spinto ben oltre l'impostazione del recente Regolamento, affermando che "*non può definirsi "libero", e risulta indebitamente necessitato, il consenso a ulteriori trattamenti di dati personali che l'interessato "debba" prestare quale condizione per conseguire una prestazione richiesta*"[471] .

Il Considerando 42 in merito aggiunge che ai fini di un consenso informato, l'interessato dovrebbe essere posto a conoscenza almeno dell'identità del titolare del trattamento e delle finalità del trattamento cui sono destinati i dati personali. Il consenso non dovrebbe essere considerato liberamente espresso se l'interessato non è in grado di operare una scelta autenticamente libera o è nell'impossibilità di rifiutare o revocare il consenso senza subire pregiudizio.

Il Considerando 43 poi afferma che è opportuno che il consenso non costituisca un valido presupposto per il trattamento dei dati personali qualora esista un evidente squilibrio tra l'interessato e il titolare del trattamento. Squilibrio che potrebbe essere tranquillamente identificato nel caso di disparità contrattuale che non può essere ritenuta non sussistente nell'ipotesi di DRM[472].

---

[468] CGUE 1° ottobre 2019, C-673/17, *Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband eV contro P. GmbH*, liberamente accessibile presso: «https://curia.europa.eu/juris/document/document.jsf?docid=218462&doclang=IT» (Ultimo accesso: 10 maggio 2022).

[469] E. LUCCHINI GUASTALLA, *Il Nuovo Regolamento Europeo Sul Trattamento Dei Dati Personali: I Principi Ispiratori* in *Contratto e Impr.*, 2018, 1, 106.

[470] Provv. 4 luglio 2013 del Garante, intitolato *Linee guida in materia di attività promozionale e contrasto allo spam* (consultabile sul sito Internet garanteprivacy.it, doc. web n. 2542348, presso: «https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/2542348» (Ultimo accesso: 10 maggio 2022)).

[471] Provv. 15 luglio 2010 del Garante, intitolato *Raccolta di dati via Internet per finalità promozionali: sempre necessario il consenso degli interessati*, cit.

[472] Per maggiori riferimenti alla disparità contrattuale che permea i contratti di licenza in cui vengono imposti sistemi di *Digital Rights Management* si vedano: R. CASO (a cura di), *Digital Rights Management: problemi teorici e prospettive applicative.* Atti del Convegno tenuto presso la Facoltà di Giurisprudenza di Trento il 21 ed il 22 marzo 2007, Università di Trento, Trento, 2008, disponibile sul sito: «http://eprints.biblio.unitn.it/1336/» (Ultimo accesso: 10 maggio 2022); R. CASO, *Digital rights management: il commercio delle informazioni digitali tra contratto e diritto d'autore*, cit.

Nel valutare la base legale espressa dalla lettera f) si deve richiedere un attento bilanciamento fra gli interessi in gioco, interesse che, come più volte affermato in questo elaborato, è di difficile realizzazione. Infatti, il Considerando 47 afferma che i legittimi interessi di un titolare del trattamento possono costituire una base giuridica del trattamento, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato, tenuto conto delle ragionevoli aspettative nutrite dall'interessato in base alla sua relazione con il titolare del trattamento. "*In ogni caso, l'esistenza di legittimi interessi richiede un'attenta valutazione anche in merito all'eventualità che l'interessato, al momento e nell'ambito della raccolta dei dati personali, possa ragionevolmente attendersi che abbia luogo un trattamento a tal fine. Gli interessi e i diritti fondamentali dell'interessato potrebbero in particolare prevalere sugli interessi del titolare del trattamento qualora i dati personali siano trattati in circostanze in cui gli interessati non possano ragionevolmente attendersi un ulteriore trattamento dei dati personali.*" Il legislatore europeo non nasconde comunque che può essere considerato legittimo interesse trattare dati personali per finalità di marketing diretto, tuttavia, anche tale interesse deve essere bilanciato con i diritti degli interessati.

In ogni caso, ove anche sussistesse una base legale per il trattamento dei dati personali, bisognerebbe poi fare i conti con l'articolo 9, a mente del quale, generalmente, è vietato trattare dati personali che rivelino "*l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona*". Per evitare un trattamento illecito, l'art. 9 chiede un consenso esplicito[473], non avendo alcuna rilevanza, in questo caso, il legittimo interesse del titolare.

---

[473] In particolare, l'art. 9 consente al paragrafo secondo il trattamento dei dati c.d. "sensibili" solo se si verifica uno dei seguenti casi:

"a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1;

b) il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato;

c) il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;

d) il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato;

e) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;

f) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;

g) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato;

h) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al paragrafo 3;

i) il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale;

j) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta

Ove, quindi, un sistema di *Digital Rights Management* riuscisse ad essere ritenuto un trattamento dei dati personali sostenuto dalla liceità di tale operazione, si dovrebbero comunque investigare le modalità e le finalità con cui tale sistema viene attuato, confrontandolo con le disposizioni normative per verificarne la correttezza.

In particolare, la materia che sovviene principalmente alla mente nell'elaborazione informatica dei dati personali dei consumatori di prodotti intellettuali da parte degli utenti, tramite il monitoraggio delle loro abitudini, è sicuramente quella concernente la profilazione degli utenti[474].

L'art. 22 del GDPR in merito dispone che l'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona. Per "profilazione" l'art. 4 intende "*qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica*". Pare dunque che la definizione sia perfettamente applicabile alla attività che abbiamo visto connaturare i sistemi di *Digital Rights Management*[475].

Il Gruppo Articolo 29, riunente le Autorità di Controllo degli Stati membri UE, ha prodotto delle linee guida dedicate alla profilazione ai fini del Regolamento 2016/679[476]. Secondo tale documento, la profilazione è costituita da tre elementi: deve essere una forma di trattamento automatizzato; deve essere effettuata su dati personali; il suo obiettivo deve essere quello di valutare aspetti personali relativi a una persona fisica.

Il Considerando 70 esplicita in merito che qualora i dati personali siano trattati per finalità di marketing diretto, l'interessato dovrebbe avere il diritto, in qualsiasi momento e gratuitamente, di opporsi a tale trattamento, compresa la profilazione nella misura in cui sia connessa a tale marketing diretto. Tale diritto dovrebbe essere esplicitamente portato all'attenzione dell'interessato e presentato chiaramente e separatamente da qualsiasi altra informazione. Il Considerando 71 poi afferma che l'interessato dovrebbe avere il diritto di non essere sottoposto a una decisione, che possa includere una misura che valuti aspetti personali che lo riguardano, che sia basata unicamente su un trattamento automatizzato e che produca effetti giuridici che lo riguardano. Tuttavia, è opportuno che sia consentito adottare decisioni sulla base di tale trattamento, compresa la profilazione, se ciò è

---

l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato".

[474] Per maggiori informazioni sulle decisioni algoritmiche ed il rapporto che queste istaurano con la normativa a tutela dei dati personali si veda G. ALPA, G. RESTA, *Le Persone e la Famiglia 1, Le persone fisiche e i diritti della personalità*, cit., 515-520.

[475] Per maggiori informazioni sull'impatto della profilazione sui sistemi di Automatic Content Recognition e sull'art.17 della nuova Direttiva 2019/790 si veda C. SCHMON, *Filtri automatici e privacy: la tempesta perfetta*, in *Electonic Frontier Foundation*, 3 marzo 2020, nella Traduzione di R. DUCATO con la collaborazione di P. GUARDA, 21 marzo 2020, liberamente accessibile presso: «https://www.eff.org/it/deeplinks/2020/02/upload-filters-are-odds-gdpr» (Ultimo accesso: 10 maggio 2022).

[476] Gruppo Di Lavoro Articolo 29 Per La Protezione Dei Dati; *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del Regolamento 2016/790*; 17/IT WP 251 rev.01, adottate il 3 ottobre 2017; versione emendata e adottata in data 6 febbraio 2018, accessibili presso: «https://ec.europa.eu/newsroom/article29/items/612053» (Ultimo accesso: 10 maggio 2022).

espressamente previsto dal diritto dell'Unione o degli Stati membri cui è soggetto il titolare del trattamento, o se è necessario per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento, o se l'interessato ha espresso il proprio consenso esplicito. In ogni caso, tale trattamento dovrebbe essere subordinato a garanzie adeguate, che dovrebbero comprendere la specifica informazione all'interessato e il diritto di ottenere l'intervento umano, di esprimere la propria opinione, di ottenere una spiegazione della decisione conseguita dopo tale valutazione e di contestare la decisione.

Proprio alla luce del Considerando 71, infatti, l'art. 22 paragrafo 2 dispone che un tale trattamento possa essere ritenuto lecito, tuttavia, a condizione che ciò sia a) necessario per la conclusione o l'esecuzione di un contratto, oppure c) si basi sul consenso esplicito dell'interessato. Da ciò comunque sempre esclusi, ai sensi del terzo paragrafo, i dati sensibili.

In ogni caso, comunque, l'art. 22 impone che tale processo di profilazione e di decisione automatizzata non sia lasciato in via esclusiva alla tecnologia, in quanto deve sempre essere garantito il diritto di ottenere l'intervento umano nella decisione. Così facendo l'art. 22 esclude quelle forme di autotutela esclusivamente tecnologica basate su algoritmi dei sistemi di *Digital Rights Management* che non prevedono un coinvolgimento umano.

Il processo decisionale automatizzato ha una portata diversa da quella della profilazione, cui può sovrapporsi parzialmente o da cui può derivare. Il processo decisionale esclusivamente automatizzato consiste nella capacità di prendere decisioni impiegando mezzi tecnologici senza coinvolgimento umano[477].

Le linee guida del Gruppo di Lavoro Articolo 29 ricordano come spesso "*il processo di profilazione è invisibile all'interessato. Funziona creando dati derivati o desunti in merito a persone fisiche, ossia dati personali "nuovi" che non sono stati forniti direttamente dagli interessati. Le persone fisiche hanno gradi diversi di comprensione e per alcune potrebbe essere difficile comprendere le complesse tecniche coinvolte nella profilazione e nei processi decisionali automatizzati*"[478]. Il titolare del trattamento, inoltre, secondo i Garanti europei, "*non può eludere le disposizioni dell'articolo 22 creando coinvolgimenti umani fittizi. Ad esempio, se qualcuno applica abitualmente profili generati automaticamente a persone fisiche senza avere alcuna influenza effettiva sul risultato, si tratterà comunque di una decisione basata unicamente sul trattamento automatico*"[479].

Per aversi un coinvolgimento umano, il titolare del trattamento deve garantire che qualsiasi controllo della decisione sia significativo e non costituisca un semplice gesto simbolico.

Chiaramente in ciò è bene ricordare che, in ogni caso, in qualunque trattamento dei dati personali, devono essere rispettati i diritti degli interessati al trattamento così come disposti dal GDPR. In particolare, gli articoli 12, 13 e 14 richiedono una informativa completa all'interessato di come avviene il trattamento e quali dati vengono raccolti; l'art. 15 consente di accedere ai dati personali ed altre informazioni in possesso del titolare del trattamento; l'art. 16 attribuisce all'interessato il diritto di rettificare i dati inesatti. In particolare, ai sensi dell'articolo 12, paragrafo 1, il titolare del trattamento deve fornire agli

[477] Gruppo Di Lavoro Articolo 29 Per La Protezione Dei Dati; *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del Regolamento 2016/790,* cit., 1 e ss.
[478] Gruppo Di Lavoro Articolo 29 Per La Protezione Dei Dati; *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del Regolamento 2016/790,* cit., 10 e ss.
[479] Gruppo Di Lavoro Articolo 29 Per La Protezione Dei Dati; *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del Regolamento 2016/790,* cit., 23 e ss.

interessati informazioni concise, trasparenti, intellegibili e facilmente accessibili sul trattamento dei loro dati personali.

Le linee guida del Gruppo art. 29 ricordano che "*le opportunità commerciali create dalla profilazione, da costi di memorizzazione più economici e dalla capacità di trattare grandi quantità di informazioni possono incoraggiare le organizzazioni a raccogliere più dati personali di quelli di cui hanno effettivamente bisogno, poiché tali dati potrebbero rivelarsi utili in futuro. Il titolare del trattamento deve assicurarsi di rispettare il principio di minimizzazione dei dati e le prescrizioni dei principi di limitazione della finalità e limitazione della conservazione*"[480]. Nel fare ciò il titolare del trattamento deve rispettare il principio di minimizzazione dei dati all'atto della raccolta e assicurare che i dati non siano conservati per un periodo superiore a quello necessario e proporzionato alle finalità per le quali i dati vengono trattati.

Inoltre, l'art. 17 consente di ottenere la cancellazione dei propri dati, attuando il c.d. "diritto all'oblio". Seguono poi nel testo normativo, il diritto di limitare il trattamento (art. 18), il diritto alla portabilità dei dati (art. 20), ed il diritto di opposizione (art. 21).

Solo ove il trattamento dei dati personali, compiuto dai titolari dei diritti d'autore per mezzo dei loro sistemi di *Digital Rights Management*, si svolga secondo le disposizioni sopra citate e nel rispetto delle libertà e dei diritti degli utenti allora potrà ritenersi legittimo, altrimenti dovrà qualificarsi come illecito. All'affermazione del diritto soggettivo, deve conseguire una possibilità di rimedio per non sfociare la legislazione in lettera morta ed il diritto del singolo in *uno ius minus quam perfectum*, se non *imperfectum*. Questa possibilità è data dall'apparato rimediale risarcitorio e dai poteri inibitori del Garante. Per il risarcimento ci riferiamo in particolare all'art. 82 GDPR con possibilità di liquidazione in senso patrimoniale e non patrimoniale, con inversione dell'onere probatorio ad esso connesso. Il Garante, adito sulla base del reclamo del soggetto interessato, potrà adottare tutte le misure idonee alla cessazione dell'illecito, in particolare ordinare la sospensione del trattamento, la cancellazione dei dati in possesso del titolare del trattamento ed eventuali sanzioni amministrative se del caso necessarie. Solo così il bilanciamento fra *l'enforcement* del diritto d'autore e la tutela della privacy potrà dirsi correttamente avvenuto.

5.5. Privacy Enhancing Technologies

Un'ultima strategia per combattere le derive autoritarie *dell'enforcement* del diritto d'autore rappresentate dalle tecnologie del *Digital Rights Management* consiste nel combattere la tecnologia con la tecnologia stessa.

Il riferimento ricade dunque sulle *Privacy Enhancing Technologies (PETs)*, definite dal Garante della Privacy come *"tecnologie o prodotti software utili per rafforzare o migliorare la protezione della privacy. Rientrano nelle PETs, ad esempio, i dispositivi per bloccare i cookies, i sistemi di cifratura, i software che ripristinano automaticamente l'anonimato dopo un certo periodo di tempo*[481]".

Questa nuova generazione di tecnologie è stata quindi sviluppata per aiutare i singoli utenti a controllare la quantità di informazioni personali che divulgano. Queste tecnologie promettono di consentire alle persone di assumere il controllo su come vengono raccolti i loro dati. L'obiettivo è ripristinare l'equilibrio di potere tra l'individuo che desidera mantenere

[480] Gruppo Di Lavoro Articolo 29 Per La Protezione Dei Dati; *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del Regolamento 2016/790,* cit.,12.

[481] Indagine conoscitiva della Commissione europea, *Tecnologie a protezione dei dati*, Doc-Web 1680228, liberamente accessibile presso: «https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1680228» (Ultimo accesso: 10 maggio 2022).

la privacy e molti attori nell'ambiente online che desiderano raccogliere informazioni personali.

Tali tecnologie rientrano nel più ampio concetto di Privacy by Design. Tale definizione è stata coniata per la prima volta dall'Information and Privacy Commissioner dell'Ontario e riguardava la possibilità di incorporare misure di privacy e tecnologie di miglioramento della privacy (PET) direttamente nella progettazione di tecnologie e sistemi informatici. Al giorno d'oggi, la Privacy by Design, o la sua variante del "Data Protection by Design", è considerata un concetto multiforme, che coinvolge varie componenti tecnologiche e organizzative che implementano i principi della privacy e della protezione dei dati nei sistemi e nei servizi.

Il GDPR in questo è molto chiaro, la Privacy by Design è oggi un obbligo giuridico per il trattamento dei dati personali nella dimensione digitale. Il Considerando 78 in questo senso dispone che "*la tutela dei diritti e delle libertà delle persone fisiche relativamente al trattamento dei dati personali richiede l'adozione di misure tecniche e organizzative adeguate per garantire il rispetto delle disposizioni del presente regolamento*". E in tal senso aggiunge che "*al fine di poter dimostrare la conformità con il presente regolamento, il titolare del trattamento dovrebbe adottare politiche interne e attuare misure che soddisfino in particolare i principi della protezione dei dati fin dalla progettazione e della protezione dei dati di default. Tali misure potrebbero consistere, tra l'altro, nel ridurre al minimo il trattamento dei dati personali, pseudonimizzare i dati personali il più presto possibile, offrire trasparenza per quanto riguarda le funzioni e il trattamento di dati personali, consentire all'interessato di controllare il trattamento dei dati e consentire al titolare del trattamento di creare e migliorare caratteristiche di sicurezza*".

Il Considerando 78 quindi chiede che in "*in fase di sviluppo, progettazione, selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati personali o che trattano dati personali per svolgere le loro funzioni, i produttori dei prodotti, dei servizi e delle applicazioni dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati allorché sviluppano e progettano tali prodotti, servizi e applicazioni e, tenuto debito conto dello stato dell'arte, a far sì che i titolari del trattamento e i responsabili del trattamento possano adempiere ai loro obblighi di protezione dei dati.*"

La normativa europea, quindi, traccia un distinguo: la Privacy by Design riguarda l'implementazione di un insieme di garanzie integrate nel sistema e nel processo del trattamento, mentre la Privacy by Default è orientata allo scopo di trattare solo i dati necessari attraverso dei meccanismi predefiniti[482].

In applicazione del Considerando 78, l'art. 25 GDPR dispone che, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso, il titolare debba mettere in atto misure tecniche e organizzative adeguate volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del GDPR e così tutelare i diritti degli interessati. In secondo luogo, poi, il titolare del trattamento dovrà porre in essere misure tecniche e organizzative adeguate a garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento.

Il maggior contributo in tema deriva sicuramente dalla Opinione emessa dal Gruppo dei Garanti Europei[483]. In tale parere il Gruppo dei Garanti distingue tra il principio generale

---

[482] In tal senso si esprime G. BINCOLETTO, *La privacy by design: Un'analisi comparata nell'era digitale*, in *Trento LawTech*, Student Paper n. 35, liberamente accessibile presso: «https://iris.unitn.it/retrieve/handle/11572/177733/511170/LawTech_Student_Papers_Bincoletto_Giorgia.pdf» (Ultimo accesso: 10 maggio 2022).

[483] European Data Protection Supervisor (EDPS) *Opinion 5/2018 - Preliminary Opinion on Privacy by Design,* 31 maggio 2018, liberamente accessibile presso: «https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf» (Ultimo accesso: 10 maggio 2022).

della Privacy by Design che racchiude una dimensione etica coerente con i principi e i valori della Carta dei diritti fondamentali dell'UE, e gli specifici obblighi di legge previsti dall'articolo 25 del GDPR a cui si fa riferimento come "Data Protection by Design" e "Data Protection by Default". L'opinione ripercorre altresì brevemente la storia del principio della Privacy by Design dalle prime ricerche sulle tecnologie per la privacy fino al GDPR.

L'Opinion è chiara nello stabilire la portata vincolante dell'art. 25 del GDPR, tanto da affermare che "*L'UE ha adottato disposizioni specifiche sulla definizione di soluzioni tecnologiche in caso di trattamento di dati personali. Dal 25 maggio 2018, quando il GDPR è diventato pienamente applicabile, la protezione dei dati fin dalla progettazione e per impostazione predefinita non sono più solo un desideratum o una buona pratica raccomandata, ma un obbligo legale e pienamente applicabile che tutti coloro che trattano dati personali ai sensi del diritto dell'UE devono rispettare*"[484].

L'opinione dell'EDPS ricorda che il termine "Privacy by Design" era stato originariamente utilizzato da Ann Cavoukian al tempo in cui ricopriva l'incarico di Information and Privacy Commissioner of Ontario, Canada. Nel suo concetto, la privacy by design poteva essere scomposta in "7 principi fondamentali" che sottolineavano la necessità di essere proattivi nel considerare i requisiti di privacy sin dalla fase di progettazione durante l'intero ciclo di vita dei dati, per essere "*integrati nella progettazione e nell'architettura dell'IT sistemi e pratiche aziendali [...] senza diminuire la funzionalità*"[485]

È tuttavia da notare che, al di là delle affermazioni di principio, la normativa dell'UE in materia di protezione dei dati e altri testi sulla privacy, come i Fair Information Practice Principles[486] o le linee guida dell'OCSE[487], specificano gli obiettivi da raggiungere senza di solito fornire indicazioni su come raggiungerli nella pratica. L'applicazione del principio della Privacy by Design tuttavia può comunque essere d'aiuto in questo contesto ove si traduca in una guida pratica per: (1) definire una metodologia per integrare i requisiti della privacy e della protezione dei dati nell'ambito di progetti volti a sviluppare e gestire un processo, una procedura o un sistema di trattamento dei dati personali; (2) individuare e attuare misure tecniche e organizzative adeguate da integrare in quei processi, procedure e sistemi a tutela delle persone e dei loro dati; (3) integrare il supporto alla privacy nel quadro gestionale e di *governance* dell'organizzazione, individuando compiti e definendo e allocando risorse e responsabilità[488].

---

[484] Nel testo dell'opinione si legge: "*The EU has adopted specific provisions on the shaping of technological solutions when there is processing of personal data. Since 25 May 2018, when the GDPR became fully applicable, data protection by design and by default are no longer only a desideratum or recommended good practice, but a legal and fully enforceable obligation that all those who process personal data under EU law must comply with. We need to keep the momentum going so that this new obligation can materialise and increase the effectiveness of the protection promised by the GDPR, and not construed too narrowly*"

[485] Così si esprime il testo originale: "*The term "privacy by design" was originally used by Ann Cavoukian when she was the Information and Privacy Commissioner of Ontario, Canada. In her concept, privacy by design can be broken down into "7 foundational principles" emphasising the need to be proactive in considering the privacy requirements as of the design phase throughout the entire data lifecycle, to be "embedded into the design and architecture of IT systems and business practices...without diminishing functionality...", with privacy as the default settings, end-to-end security including secure data destruction and strong transparency subject to independent verification.*"

[486] The Fair Information Practice Principles (FIPPs), liberamente rinvenibili presso: «https://web.archive.org/web/20090331134113/http://www.ftc.gov/reports/privacy3/fairinfo.shtm» (Ultimo accesso: 10 maggio 2022).

[487] Si veda in merito anche quanto affermato dalle linee guida OCSE, presso: «http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm» (Ultimo accesso: 10 maggio 2022).

[488] Nel testo originale si legge: "*Applying the principle of privacy by design can help to solve this issue as it translates into practical guidance, to:*

L'Opinion dei Garanti mostra alcune soluzioni ad oggi applicate che possono venire utili. In particolare, si concentra nel mostrare il lavoro di standardizzazione tecnologica oggi in corso per implementare sistemi di Privacy by Design direttamente all'interno delle tecnologie. Ad esempio, l'ISO ha emesso standard per un quadro per la privacy (ISO/IEC 29100) e un'architettura per la privacy (ISO IEC 29101) all'interno di un ambiente di tecnologia dell'informazione e della comunicazione. Il loro lavoro include l'estensione degli standard ISO/IEC 27001 e 27002 sulla gestione della sicurezza delle informazioni alla gestione della privacy. Un altro esempio è la RFC 697398 rilasciata dall'IETF su "Privacy Considerations for Internet Protocols", che mira all'inclusione dei requisiti di privacy nei protocolli Internet.

Nel 2015 la Commissione UE ha richiesto alle European Standardisation Organisations (ESOs), che hanno un accordo di cooperazione con la Commissione, di lavorare su un "*approccio alla privacy e alla protezione dei dati personali fin dalla progettazione*" e un "*quadro di gestione della privacy e della protezione dei dati" per il settore della sicurezza*[489] . Nel 2017, dopo l'adozione del GDPR, le ESO hanno considerato l'opportunità per un piano di lavoro più ampio e articolato che integri privacy, protezione dei dati e *cybersecurity*. Questa attività di standardizzazione può fornire una base per l'industria e tutte le parti interessate per stabilire lo stato dell'arte in materia di privacy fin dalla progettazione.

Non sarebbe chiaramente possibile procedere ad analizzare tutte le possibili forme tecnologiche di *Privacy Enhancing Technologies*, tuttavia possiamo fare riferimento ad alcuni esempi rilevanti come le strategie di progettazione chiamate "*attribute-based credentials*", o "*anonymous credentials*", che danno agli utenti la possibilità di autenticarsi presso un servizio senza rivelare la loro piena identità, ma semplicemente rivelando selettivamente, in modo affidabile, solo quegli attributi che sono strettamente necessari in quel contesto. Ciò è reso possibile dall'utilizzo di concetti crittografici specifici come le prove a conoscenza zero (*zero-knowledge proofs*).

Qualche successo è stato osservato anche in aree come i motori di ricerca. I browser più diffusi hanno aggiunto più controlli sulla privacy, come le funzionalità *Do Not Track* (DNT)[490] e il controllo dell'utente sulle funzionalità di tracciamento, e possono essere migliorati tramite molti componenti aggiuntivi che sopprimono i tentativi di tracciamento o limitano la profilazione. Il Gruppo dei Garanti nota altresì che "*anche le infrastrutture di comunicazione, come le reti Mix, e anche i sistemi operativi completi, sono stati sviluppati per la piena usabilità. Gli elementi orientati alla tecnologia del GDPR stanno innescando nuove idee commerciali basate*

---

1. define a methodology to integrate privacy and data protection requirements as part of projects aiming at developing and operating a process, procedure or system processing personal data;
2. identify and implement adequate technical and organisational measures to be integrated in those processes, procedures and systems to protect individuals and their data. Technological innovation can be a tool to support those measures;
3. integrate the support for privacy in the management and governance framework of the organisation, by identifying tasks and defining and allocating resources and responsibilities".

[489] Commissione Europea (2015) M/530 *Commission Implementing Decision C(2015) 102 final of 20.1.2015 on a standardisation request to the European standardisation organisations as regards European standards and European standardisation deliverables for privacy and personal data protection management pursuant to Article 10(1) of Regulation (EU) No 1025/2012 of the European Parliament and of the Council in support of Directive 95/46/EC of the European Parliament and of the Council and in support of Union's security industrial policy*, liberamente accessibile presso: «http://ec.europa.eu/growth/tools-databases/mandates/index.cfm?fuseaction=search.detail&id=548» (Ultimo accesso: 10 maggio 2022).

[490] La funzione DNT implementata nei client Web invia al sito Web un segnale comunicando che il client non desidera essere tracciato. Il W3C ha realizzato un'iniziativa di standardizzazione denominata Tracking Preference Expression, reperibile all'indirizzo: «http://www.w3.org/2011/tracking-protection/» (Ultimo accesso: 10 maggio 2022).

sulla tecnologia, ad es. supportare un meccanismo di consenso significativo e la portabilità dei dati. Tutti questi sviluppi dimostrano che la competenza tecnologica per l'implementazione della privacy by design è disponibile"[491].

L'Opinion dei Garanti ricorda che negli ultimi anni, l'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, ha continuato ad analizzare lo stato dell'arte e ha fornito raccomandazioni [492] rivolte a tutte le parti interessate, dagli sviluppatori alle autorità competenti, verso la creazione e il mantenimento di un archivio di *PET* adeguato e qualificato. Nell'ultima edizione della relazione, l'ENISA raccomanda che le autorità competenti e le autorità di regolamentazione promuovano "*l'uso dello strumento come archivio online delle valutazioni PET, nel contesto dell'attuazione pratica del principio della protezione dei dati fin dalla progettazione*", e che la comunità sostenga la ricerca "*partecipando attivamente come valutatori e utenti della piattaforma, oltre a incoraggiarne l'ulteriore utilizzo*"[493].

Altro esempio potrebbe essere quello dello strumento protettore dell'identità (c.d. "*identity protector*") che può essere visto come un elemento del sistema che controlla il rilascio della vera identità di un individuo a vari processi all'interno del sistema informativo. Il suo effetto è di isolare alcune aree del sistema, che non richiedono l'accesso alla vera identità dell'utente. Una delle sue funzioni più importanti è convertire l'identità effettiva di un utente in una pseudo-identità, un'identità alternativa (digitale) che l'utente può adottare quando utilizza il sistema. Identità alternative esistono anche nei sistemi convenzionali come numeri di conto bancario, numeri di previdenza sociale e numeri di assicurazione sanitaria, nonostante questi possano essere ricondotti alla vera identità dell'utente. Nei sistemi di protezione della privacy di questo tipo, il protettore dell'identità assumerebbe ad esempio la forma di una *smart card* controllata dall'utente, che potrebbe generare pseudo-identità come desiderato. In questo modo, la protezione dell'identità consente al progettista di un sistema di ridurre al minimo i dati personali archiviati in un database. In effetti, il fornitore di servizi non registrerebbe le attività dell'utente sotto la sua vera identità, ma piuttosto, sotto la sua pseudo-identità[494].

Ulteriori possibilità sono offerte da altri strumenti che eliminano le informazioni personali al fine di proteggere la privacy. I servizi di anonimizzazione consentono all'utente di navigare in Internet senza timore. Sono stati proposti numerosi schemi, ad esempio *proxy* anonimi, server anonimi/pseudonimi, *firewall* e similari . Ad esempio, il principio dei sistemi di *proxy* anonimi è semplice: viene creato un account con un *provider* di servizi Internet

---

[491] Nel testo originale si legge: "*Communication infrastructures, such as Mix networks, and also complete operating systems, have also been developed to full usability. The technology-oriented elements of the GDPR are triggering new business ideas based on technology, e.g. supporting meaningful consent mechanism and data portability. All these developments demonstrate that the technological competence for privacy by design implementation is available".*

[492] Per maggiori informazioni si veda Enisa Europa, "*Privacy by design in big data*", in *ENISA*, dicembre 2015, liberamente consultabile presso: «https://www.enisa.europa.eu/publications/big-data-protection» (Ultimo accesso: 10 maggio 2022); è altresì possibile rinvenire il lavoro dell'ENISA presso: «https://www.enisa.europa.eu/topics/data-protection/privacy-enhancing-technologies» (Ultimo accesso: 10 maggio 2022).

[493] Nel testo originale: "*In the latest edition of the report, ENISA recommends that competent authorities and regulators promote "the use of the tool as an online repository of PETs assessments, in the context of the practical implementation of the principle of data protection by design", that the research community support it by "actively participating as assessors and users of the platform, as well as encouraging its further use" and that the research community, the Commission, the EU institutions in the field of security and privacy engage in improving the platform."*

[494] V. SENICAR, B. JERMAN-BLAZIC, T. KLOBUCAR, *Privacy-Enhancing Technologies—approaches and development,* in *Laboratory for Open Systems and Networks*, Jozef Stefan Institute, Jamova 39, 1000 Ljubljana, Slovenia, liberamente accessibile presso: «https://www.researchgate.net/publication/223673501_Privacy-Enhancing_Technologies-approaches_and_development» (Ultimo accesso: 10 maggio 2022).

"fidato" (ovvero un ISP considerato affidabile sia dagli utenti che dalle organizzazioni commerciali). Un utente può registrare i propri dati personali con la certezza che non saranno ceduti a terzi o utilizzati per scopi di *marketing*. Tramite i *proxy,* quindi, alcuni tipi di comunicazione possono essere bloccati completamente, come ad esempio alcuni cookie o posta elettronica indesiderata. Il *firewall* è un dispositivo di protezione per proteggere una rete da accessi non autorizzati. I *firewall* sono considerabili come barriere tra un computer e Internet, configurandosi come dispositivi di protezione per schermare una rete da accessi non autorizzati. I *firewall* impongono una politica di accesso operando come gateway tra due reti. Diversi prodotti software consentono a un utente di configurare firewall personali che dipendono dalle sue preferenze.

Altri esempi sono quelli oggi offerti da sistemi di navigazione in Internet come Crowds, Tor (The Onion Router) e similari, intesi come un sistema per proteggere la privacy degli utenti durante la navigazione sul Web. Ad esempio, tali servizi di navigazione riescono ad impedire a un server Web visitato da un utente di apprendere informazioni che potrebbero identificarlo. Il sistema Crowds, ad esempio, opera raggruppando gli utenti in un gruppo (*crowd*) ampio e geograficamente diversificato che invia collettivamente richieste per conto dei suoi membri. I server Web non sono in grado di conoscere la vera fonte di una richiesta perché è altrettanto probabile che provenga da qualsiasi membro della folla[495]. Similmente il modello di Tor[496] dirige il traffico Internet attraverso una rete c.d "*overlay*" gratuita, mondiale e volontaria, composta da più di seimila nodi per nascondere la posizione e l'utilizzo di un utente a chiunque stia effettuando la sorveglianza della rete o l'analisi del traffico. L'uso di Tor rende più difficile tracciare l'attività su Internet dell'utente.

Appare dunque, in linea evolutiva, che possa essere richiesto ai titolari del trattamento, ai titolari quindi, nel nostro caso, dei diritti d'autore ed ai produttori di sistemi di *Digital Rights Management,* non solo di rispettare le normative in tema di trattamento dei dati personali, ma altresì di adottare soluzioni tecniche che possano incorporare direttamente la tutela della privacy nei software di DRM.

6. Considerazioni conclusive

In questo capitolo ci si era posti l'obiettivo di analizzare una delle strategie di *enforcement* del diritto d'autore che connotano la dimensione digitale, ossia la "*produzione di sistemi di Digital Rights Management (DRM) che abilitano la gestione ed il commercio di file associati a misure tecnologiche di protezione che, tra l'altro, possono impedire la copia e la distribuzione non autorizzate*[497]".

In particolare, dopo un breve chiarimento tecnologico si è avuto modo di vedere come i maggiori sistemi di *Digital Rights Management* basino la propria attività su un intenso monitoraggio delle attività compiute dagli utenti, nello specifico con riguardo al consumo di prodotti intellettuali. In questo senso il richiamo alle tecnologie quali *l'hashing*, il *watermarking*, il *fingerprinting* hanno dimostrato la potenzialità lesiva di una deriva autoritaria di questi sistemi di gestione dei contenuti digitali.

---

[495] V. SENICAR, B. JERMAN-BLAZIC, T. KLOBUCAR, *Privacy-Enhancing Technologies—approaches and development,* cit., 148 e ss.

[496] Per maggiori informazioni si faccia riferimento alla pagina informativa di Tor liberamente accessibile presso: «https://metrics.torproject.org» (Ultimo accesso: 10 maggio 2022).

[497] R. CASO, *Il conflitto tra copyright e privacy nelle reti Peer to Peer: il caso Peppermint – Profili di diritto comparato*, cit. 5 e ss.

Le disposizioni sia nazionali che internazionali riguardanti tanto l'ordinamento statunitense, quanto quello italiano, partono dalla prospettiva della tutela del diritto d'autore, disponendo normative volte a fornire un'adeguata tutela giuridica contro le elusioni delle misure tecnologiche. In particolare, si è visto come nessuna norma internazionale chieda di concentrarsi sul bilanciamento fra gli interessi dei *copyright holders* e quelli degli utenti alla loro privacy. Le disposizioni internazionali dei trattati WIPO, come visto, ebbero un forte impatto sulle normative nazionali, tanto che sia il DMCA che la Direttiva 29/2001 ne ripropongono le prospettive. In questo senso l'approccio europeo è volto ad evitare soluzioni frammentarie dei singoli Stati, avendo invece ritenuto necessario un approccio armonizzato alle sfide tecnologiche poste dai sistemi di *Digital Rights Management*, motivo per cui il Decreto Legislativo 68/2003, che ¢traspone in Italia la Direttiva, aggiunge poco o nulla alla normazione europea. Analizzando la Direttiva 29/2001 è emerso come il legislatore europeo paia quasi incoraggiare l'uso di queste tecnologie nel campo della tutela della proprietà intellettuale sebbene, come emerso dal Considerando 60, tali misure non dovrebbero ostare alla tutela della privacy. Nella Direttiva, infatti, sono presenti disposizioni che chiedono di attuare un corretto bilanciamento fra contrapposte esigenze, ma non si spingono fino a dire come questo bilanciamento debba avvenire, risolvendosi in vuote declamazioni di principio. Similmente, anche la legislazione statunitense, tramite il DMCA, procede a criminalizzare la produzione e la diffusione di tecnologie che consentano agli utenti di eludere i sistemi di DRM. Tuttavia, allo stesso tempo, dispone che una simile elusione non sarebbe illecita ove compiuta per tutelare la propria privacy in presenza di una violazione della stessa. In ogni caso, tutte le normative analizzate sembrano disperatamente sbilanciate verso la tutela degli interessi dei *copyright holders*.

Dopo un riferimento alle varie tecnologie utilizzabili per la progettazione dei sistemi di *Digital Rights Management*, analizzate poi sotto il particolare angolo previlegiato dei sistemi di *Automatic Content Recognition*, abbiamo tentato di mettere in luce quali aspetti della privacy vengono coinvolti nell'applicazione dei DRM.

In questo, un contributo principale è venuto dalla dottrina di Julie E. Cohen che efficacemente distingue fra una privacy intellettuale ed una privacy spaziale in relazione al consumo dei prodotti intellettuali.

Tali tecnologie, infatti, creano le potenzialità per una vasta attività di raccolta di informazioni circa le abitudini di consumo dei prodotti protetti dal diritto d'autore, con una conseguente limitazione del "*breathing space*" lasciato agli individui nei loro spazi privati. Questa forma di monitoraggio, infatti, tocca anche quella dimensione della privacy che è stata definita "spaziale" e che protegge certi luoghi come zone di ritiro ed escluse dall'osservatore esterno, riducendo l'autonomia nell'uso e nel godimento dei prodotti intellettuali.

Inoltre, simili tecnologie, come visto, monitorando gli utenti, possono creare dei repertori di preferenze, utili per una completa profilazione dell'utente utilizzabile poi ai fini di *marketing* e di pubblicità mirata. La raccolta di informazioni sul consumo intellettuale rende accessibili le preferenze intellettuali, sia al fornitore delle informazioni che a terzi che potrebbero acquistarle o invocare procedimenti legali per costringerne la produzione. Spesso questo monitoraggio è poi alla base di forme sanzionatorie in via di autotutela nelle ipotesi in cui sia intervenuto un comportamento da parte dell'utente contrastante con la volontà dei titolari del diritto d'autore. Nel fare questo, ci si scontra anche con i principi che vietano il ricorso all'autotutela e che al contempo escludono la possibilità di decisioni automatizzate che abbiano un effetto giuridico sulla persona.

In questo senso, un'attenta dottrina ha recentemente rilevato come l'obiettivo odierno sia quello di "*lavorare all'adozione di strumenti regolatori e di governo, preordinati ad evitare che la saldatura tra potere economico e potere tecnologico produca una società della sorveglianza e della discriminazione, in cui tutti siano profilati, segmentati in gruppi e resi destinatari di effetti giuridici o sociali in funzione dell'assetto di potere esistente. Non può, infatti, ignorarsi il pericolo che […] i nuovi modelli algoritmici creino le condizioni per un nuovo medioevo digitale. Si delinea cioè il rischio «di una società connotata da una segmentazione per caste, ove lo status non è però dato dalla nascita o dall'appartenenza a classificazioni sociali tradizionali […], ma da algoritmi e dai valori di coloro che li generano. Classificazioni che sono poi impiegate per prendere decisioni che coinvolgono una pluralità di soggetti, i quali però non hanno contezza della propria posizione*»"[498].

L'ultima parte del presente capitolo quindi si è voluta profondere nel ricercare nell'attuale sistema legislativo e giurisprudenziale un possibile punto di equilibrio con la tutela della riservatezza e dei dati personali. Si è quindi riscontrata la presenza, tanto nel sistema americano quanto in quello europeo, di sufficienti strumenti per tutelare gli utenti che potrebbero essere utilizzati per arginare quantomeno le forme più palesi e vistose di violazione dei diritti degli interessati.

Partendo dalla costatazione per cui il nemico naturale dell'autotutela tecnologica è il legislatore e in definitiva lo Stato, si è avuto modo di ricorrere, alla ricerca di strumenti normativi statunitensi, all'opera di Prosser ed al Restatament of torts, mostrando come istituti nati in un mondo predigitale possano essere interpretati dalle Corti di *Common Law* sotto una nuova luce, comprendendo entro il loro ambito applicativo alcuni aspetti della moderna società. In questo i tort della *intrusion upon seclusion*, della *public disclosure of private facts* e della *appropriation of name or likeness* potrebbero, se riletti alla luce delle recenti pronunce giurisprudenziali, comprendere anche le intrusioni nella vita privata degli utenti tramite monitoraggio digitale.

Parimenti, si è avuto modo di constatare come l'ordinamento europeo disponga di un potente strumento a tutela degli utenti, ossia il Regolamento 2016/679. Per il tramite delle norme in esso contenute abbiamo visto come difficilmente un trattamento dei dati personali potrebbe essere effettuato, possibile solo ove tutti i requisiti richiesti dalla normativa, come commentata, fossero effettivamente rispettati. L'assenza di una legittima base legale quale il consenso esplicito, o la mancanza dell'adozione di soluzioni tecniche volte a rispettare i principi di minimizzazione dei dati porterebbe ad escludere *ictu oculi* la validità di simili trattamenti. Guardando poi all'art. 22 ed al tema della profilazione o dei modelli decisori automatizzati, si è visto che molte delle forme di autotutela tecnologica adottabili tecnicamente dai titolari dei diritti d'autore sarebbero illecite.

Solo al termine del capitolo si è tentato un approccio differente. Senza voler vedere necessariamente la tecnologia come un mostro da combattere con le poderose armi delle norme giuridiche, si è tentato di mettere in luce come forse si potrebbe imporre alla tecnologia stessa di tutelare i vari interessi in gioco. L'intento lodevole di voler tutelare il diritto d'autore potrebbe combinarsi con l'intento, altrettanto lodevole, di tutelare il corretto trattamento dei dati personali.

Non è tuttavia compito di questo elaborato tentare in via aleatoria di prevedere il futuro, non resta dunque che rimandare alle prossime elaborazioni, con una certa qual

[498] G. ALPA, G. RESTA, *Le Persone e la Famiglia 1, Le persone fisiche e i diritti della personalità*, cit., 525.

speranza, per tutti i giuristi, di poter lasciare il mondo un po' meglio di come lo abbiamo trovato[499].

[499] Come diceva BADEN-POWELL, in *L'ultimo messaggio di B.-P. agli Esploratori*: "*Prova a lasciare questo mondo un po' meglio di come l'hai trovato e quando arriva il tuo momento per morire, tu puoi morire felice nel sentire che in ogni caso tu non hai perso il tuo tempo ma hai fatto del tuo meglio*".

CAPITOLO QUARTO
DIRETTIVA 2019/790, ART. 17: ANALISI E CRITICHE

1. Considerazioni preliminari: una nuova strategia di *enforcement* del diritto d'autore.

In quest'ultimo capitolo del presente elaborato, l'attenzione si volge ad una specifica introduzione legislativa: la Direttiva 2019/790 "*sul diritto d'autore e sui diritti connessi nel mercato unico digitale*". In particolare, il suo articolo 17 tratta dell' "*utilizzo di contenuti protetti da parte di prestatori di servizi di condivisione di contenuti online*" e nella sua analisi vedremo come le norme in esso contenute possano scontrarsi con altri diritti ed istanze del panorama digitale ed in particolare quelle alla privacy ed al corretto trattamento dei dati personali.

Sin dalle prime righe del presente elaborato si è tentato di tracciare un attento contesto in cui si inseriscono i diritti d'autore ed i diritti alla riservatezza ed al trattamento dei dati personali, non nascondendo che il bilanciamento che deve guidare l'interprete nell'approcciarsi ad essi non è di facile risoluzione, anzi spesso è altalenante o dimenticato dalle Corti. I nodi vengono al pettine proprio oggi, momento in cui massimamente si percepisce tale tensione, e si congiungono proprio nell'articolo 17 in commento.

Pare essenzialmente che il diritto d'autore abbia rinvenuto nel legislatore europeo un formidabile alleato per i fini di *enforcement* delle prerogative dei titolari del *copyright* nel mondo digitale. Senza voler anticipare oltremodo le analisi che verranno di seguito compiute, pare evidente che l'ultima battaglia si stia combattendo proprio sulle piattaforme online, quali *YouTube* o *Facebook*. Si chiede, meno velatamente di quanto il legislatore europeo voglia far trasparire, di adottare soluzioni tecniche volte a tutelare tecnologicamente il diritto d'autore mediante meccanismi di filtraggio dei contenuti e tramite una sorveglianza generale e capillare dei comportamenti degli utenti su tali piattaforme. E come ormai si avrà modo di immaginare, ogni volta che si tenta di procedere ad un *enforcement* del diritto d'autore, l'eccesso di tutela è sempre in agguato e, conseguentemente, a rimetterci sono le tutele di cui dovrebbe godere l'utente, declamate, certo, ma poi dimenticate.

In questo capitolo, dunque, si è scelto di concentrarsi in via esclusiva su tale disposizione normativa, rimandando ad altri elaborati per una compiuta analisi delle altre novità introdotte con la Direttiva 2019/790. Dopo un breve riferimento al contesto di concepimento di questo testo normativo e alla sua attuazione, si passerà in un primo momento all'analisi dell'articolo 17, necessaria al fine della comprensione dei ragionamenti in tema di bilanciamento con il diritto alla privacy degli utenti. La seconda parte dell'esposizione, quindi, sarà proprio diretta a mettere in luce tutte le difficoltà che la Direttiva pone in tema di riservatezza ed altri diritti fondamentali, tentando di rinvenire nel panorama normativo attuale, argini e soluzioni che, senza sacrificare il diritto d'autore, tengano in debito conto gli interessi degli utenti.

1.1. La strada verso la nuova Direttiva: l'art. 17

La storia della direttiva in commento può essere, secondo alcuni autori,[500] fatta risalire alla consultazione pubblica sulla revisione delle norme dell'UE sul diritto d'autore, tenutasi

[500] J. P. QUINTAIS, P. MEZEI, I. HARKAI, J. C. MAGALHÃES, C. KATZENBACH, S. F. SCHWEMER, & T. RIIS, *Final Report on mapping of EU legal framework and intermediaries' practices on copyright content moderation and removal*, 2022, 49

tra il dicembre 2013 ed il marzo 2014[501]. La consultazione ha coperto un'ampia gamma di questioni sull'applicazione delle norme dell'UE in materia di diritto d'autore nell'ambiente digitale, tra cui territorialità, la definizione di diritti ed eccezioni al diritto d'autore nel panorama online, e persino la possibilità di un'unificazione del diritto d'autore dell'UE. La consultazione ha prodotto molte risposte, riassunte dalla Commissione in una relazione pubblicata nel 2014[502], seguita poi da un "libro bianco" della Commissione, pubblicato nel giugno 2014[503]

Il 6 maggio 2015, sotto la firma del Presidente della Commissione Jean-Claude Juncker, venne presentata in sede europea la Comunicazione 2015/192 con la quale venne proposta la nuova strategia per il Mercato Unico Digitale. Nelle parole del Presidente della Commissione, si legge: "*Sono convinto che dobbiamo sfruttare in maniera decisamente migliore le notevoli opportunità offerte dalle tecnologie digitali, che non conoscono confini. Per realizzare questo obiettivo dovremo avere il coraggio di superare i compartimenti stagni delle regolamentazioni nazionali nel settore delle telecomunicazioni, nella legislazione sui diritti d'autore e sulla protezione dei dati, nella gestione delle onde radio e nell'applicazione del diritto della concorrenza. Se agiamo in tal senso, presto potremo […] creare condizioni eque affinché tutte le imprese che offrono prodotti o servizi nell'Unione europea siano soggette alle medesime norme sulla protezione dei dati e dei consumatori, indipendentemente dal luogo in cui si trovano i loro server. Per realizzare questo proposito, nei primi sei mesi del mio mandato intendo prendere decisioni legislative ambiziose per realizzare un mercato unico del digitale connesso, in particolare concludendo rapidamente i negoziati sulla normativa comune europea in materia di protezione dei dati, ampliando la portata dell'attuale riforma della regolamentazione nel settore delle telecomunicazioni, aggiornando la normativa sui diritti d'autore tenendo conto della rivoluzione digitale e dei comportamenti mutati dei consumatori nonché modernizzando e semplificando le norme che disciplinano gli acquisti in linea e digitali dei consumatori*"[504].

Nel corso del suo mandato tali obiettivi vennero rispettati, non solo con la conclusione del Regolamento 2016/679, il GDPR, ma anche con la conclusione dei negoziati e la conseguente adozione della Direttiva 2019/790, riformante il diritto d'autore, tentando una armonizzazione delle legislazioni degli Stati membri per far fronte alle sfide poste dalle evoluzioni digitali.

Sul piano che ora ci interessa, la Comunicazione afferma che il diritto d'autore deve essere visto come il supporto della creatività e dell'industria della cultura in Europa. L'Unione Europea infatti, in questo, fa un forte affidamento sulla creatività per essere competitiva su scala globale tanto che dalla Comunicazione emerge che i contenuti digitali sono uno dei propulsori principali della crescita dell'economia digitale: il 56% degli europei, già nel 2015, usava Internet con finalità culturali e le previsioni indicavano un tasso di crescita per tale settore.

---

e ss, in *Zenodo*, liberamente accessibile presso: «https://doi.org/10.5281/zenodo.6461568» (Ultimo accesso: 10 maggio 2022)

[501] Commissione Europea, *Public Consultation on the Review of EU Copyright Rules* (2013) (On file with the authors).

[502] Commissione Europea, *Report on the responses to the Public Consultation on the Review of the EU Copyright Rules*, Directorate General Internal Market and Services, Directorate D – Intellectual property, D1 – Copyright (July 2014) (On file with the authors).

[503] Commissione Europea, White Paper, *A Copyright Policy for Creativity and Innovation the European Union* (2014), liberamente accessibile presso: «https://www.dropbox.com/s/0xcflgrav01tqlb/White%20Paper%20%28internal%20draft%29%20%281%29.PDF» (Ultimo accesso: 10 maggio 2022)

[504] Comunicazione della Commissione al Parlamento europeo e al Comitato delle regioni, *Strategia per il mercato unico digitale in Europa* (COM 2015 192), 6 maggio 2015, disponibile al link:«https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A52015DC0192» (Ultimo accesso: 10 maggio 2022).

In questo ragionamento, dunque, appariva chiara la necessità di una armonizzazione del diritto d'autore, comprendendo come fosse centrale, ai fini dell'investimento nell'innovazione, intavolare un dialogo sulla posizione delle piattaforme di condivisione di contenuti culturali. Dato il ruolo sempre maggiore che gli intermediari online andavano assumendo nella distribuzione dei contenuti, occorreva proprio chiarire le norme applicabili all'attività che essi svolgono in relazione alle opere protette da diritto d'autore.

La Comunicazione del 2015, inoltre, afferma che lo sviluppo di Internet in Europa ha poggiato sul principio, affermato nella Direttiva sul commercio elettronico, come visto, secondo il quale i prestatori intermediari di servizi via Internet non sono responsabili dei contenuti che trasmettono, conservano o ospitano purché mantengano al riguardo un comportamento passivo. Allo stesso tempo, gli intermediari sono tenuti ad intervenire efficacemente per rimuovere i contenuti illeciti individuati, siano essi informazioni inerenti ad attività illegali quali il terrorismo o la pedopornografia oppure informazioni che violano i diritti di proprietà intellettuale altrui. La Commissione europea, tuttavia, nota che i risultati dell'attuazione di quella normativa non sono stati soddisfacenti, come invece auspicato. Per questo afferma che "*attualmente la disattivazione dell'accesso a contenuti illeciti e la rimozione di questi da parte dei prestatori di servizi di hosting può rivelarsi un processo lungo e complicato, con il rischio che siano rimossi per errore anche contenuti che sono invece leciti*[505]".

È quindi sulla base di questi obiettivi che vennero presentate le proposte per l'adozione di una nuova Direttiva europea sul diritto d'autore, la quale, per la visuale prescelta dal presente elaborato, si concentra proprio, nel suo articolo 17, sulla posizione degli intermediari e sulla conseguente riforma della loro responsabilità per quanto riguarda l'illecita comunicazione al pubblico di materiali protetti dal diritto d'autore.

Nel frattempo, il 9 dicembre 2015, la Commissione aveva altesì proposto una *Public Consultation on the Evaluation and Modernisation of the Legal Framework for the Enforcement of Intellectual Property Rights*[506]. Essa venne subito seguita nel 2016 dalla Comunicazione 2016/228[507] concernente nello specifico proprio le piattaforme online e il mercato unico digitale. In questa Comunicazione, la Commissione europea concentra la propria attenzione sull'emersione di nuove forme di distribuzione dei contenuti online, grazie alle quali i contenuti protetti dal diritto d'autore, caricati dagli utilizzatori finali, vengono messi a disposizione del pubblico.

Questo comporta, a parere della Commissione, delle perplessità sulla correttezza della ripartizione, tra i distributori e i titolari dei diritti, del valore generato da alcune di queste nuove forme di distribuzione. La Commissione si proponeva quindi di occuparsi di tale questione attraverso una normativa settoriale nell'ambito del diritto d'autore e si impegnava inoltre nell'affrontare il problema dell'equa remunerazione dei creatori nei loro rapporti con le piattaforme online. La Commissione decise dunque di continuare, in questo senso, a

---

505 Comunicazione della Commissione al Parlamento europeo e al Comitato delle regioni, *Strategia per il mercato unico digitale in Europa* (COM 2015 192), 6 maggio 2015, cit.

506 Per maggiori riferimenti si veda il file PPT qui allegato: «https://www.google.it/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiLxoHvpYb2AhUI57sIHahYBsoQFnoECAoQAQ&url=https%3A%2F%2Fec.europa.eu%2Fdocsroom%2Fdocuments%2F18944%2Fattachments%2F1%2Ftranslations%2Fen%2Frenditions%2Fnative&usg=AOvVaw1vfiwRBHYIhOTApTtdqO7N» (Ultimo accesso: 10 maggio 2022).

507 Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions: *Online Platforms and the Digital Single Market Opportunities and Challenges for Europe*, COM/2016/0288 final, liberamente accessibile presso: «https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52016DC0288&from=EN» (Ultimo accesso: 10 maggio 2022).

collaborare con le piattaforme alla costituzione e all'applicazione di meccanismi di cooperazione su base volontaria che permettano, utilizzando un approccio c.d. "*follow the money*", di privare le persone che commettono violazioni commerciali dei diritti di proprietà intellettuale delle entrate provenienti da tali attività illegali.

Allo stesso tempo, la medesima Comunicazione si interessa del trattamento dei dati personali che può insorgere nella gestione di queste piattaforme online, a dimostrazione che un discorso sul diritto d'autore, oggi, è, quantomeno in questo campo, difficilmente slegabile da considerazioni in tema di privacy.

La Commissione, nella Comunicazione 2016/228, notava infatti come ampie fasce del pubblico continuassero a diffidare della raccolta dei dati e ritenessero necessaria una maggiore trasparenza da parte di tutti gli attori del mondo digitale. Le piattaforme online, secondo la Commissione, avrebbero dovuto rispondere a queste preoccupazioni spiegando agli utenti in modo più efficace quali sono i dati personali che vengono raccolti e come vengono condivisi e utilizzati, conformemente a quanto comunque oggi previsto dal GDPR. Più in generale, secondo la Commissione, rientrano in tale problematica anche le modalità con cui gli utenti si identificano per accedere a piattaforme e servizi online. È pacifico che una moltitudine di combinazioni di nomi utente e password, oltre che essere scomoda, rappresenta anche un rischio per la sicurezza. Tuttavia, la pratica frequente di utilizzare il proprio profilo di accesso ad una piattaforma per accedere a una gamma di siti web e servizi implica spesso scambi e interconnessioni non trasparenti di dati personali tra varie piattaforme online e siti web. Nello stesso senso, la Commissione riteneva necessaria una maggiore trasparenza per gli utenti affinché potessero comprendere come venivano filtrate, determinate o personalizzate le informazioni presentate dalle piattaforme stesse, soprattutto quando tali informazioni costituivano la base di decisioni di acquisto o influenzavano la loro partecipazione alla vita civile o democratica.

1.2. L'adozione della Direttiva 2019/790: il nuovo art. 17

Il 14 settembre 2016 la Commissione Europea lanciò la sua nuova *Proposta di Direttiva del Parlamento europeo e del Consiglio sul diritto d'autore nel mercato unico digitale*[508]. Senza procedere all'analisi del testo della proposta, basti notare che l'art. 13[509] della stessa venne elaborato considerevolmente in sede di adozione della Direttiva, risultando nell'attuale art. 17.

---

[508] Proposta di Direttiva del Parlamento Europeo e del Consiglio sul diritto d'autore nel mercato unico digitale COM/2016/0593 final - 2016/0280 (COD), liberamente accessibile presso: «https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52016PC0593&from=IT» (Ultimo accesso: 10 maggio 2022).

[509] In particolare, il testo della proposta poi confluito nell'art 17 della Direttiva disponeva che "*I prestatori di servizi della società dell'informazione che memorizzano e danno pubblico accesso a grandi quantità di opere o altro materiale caricati dagli utenti adottano, in collaborazione con i titolari dei diritti, misure miranti a garantire il funzionamento degli accordi con essi conclusi per l'uso delle loro opere o altro materiale ovvero volte ad impedire che talune opere o altro materiale identificati dai titolari dei diritti mediante la collaborazione con gli stessi prestatori siano messi a disposizione sui loro servizi. Tali misure, quali l'uso di tecnologie efficaci per il riconoscimento dei contenuti, sono adeguate e proporzionate. I prestatori di servizi forniscono ai titolari dei diritti informazioni adeguate sul funzionamento e l'attivazione delle misure e, se del caso, riferiscono adeguatamente sul riconoscimento e l'utilizzo delle opere e altro materiale.*

2.Gli Stati membri provvedono a che i prestatori di servizi di cui al paragrafo 1 istituiscano meccanismi di reclamo e ricorso da mettere a disposizione degli utenti in caso di controversie in merito all'applicazione delle misure di cui al paragrafo 1.

3.Gli Stati membri facilitano, se del caso, la collaborazione tra i prestatori di servizi della società dell'informazione e i titolari dei diritti tramite dialoghi fra i portatori di interessi, al fine di definire le migliori prassi, ad esempio l'uso di tecnologie adeguate e proporzionate per il riconoscimento dei contenuti, tenendo conto tra l'altro della natura dei servizi, della disponibilità delle tecnologie e della loro efficacia alla luce degli sviluppi tecnologici". Per maggiori informazioni e commenti dottrinali si segnalano: L. ALBERTINI, *La modifica al diritto d'autore europeo per tener conto del contesto digitale: note sugli artt. 11 (diritto degli editori)*

Ad oggi dunque, in seguito ai lavori durati quasi un lustro, la Direttiva 2019/790 dispone al suo art. 17 una normativa specifica per la responsabilità di quei *provider* che concedano l'accesso al pubblico a contenuti protetti dal diritto d'autore.

Compiendo una veloce panoramica introduttiva, possiamo notare che il primo paragrafo tratta dei "*prestatori di servizi di condivisione di contenuti online*" e procede ad affermare che essi effettuano un "*atto di comunicazione al pubblico o un atto di messa a disposizione del pubblico*" ove concedano l'accesso ad opere protette dal diritto d'autore o altri materiali protetti caricati dai suoi utenti. Questo primo paragrafo, come di seguito procederemo a denotare, stabilisce l'ambito soggettivo ed oggettivo di applicazione della nuova disciplina dell'art. 17.

In secondo luogo, l'art. 17 dispone che un prestatore di servizi di condivisione di contenuti online è oggi tenuto ad ottenere un'autorizzazione dai titolari dei diritti d'autore, ad esempio mediante la conclusione di un accordo di licenza, al fine di comunicare al pubblico o rendere disponibili al pubblico opere o altri materiali, tenendo in debito conto che una tale autorizzazione dovrebbe includere anche gli atti compiuti dagli utenti (c.d *User Generated Content)* qualora non agiscano su base commerciale o qualora la loro attività non generi ricavi significativi.

In terzo luogo, poi, si stabilisce che ove non sia concessa alcuna autorizzazione o licenza, i prestatori di servizi di condivisione di contenuti online sono responsabili per atti lesivi dei diritti di proprietà intellettuale a meno che non dimostrino di soddisfare alcune condizioni, previste al quarto paragrafo, per andare esenti da responsabilità. Su queste condizioni si avrà modo di soffermarsi con maggior attenzione, in quanto, proprio su questi punti, si percepisce maggiormente il delicato bilanciamento che deve essere compiuto con altri diritti fondamentali.

Le altre disposizioni dell'art. 17, meno rilevanti ai fini della presente dissertazione, verranno toccate nell'analisi che si propone di seguito e che si concentrerà tuttavia, per economia di pensieri, sui tre punti sopra citati. Dopo aver inquadrato il tema controverso, quindi, si procederà ad un'attenta analisi in chiave di bilanciamento rispetto all'*enforcement* del diritto d'autore ed il suo conflitto con i diritti fondamentali ed in particolare con la riservatezza.

2. L'ambito di applicazione soggettivo: "OCSSP"

Per analizzare le implicazioni giuridiche dell'art. 17 della Direttiva in commento, il necessario punto di partenza è la definizione dell'ambito soggettivo di sua applicazione. Come accennato, il paragrafo primo tratta di quei "*prestatori di servizi di condivisione di contenuti online*", (*online content-sharing service provider,* in acronimo "*OCSSP*"). Tale tipologia di *provider* viene definito dall'art. 2 al punto 6 come "*un prestatore di servizi della società dell'informazione il cui scopo principale o uno dei principali scopi è quello di memorizzare e dare accesso al pubblico a grandi quantità di opere protette dal diritto d'autore o altri materiali protetti caricati dai suoi utenti, che il servizio organizza e promuove a scopo di lucro*".

---

e 13 (responsabilità dei provider) della bozza di Direttiva UE nel febbraio 2019, uscita dalla fase c.d. trilogue, in *MediaLaws, Law and Media Working Paper Series* no. 2/2019, disponibile sul sito: «https://www.medialaws.eu/wp-content/uploads/2019/04/Lorenzo.pdf» (Ultimo accesso: 10 maggio 2022); C. ANGELOPOULOS, *On Online Platforms and the Commission's New Proposal for a Directive on Copyright in the Digital Single Market*, 2017, disponibile sul sito: DOI:10.2139/SSRN.2947800 (Ultimo accesso: 10 maggio 2022); A. GIANNOPOULOU, *Proposed Directive on Copyright in the Digital Single market: a missed opportunity?*, in *Zenodo,* 2018, disponibile sul sito: «https://doi.org/10.5281/zenodo.1415493» (Ultimo accesso: 10 maggio 2022).

Come fatto notare da alcuni recenti contributi dottrinali[510], il disegno normativo dell'art. 17 costituisce un approccio del tutto nuovo al tema della responsabilità dei Service Provider. Prima di questa nuova introduzione legislativa, infatti, il diritto dell'UE non attribuiva alcuna responsabilità specificamente ad una categoria di ISP legalmente individuata, piuttosto la connetteva ad atti, servizi o funzioni svolti dagli stessi provider. In questo, si consideri anche che la forma di responsabilità prevista dalla Direttiva *e-commerce* era chiaramente "indiretta". Ora, invece, la responsabilità si è trasformata in "diretta" in connessione ad atti compiuti dagli utenti, nonché connessa alla stessa qualificazione giuridica di un provider come OCSSP. Appare dunque di estrema importanza, proprio per queste ragioni, partire, nell'analisi dell'articolo 17 in commento, dall'ambito soggettivo di sua applicazione.

Il Considerando 62 della Direttiva specifica in merito che alcuni servizi della società dell'informazione, nel quadro del loro normale utilizzo, sono concepiti in modo da dare al pubblico l'accesso a contenuti o altri materiali protetti dal diritto d'autore caricati dai loro utenti. Tali servizi, secondo la Direttiva, sarebbero svolti da questi *provider* "OCSSP", la cui definizione sarebbe intesa a comprendere unicamente i servizi online che svolgono un ruolo importante sul mercato dei contenuti digitali, in concorrenza con altri servizi di pari portata. Esempi, secondo il Considerando 62, sarebbero i servizi di streaming audio e video online. Chiaramente, il legislatore europeo, nello stilare le caratteristiche che simili *provider* dovrebbero possedere, aveva in mente l'operato di piattaforme come *YouTube, Instagram* e *Pinterest*: i colossi della condivisione dei contenuti digitali.

Per questa ragione, allora, tale ambito soggettivo di applicazione della Direttiva in commento mira a comprendere tutti quei servizi che hanno come scopo principale, o come uno degli scopi principali, quello di memorizzare e consentire agli utenti di caricare e condividere un gran numero di contenuti, al fine di trarne profitto. Tale risultato può essere ottenuto, secondo il legislatore, direttamente o indirettamente, organizzando e promuovendo simili contenuti per attirare un pubblico più vasto.

Prima di focalizzarci sugli elementi distintivi di una simile definizione è bene chiarire preliminarmente, come del resto compie il legislatore europeo, quali *provider* sono invece categoricamente esclusi da tale disciplina. In tal senso, l'art. 2 paragrafo 6 afferma che "*i prestatori di servizi quali le enciclopedie online senza scopo di lucro, i repertori didattici o scientifici senza scopo di lucro, le piattaforme di sviluppo e di condivisione di software open source, i fornitori di servizi di comunicazione elettronica ai sensi della Direttiva (UE) 2018/1972, i mercati online, i servizi cloud da impresa a impresa e i servizi cloud che consentono agli utenti di caricare contenuti per uso personale non sono prestatori di servizi di condivisione di contenuti online ai sensi della presente Direttiva*".

Parimenti, il Considerando 62 afferma che non si dovrebbero comprendere nell'ambito applicativo soggettivo dell'art. 17 tutti quei servizi che hanno uno scopo principale diverso da quello di consentire agli utenti di caricare e condividere una grande quantità di contenuti protetti dal diritto d'autore allo scopo di trarne profitto. Si tratta per esempio anche di quei *provider* che consentono agli utenti di caricare contenuti per uso personale, come i *cyberlocker*, o i mercati online la cui attività principale è la vendita al dettaglio, e che non danno accesso a contenuti protetti dal diritto d'autore.

[510] Per maggiori informazioni sul concetto di Online Content-Sharing Service Providers si veda: J. P. QUINTAIS, P. MEZEI, I. HARKAI, J. C. MAGALHÃES, C. KATZENBACH, S. F. SCHWEMER, & T. RIIS, *Final Report on mapping of EU legal framework and intermediaries' practices on copyright content moderation and removal*, 2022, cit., 52 e ss.

In merito ai *provider* da considerare esclusi dalla disciplina, le linee guida[511] della Commissione del 2021, emanate in forza del decimo paragrafo dell'art. 17 della Direttiva 2019/790, dispongono che tali esclusioni non sono esaustive. La Commissione infatti afferma che al fine di garantire la certezza del diritto, "*le leggi di attuazione degli Stati membri devono stabilire in modo esplicito e completo la definizione di "prestatore di servizi di condivisione di contenuti online" di cui all'articolo 2, paragrafo 6, primo comma, ed escludere esplicitamente i prestatori di servizi elencati all'articolo 2, paragrafo 6, secondo comma, specificando, alla luce del considerando 62, che tale elenco di prestatori di servizi esclusi non è esaustivo. Gli Stati membri non dispongono di alcun margine per "andare oltre", ossia ampliare o ridurre l'ambito di applicazione della definizione*".

Il legislatore italiano, recependo la Direttiva europea con D.lgs. 8 novembre 2021, n. 177, introduce un nuovo Titolo II-quater nella L.633/1941 il quale, all'art. 102-sexies, comma secondo, tratta delle esclusioni dall'ambito applicativo, senza tuttavia andare oltre quanto previsto in sede comunitaria[512].

Infine, il legislatore europeo stabilisce che, per garantire un elevato livello di protezione del diritto d'autore, l'art. 17 non dovrebbe applicarsi ai prestatori di servizi il cui scopo principale è quello di attuare o facilitare la pirateria in materia di diritto d'autore, così escludendo dalla nostra considerazione tutte quelle piattaforme, analizzate nel capitolo secondo, che consentono lo scambio di materiale protetto dal diritto d'autore.

Avendo dunque tracciato in negativo le ipotesi cui la disciplina in commento non può applicarsi, per disposizione legislativa espressa, diventa necessario analizzare in positivo i tratti qualificativi di un *provider*, capaci di rendere lo stesso un "*prestatore di servizi di condivisione di contenuti online*".

In particolare, un OCSSP, ai sensi dell'art. 2 punto 6, deve: (a) essere un servizio della società dell'informazione ai sensi dell'articolo 1, paragrafo 1, lettera b), della Direttiva (UE) 2015/1535[513]; (b) avere come scopo principale: (i) memorizzare e dare accesso al pubblico a (ii) grandi quantità di opere protette dal diritto d'autore o altri materiali protetti (iii) caricati dai suoi utenti, (iv) che il servizio organizza e promuove a scopo di lucro. Il legislatore

---

[511] Communication From The Commission To The European Parliament And The Council: *Guidance on Article 17 of Directive 2019/790 on Copyright in the Digital Single Market* COM/2021/288 final, liberamente accessibili presso: «https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52021DC0288&from=EN» (Ultimo accesso: 10 maggio 2022).

[512] L'art 102-sexies della L. 633/1941 oggi dispone, al comma secondo, che "*Non sono considerati prestatori di servizi di condivisione di contenuti online ai sensi del presente Titolo quelli che danno accesso alle enciclopedie online senza scopo di lucro, ai repertori didattici o scientifici senza scopo di lucro, nonché le piattaforme di sviluppo e di condivisione di software open source, i fornitori di servizi di comunicazione elettronica, i prestatori di mercati online, di servizi cloud da impresa a impresa e di servizi cloud che consentono agli utenti di caricare contenuti per uso personale, salvo che il mercato online o il servizio cloud consenta di condividere opere protette dal diritto d'autore tra più utenti*". Per maggiori informazioni ed un commentario critico si faccia riferimento a D. DE ANGELIS, F. LEVA, *The Italian transposition of the CDSM Directive: A missed opportunity?*, in *Communia*, April 28, 2021, liberamente accessibile presso: «https://www.communia-association.org/2021/04/28/the-italian-transposition-of-cdsm-a-missed-chance/» (Ultimo accesso: 10 maggio 2022).

[513] L'articolo 1, paragrafo 1, lettera b), della Direttiva (UE) 2015/1535 dispone in particolare che per tale definizione si intende: "*qualsiasi servizio della società dell'informazione, vale a dire qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi.*
Ai fini della presente definizione si intende per:
i) «a distanza»: un servizio fornito senza la presenza simultanea delle parti;
ii) «per via elettronica»: un servizio inviato all'origine e ricevuto a destinazione mediante attrezzature elettroniche di trattamento (compresa la compressione digitale) e di memorizzazione di dati, e che è interamente trasmesso, inoltrato e ricevuto mediante fili, radio, mezzi ottici o altri mezzi elettromagnetici;
iii) «a richiesta individuale di un destinatario di servizi»: un servizio fornito mediante trasmissione di dati su richiesta individuale".

italiano, all'art. 102-sexies co.1, traduce tali requisiti chiedendo che un simile *provider* abbia cumulativamente: (a) come scopo principale, o tra i principali scopi, di memorizzare e dare accesso al pubblico a grandi quantità di opere o di altri materiali protetti dal diritto d'autore; (b) le opere o gli altri materiali protetti sono caricati dai suoi utenti; (c) le opere o gli altri materiali protetti sono organizzati e promossi allo scopo di trarne profitto direttamente o indirettamente.

Per "scopo principale" dovrebbe intendersi, in accordo alle linee guida della Commissione, la funzione o il ruolo principale o predominante del prestatore di servizi[514]. Ad esempio, in negativo, come indicato al Considerando 63, i mercati online possono dare accesso a una grande quantità di opere protette dal diritto d'autore, pur se questa non costituisce la loro attività principale, che è invece la vendita al dettaglio online, conseguentemente escludendo la portata della disciplina. La valutazione riguardante lo "*scopo principale o uno dei principali scopi*" dovrebbe essere neutrale sotto il profilo tecnologico e del modello di business, in quanto, ad avviso della Commissione, dovrebbe essere sufficientemente ampia per poter rispondere alle esigenze future.

In secondo luogo, è richiesto il requisito della memorizzazione e dell'accesso del pubblico ai contenuti, il quale non pone problemi interpretativi oltre alla specificazione per cui la memorizzazione non dovrebbe essere intesa in senso meramente temporaneo.

In terzo luogo, poi, la Direttiva fa riferimento alla "grande quantità" di opere protette dal diritto d'autore. Chiaramente, il concetto è di per sé vago, probabilmente è volutamente tale: la Direttiva non quantifica in alcun modo tale requisito. Gli Stati membri dovrebbero astenersi dal dare notazioni in termini quantitativi nei rispettivi ordinamenti nazionali al fine, nota la Commissione, di evitare la frammentazione giuridica che potrebbe derivare dalla previsione di ambiti di applicazione diversi per i *provider* nei vari Stati membri. Tale interpretazione è confortata anche dal Considerando 63 il quale dispone che l'accertamento relativo al fatto che un prestatore di servizi di condivisione di contenuti online memorizzi e dia accesso a una grande quantità di contenuti protetti dal diritto d'autore "*dovrebbe essere effettuata caso per caso e dovrebbe tener conto di una combinazione di elementi, come l'utenza del servizio e il numero di file […] caricati dagli utilizzatori del servizio*".

L'ultimo requisito è lo "scopo di lucro". Per esso si dovrebbe identificare, in accordo al Considerando 62, il profitto derivante dai contenuti caricati che potrebbe essere realizzato "*direttamente o indirettamente, organizzandoli e promuovendoli per attirare un pubblico più vasto, anche classificandoli e ricorrendo a promozioni mirate al loro interno*". Le linee guida della Commissione specificano che lo scopo di lucro non dovrebbe essere presunto in base al mero fatto che il servizio si configura come un operatore economico o come un soggetto di diritto avente natura commerciale. La finalità lucrativa dovrebbe invece essere collegata ai profitti derivanti dall'organizzazione e dalla promozione dei contenuti caricati dagli utenti, ad esempio per il tramite di annunci pubblicitari inseriti sulla piattaforma[515].

Ove, quindi, un *provider* rispetti tutti i punti fin qui tracciati si potrà qualificare come un "*prestatore di servizi di condivisione di contenuti online*", sicuro dunque dell'applicabilità soggettiva delle disposizioni dell'art. 17.

---

514 Communication From The Commission To The European Parliament And The Council: *Guidance on Article 17 of Directive 2019/790 on Copyright in the Digital Single Market* COM/2021/288 final, cit.

515 Communication From The Commission To The European Parliament And The Council: *Guidance on Article 17 of Directive 2019/790 on Copyright in the Digital Single Market* COM/2021/288 final, cit.

Chiaramente, a questo punto, ove non si integrasse anche uno solo dei canoni condizionali richiesti dalla Direttiva e dal legislatore nazionale, il nuovo regime di responsabilità di cui all'art. 17 paragrafo quarto non potrà valere. Di conseguenza, il regime ordinario di cui alla Direttiva e-commerce, già introdotto al capitolo secondo, troverà applicazione in tutti quei casi in cui un *provider* sia "*mere conduit", "caching"* o *"hosting*" passivo. Ove invece si esuli anche da quest'ultima disciplina, in Italia troveranno applicazione le normali regole di responsabilità extracontrattuale o quelle settorialmente applicabili[516].

In questo senso si deve infatti notare come l'art. 17 si pone quale *lex specialis* rispetto ai regimi di responsabilità già delineati dalla Direttiva e-commerce. Oltre alla dottrina,[517] anche le linee guida della Commissione dispongono in tal senso, affermando che, ai sensi dell'articolo 17, paragrafi 1 e 2, quando i prestatori di servizi di condivisione di contenuti online forniscono l'accesso a contenuti protetti dal diritto d'autore caricati dai propri utenti, effettuano un atto di "comunicazione al pubblico", come vedremo nel paragrafo successivo, e tuttavia la limitazione di responsabilità di cui all'articolo 14, paragrafo 1, della Direttiva 2000/31/CE non trova applicazione[518].

L'articolo 17 rappresenta dunque una *lex specialis* rispetto all'articolo 3 della Direttiva 2001/29/CE e all'articolo 14 della Direttiva 2000/31/CE, disciplinando in modo completo e specifico l'atto di "comunicazione al pubblico" nelle limitate circostanze contemplate da tale disposizione ai fini della Direttiva. Ciò è confermato dai Considerando 64 e 65. Il Considerando 65, in particolare, stabilisce che ove i prestatori di servizi di condivisione di contenuti online dovessero essere responsabili di atti di comunicazione al pubblico o di messa a disposizione del pubblico, l'articolo 14, paragrafo 1, della Direttiva 2000/31/CE non dovrebbe applicarsi. Tuttavia, a conferma della specialità della disposizione di cui all'art. 17, ove invece non potesse trovare applicazione quest'ultimo, tornerebbe applicabile la disciplina ordinaria. In questo senso, infatti, il Considerando 65 afferma che, quanto sin ora detto, "*non dovrebbe pregiudicare l'applicazione dell'articolo 14, paragrafo 1, della Direttiva 2000/31/CE a tali prestatori di servizi per scopi che non rientrano nell'ambito di applicazione della presente Direttiva.*" In considerazione di ciò, l'art. 17 paragrafo terzo oggi dispone la normativa speciale per gli OCSSP che non pregiudica la possibile applicazione dell'articolo 14, paragrafo 1, della Direttiva 2000/31/CE a tali prestatori di servizi per finalità che non rientrano nell'ambito di applicazione della Direttiva.

Alcuni recenti contributi in dottrina confermano la specialità della disciplina, affermando che l'OCSSP è direttamente responsabile nelle ipotesi previste dall'articolo in

---

516 Per un'analisi maggiormente approfondita in merito si veda L. CAMARELLA, *La responsabilità dell'Internet Service Provider alla luce della nuova Direttiva sul diritto d'autore nel mercato unico digitale*, in *Trento Law and Technology Research Group,* Student Paper n. 58, liberamente accessibile presso: «https://iris.unitn.it/retrieve/handle/11572/255244/311950/Trento%20LawTech%20-%20Laura%20Camarella_58.pdf» (Ultimo accesso: 10 maggio 2022). In merito si faccia altresì riferimento a L. ALBERTINI *La modifica al diritto d'autore europeo per tener conto del contesto digitale: note sugli artt. 11 (diritto degli editori) e 13 (responsabilità dei provider) della bozza di Direttiva UE nel febbraio 2019, uscita dalla fase c.d. trilogue*, cit.

517 In tal senso si esprime anche A. LA ROSA, *La nuova Direttiva "Copyright" (n. 2019/790): focus su art. 17*, in *4cLegal*, 11 gennaio 2021, liberamente accessibile presso: «https://www.4clegal.com/opinioni/nuova-Direttiva-*copyright*-n-7902019-focus-art-17» (Ultimo accesso: 10 maggio 2022).

518 Come affrontato nel capitolo secondo, Infine, l'attività di "hosting" è definita dagli artt. 14 della Direttiva e 16 del decreto italiano come quella attività di memorizzazione di informazioni fornite da un utente o destinatario del servizio. Il *provider* in questi casi non è ritenuto responsabile ove a) non sia effettivamente al corrente del fatto che l'attività o l'informazione è illecita e, per quanto attiene ad azioni risarcitorie, non sia al corrente di fatti o di circostanze che rendono manifesta l'illegalità dell'attività o dell'informazione, o b) non appena al corrente di tali fatti, agisca immediatamente per rimuovere le informazioni o per disabilitarne l'accesso.

commento, senza la possibilità di beneficiare dell'esenzione dalla responsabilità per i fornitori di servizi di hosting come invece prevista nella direttiva sul commercio elettronico. Per gli atti delle stesse piattaforme online che non rientrino nell'ambito di applicazione degli artt. 17, commi 1 e 2 – in particolare l'hosting di contenuti illegali che non costituiscano violazione del diritto d'autore – l'art. 14 Direttiva sul commercio elettronico resta applicabile. La logica conclusione di tale regime, quindi, è che l'art. 17 non è solo *lex specialis* dell'art. 3 Direttiva 2001/29/CE, ma anche all'art. 14 Direttiva sul commercio elettronico, come ribadito.[519]

3. Ambito oggettivo di applicazione: la nozione di comunicazione al pubblico

Una volta stabilito l'ambito di applicazione soggettivo della Direttiva 2019/790, avendo chiarito il concetto di "*prestatori di servizi di condivisione di contenuti online*", diventa necessario investigare l'ambito oggettivo di applicazione, ossia quale attività posta in essere da tali *provider* comporti l'estrinsecarsi dell'art. 17.

I concetti che vengono in riferimento sono quelli di "*comunicazione al pubblico*" e "*messa a disposizione del pubblico*". L'art. 17 paragrafo 1 in particolare afferma che "*il prestatore di servizi di condivisione di contenuti online effettua un atto di comunicazione al pubblico o un atto di messa a disposizione del pubblico ai fini della presente Direttiva quando concede l'accesso al pubblico a opere protette dal diritto d'autore o altri materiali protetti caricati dai suoi utenti*". Tale disposizione viene ribadita anche dal Considerando 64 il quale tuttavia non chiarifica la disposizione, riproponendone, *verbatim*, il fraseggio.

Come abbiamo già avuto modo di notare, il diritto di comunicazione al pubblico è fattispecie nota al diritto europeo sin dalla Direttiva 2001/29, a norma del cui articolo 3, gli Stati membri riconoscono agli autori il "*diritto esclusivo di autorizzare o vietare qualsiasi comunicazione al pubblico, su filo o senza filo, delle loro opere, compresa la messa a disposizione del pubblico delle loro opere in maniera tale che ciascuno possa avervi accesso dal luogo e nel momento scelti individualmente*". Il secondo paragrafo, a sua volta, determina il "*diritto di messa a disposizione del pubblico*".

Tale norma è sicuramente debitrice dei Trattati WIPO del 1996, in particolare del WCT e del suo art. 8. Secondo la giurisprudenza consolidata della Corte di Giustizia[520] la nozione di comunicazione al pubblico consta di due elementi necessari: a) un atto di comunicazione di un'opera e b) la comunicazione di quest'ultima a un pubblico. Senza voler entrare tuttavia

[519] Per maggiori informazioni sul concetto di Online Content-Sharing Service Providers si veda: J. P. QUINTAIS, P. MEZEI, I. HARKAI, J. C. MAGALHÃES, C. KATZENBACH, S. F. SCHWEMER, & T. RIIS, *Final Report on mapping of EU legal framework and intermediaries' practices on copyright content moderation and removal*, 2022, cit., 55-56.

[520] In riferimento si vedano: CGUE 7 dicembre 2006, causa C-306/05, *Sociedad General de Autores y Editores de España (SGAE)*, liberamente accessibile presso: «https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A62005CJ0306&qid=1645712058879» (Ultimo accesso: 10 maggio 2022); CGUE 7 marzo 2013, causa C-607/11, *ITV Broadcasting*, liberamente accessibile presso: «https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX%3A62011CJ0607» (Ultimo accesso: 10 maggio 2022); CGUE 14 giugno 2017, C-610/15, *Stichting Brein contro Ziggo BV*, liberamente accessibile presso «https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX%3A62015CJ0610» (Ultimo accesso: 10 maggio 2022).

nelle tematiche relative al complesso diritto di comunicazione al pubblico[521], si procede meramente a segnalare alcune pronunce giurisprudenziali al fine di chiarificarne i contorni[522].

Il primo caso degno di nota in tema di comunicazione al pubblico è sicuramente dato dalla sentenza Svensson et al c. Retriever Sverige AB[523]. La domanda di pronuncia pregiudiziale verteva sull'interpretazione dell'articolo 3, paragrafo 1, della Direttiva 2001/29/CE ed era stata presentata nell'ambito di una controversia avviata dai sigg. Svensson e Sjögren, nonché dalle sig.re Sahlman e Gadd, nei confronti della società Retriever Sverige AB ai fini del risarcimento del preteso danno da essi subito per effetto dell'inserimento, sul sito Internet di tale società, di collegamenti cliccabili che rinviavano ad articoli di cui i medesimi affermavano di essere titolari del relativo diritto d'autore, pubblicati su Internet.

La Corte notava nel caso di specie che l'art. 3, paragrafo 1, della Direttiva 2001/29 prevedeva che qualsiasi comunicazione di un'opera al pubblico dovesse essere autorizzata dal titolare del diritto d'autore. Ne risultava quindi che la nozione di comunicazione al pubblico constava di due elementi cumulativi, vale a dire "*un atto di comunicazione*" di un'opera e la comunicazione di quest'ultima a un "*pubblico*"[524].

---

[521] Tanto che secondo alcuni autori la natura di questo diritto e del suo richiamo all'articolo 17 non sono chiare. In merito si segnalano i seguenti contributi: B. HANUZ, *Direct Copyright Liability As Regulation Of Hosting Platforms For The CopyrightInfringing Content Uploaded By Their Users: Quo Vadis ?*, 11(3) *Journal of Intellectual Property, Information Technology and E-Commerce Law* (2020), 315-339, liberamente accessibile presso: «https://www.jipitec.eu/issues/jipitec-11-3-2020/5186» (Ultimo accesso: 10 maggio 2022); M. HUSOVEC, J. P. QUINTAIS, *How to License Article 17? Exploring the Implementation Options for the New EU Rules on ContentSharing Platforms*, liberamente accessibile presso: «https://ssrn.com/abstract=3463011» (Ultimo accesso: 10 maggio 2022) o «http://dx.doi.org/10.2139/ssrn.3463011» (Ultimo accesso: 10 maggio 2022) (2019), 1-27, 5-10; J.B. NORDEMANN, J. WAIBLINGER, *Art. 17 DSMCD: a class of its own? How to implement Art. 17 into the existing national copyright acts, including a comment on the recent German Discussion Draft – Part 1*, in *Kluwer Copyright Blog*, 2020, liberamente accessibile presso: «http://copyrightblog.kluweriplaw.com/2020/07/16/art.-17-dsmcd-a-class-of-its-ownhow-to-implement-art.-17-into-the-existing-national-copyright-acts-including-acomment-on-the-recent-german-discussion-draft-part1/?doing_wp_cron=1597142146.3135290145874023437500». (Ultimo accesso: 10 maggio 2022); J.B. NORDEMANN, J. WAIBLINGER, *Art. 17 DSMCD: a class of its own? How to implement Art. 17 into the existing national copyright acts, including a comment on the recent German Discussion Draft – Part 2*, in *Kluwer Copyright Blog*, 2020, liberamente accessibile presso: «http://copyrightblog.kluweriplaw.com/2020/07/17/art.-17-dsmcd-a-class-of-its-ownhow-to-implement-art.-17-into-the-existing-national-copyright-acts-including-acomment-on-the-recent-german-discussion-draft-part2/?doing_wp_cron=1597144877.2035028934478759765625». (Ultimo accesso: 10 maggio 2022).

[522] Per maggiori informazioni si veda in merito: J. P. QUINTAIS, P. MEZEI, I. HARKAI, J. C. MAGALHÃES, C. KATZENBACH, S. F. SCHWEMER, & T. RIIS, *Final Report on mapping of EU legal framework and intermediaries' practices on copyright content moderation and removal*, 2022, 44 e ss, in *Zenodo*, liberamente accessibile presso: «https://doi.org/10.5281/zenodo.6461568» (Ultimo accesso: 10 maggio 2022)

[523]CGUE 13 febbraio 2014, C-466/12, *Svensson et al c. Retriever Sverige AB*, liberamente consultabile presso: «https://curia.europa.eu/juris/document/document.jsf?text=&docid=147847&pageIndex=0&doclang=it&mode=lst&dir=&occ=first&part=1&cid=327328» (Ultimo accesso: 10 maggio 2022); per notazioni dottrinali in merito si veda: F. GIANNI, G. ORIGONI, E. GRIPPO, *Linking e diritto d'autore - La sentenza Svensson e altri contro Retriever Sverige AB della Corte di Giustizia dell'Unione Europea sul linking ad opere dell'ingegno messe a disposizione su Internet*, in www.gop.it (Proprietà intellettuale, IT e Media), marzo 2014, liberamente accessibile presso «https://www.gop.it/doc_pubblicazioni/367_jswrs4qohr_cn.pdf» (Ultimo accesso: 10 maggio 2022); L. CAMARELLA *La responsabilità dell'Internet Service Provider alla luce della nuova Direttiva sul diritto d'autore nel mercato unico digitale*, *in Trento Law and Technology Research Group*, Student Paper n. 58, liberamente accessibile presso: «https://iris.unitn.it/retrieve/handle/11572/255244/311950/Trento%20LawTech%20-%20Laura%20Camarella_58.pdf» (Ultimo accesso: 10 maggio 2022).

[524] La Corte in questo ricorda il proprio precedente: CGUE 7 marzo 2013, causa C-607/11, *ITV Broadcasting*, liberamente accessibile presso: «https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX%3A62011CJ0607» (Ultimo accesso: 10 maggio 2022).

La Corte di Giustizia notava che, per quanto riguarda il primo di tali elementi, ossia l'esistenza di un "atto di comunicazione", tale nozione dovesse essere intesa "in senso ampio" e ciò allo scopo di garantire un elevato livello di protezione ai titolari del diritto d'autore. Con riferimento alla fattispecie concreta, secondo la Corte, il fatto di mettere a disposizione su un sito Internet dei collegamenti cliccabili verso opere protette costituiva un "atto di comunicazione".

Per quanto riguarda il secondo degli elementi summenzionati, ossia che l'opera protetta deve essere effettivamente comunicata ad un "pubblico", l'art. 3, paragrafo 1, della Direttiva 2001/29 si voleva riferire ad un numero indeterminato di destinatari potenziali e comprendere, peraltro, un numero di persone piuttosto considerevole. Su questo punto la Corte notava che il pubblico cui gli articoli dei ricorrenti erano diretti, con la prima comunicazione, era costituito dal complesso dei potenziali visitatori del sito considerato. Infatti, l'accesso alle opere su tale sito non era assoggettato ad alcuna misura restrittiva, quindi tutti gli internauti potevano avere liberamente accesso ad esse.

Di conseguenza, ad avviso della Corte, dato che gli utenti della società Retriever Sverige AB avrebbero astrattamente potuto essere anche destinatari della comunicazione al pubblico originaria, ossia degli articoli dei ricorrenti, essendo questi liberamente accessibili sulla rete, veniva meno il requisito della presenza di un pubblico diverso da quello originario. Per queste ragioni, la Corte afferma un importante principio di diritto tale per cui, ove gli utenti di un determinato sito Internet cui siano state comunicate opere protette dal diritto d'autore possano anche direttamente accedere a tali opere sul sito sul quale erano state inizialmente comunicate, tali utenti dovrebbero essere ricompresi nel "pubblico" previsto dai titolari del diritto d'autore al momento in cui hanno autorizzato l'originaria comunicazione delle loro opere. In tal senso allora, in mancanza di un pubblico nuovo, l'autorizzazione dei titolari del diritto d'autore non era necessaria per una comunicazione al pubblico come quella di cui al procedimento principale.

Simili principi vennero confermati anche dalla successiva giurisprudenza sul punto, ed in particolare dal caso "BestWater International GmbH contro Michael Mebes e Stefan Potsch"[525]. Maggiormente interessante tuttavia si dimostra il successivo caso GS Media[526] che vedeva contrapposte da un lato la GS Media BV e, dall'altro, la Sanoma Media Netherlands BV, la Playboy Enterprises International Inc. e la sig.ra Britt Geertruida Dekker, in merito, in particolare, alla messa a disposizione sul sito GeenStijl.nl, gestito dalla GS Media, di collegamenti ipertestuali verso altri siti per la consultazione di fotografie rappresentanti la sig.ra Dekker, realizzate per la rivista Playboy.

Senza voler addentrarsi sulle complesse vicende fattuali, quello che interessa è il ragionamento della Corte in merito al concetto di comunicazione al pubblico. In particolare, la Corte distingue, ai fini del concetto di comunicazione al pubblico, le ipotesi in cui tali atti vengano compiuti per scopo di lucro o meno. Se un collegamento è determinato senza scopo di lucro e senza che vi sia una conoscenza, o una ragionevole presunzione di conoscenza della possibile violazione realizzata, tale comunicazione non sarebbe di per sé illecita. Viceversa, secondo la Corte, ove i collegamenti ipertestuali abbiano scopo lucrativo, si deve

[525] Ordinanza della CGUE 21 ottobre 2014, C- 348/13, *BestWater International GmbH contro Michael Mebes e Stefan Potsch*, liberamente consultabile presso: «https://eur-lex.europa.eu/legal-content/it/TXT/?uri=CELEX:62013CO0348» (Ultimo accesso: 10 maggio 2022).

[526] CGUE 8 settembre 2016, C-160/15, *GS Media BV contro Sanoma Media Netherlands BV, Playboy Enterprises International Inc., Britt Geertruida Dekker*, liberamente accessibile presso: «https://curia.europa.eu/juris/document/document.jsf?docid=183124&doclang=IT». (Ultimo accesso: 10 maggio 2022)

altresì presumere la conoscenza della violazione, così ritenendosi più probabilmente integrati i requisiti del *copyright infringement*.

Come ricorda un recente contributo allora, in seguito alle elaborazioni giurisprudenziali in materia di comunicazione al pubblico, la situazione che si presenta è la seguente: "*in primo luogo, il diritto in commento deve essere interpretato in senso ampio. In secondo luogo, la "comunicazione al pubblico" è un concetto autonomo del diritto dell'UE. In terzo luogo, la comunicazione al pubblico implica diversi tipi di attività sia offline che online. In ambito on line, la Corte ha confermato che il diritto esclusivo si applica a una miriade di usi: il "live streaming" o la diffusione da parte di terzi su Internet di segnali provenienti da emittenti televisive commerciali (ITV Broadcasting); la fornitura di "link cliccabili" che danno accesso alle opere protette (Svensson); la fornitura di collegamenti di framing alle opere protette (BestWater); la trasmissione diretta di una partita sportiva su un sito Internet (C More Entertainment); la pubblicazione di collegamenti ipertestuali ad opere su siti web di terzi senza il consenso del titolare del diritto (GS Media); la vendita di lettori multimediali con add-on preinstallati che contengono collegamenti ipertestuali a siti web che mettono a disposizione del pubblico opere senza il consenso degli aventi diritto (Filmspeler); la fornitura di una piattaforma online peer-to-peer (P2P) che consente la condivisione di file protetti senza il consenso dei titolari dei diritti (Ziggo); l'incorporamento, mediante la tecnica del framing, in una pagina di un sito web di terzi, di contenuti protetti liberamente accessibili in un altro sito web, laddove tale inclusione eluda le misure tecniche di protezione (VG Bild Kunst); e il caricamento da parte degli utenti di una rete P2P di file multimediali contenenti un'opera protetta (Mircom)".*[527]

La Corte di Giustizia ha poi in proposito recentemente chiarito che il gestore di una piattaforma di condivisione di video sulla quale gli utenti possono mettere illecitamente a disposizione del pubblico contenuti protetti, tendenzialmente non effettua una comunicazione al pubblico di detti contenuti salvo che esso contribuisca, al di là della semplice messa a disposizione della piattaforma, a dare al pubblico accesso a siffatti contenuti in violazione del diritto d'autore. Ciò si verifica, in particolare, qualora tale gestore sia concretamente al corrente della messa a disposizione illecita di un contenuto protetto sulla sua piattaforma e si astenga dal rimuoverlo o dal disabilitare immediatamente l'accesso ad esso, o nel caso in cui detto gestore si astenga dal mettere in atto le opportune misure tecniche che ci si può attendere da un operatore normalmente diligente nella sua posizione per contrastare in modo credibile ed efficace violazioni del diritto d'autore su tale piattaforma. Le stesse conclusioni varrebbero, a detta della Corte, nel caso in cui il provider partecipi alla selezione di contenuti protetti comunicati illecitamente al pubblico o fornisca sulla propria piattaforma strumenti specificamente destinati alla condivisione illecita od ancora promuova scientemente condivisioni del genere[528].

---

[527] Libera traduzione tratta da J. P. QUINTAIS, P. MEZEI, I. HARKAI, J. C. MAGALHÃES, C. KATZENBACH, S. F. SCHWEMER, & T. RIIS, *Final Report on mapping of EU legal framework and intermediaries' practices on copyright content moderation and removal*, 2022, cit., 44 e ss. Si riporta di seguito il testo originale citato: "*First, the right must be interpreted broadly.152 Second, "communication to the public" is an autonomous concept of EU law. Third, communication to the public involves different types of activities both offline and online. In the online context, the Court has confirmed that the exclusive right applies to myriad uses: the "live str eaming" or broadcasting by a third party over the Internet of signals from commercial television broadcasters (ITV Broadcasting); the provision of "clickable links" giving access to protected works (Svensson); the provision of framing links to protected works (BestWater); the direct broadcast of a sporting fixture on an Internet site (C More Entertainment); the posting of hyperlinks to works on third party websites without the right holder's consent (GS Media); the sale of multi-media players with pre- installed add-ons that contain hyperlinks to websites making available works to the public without the consent of the right holders (Filmspeler); the provision of an online peer-to-peer (p2p) platform that enables the sharing of protected files without the consent of right holders (Ziggo); the embedding, by means of the technique of framing, in a third-party website page, of freely accessible protected content on another website, where that embedding circumvents technical protection measures (VG Bild Kunst); and the uploading by users of a p2p networks of media files containing a protected work (Mircom)."*

[528] CGUE 26 aprile 2022, C-401/2019, Repubblica di Polonia contro Parlamento europeo, Consiglio dell'Unione europea, liberamente accessibile presso:

Così dunque delineati gli elementi essenziali che determinano il significato del diritto di "comunicazione al pubblico", è ora possibile affermare che, ove si ponga in essere un atto definibile in tali termini, si potrà ritenere integrato il requisito oggettivo di applicabilità dell'articolo 17, paragrafo primo, della Direttiva 2019/790, in alternativa, torneranno applicabili le regole ordinarie, in particolare disposte dall'articolo 3 della Direttiva 2001/29/CE e dall'articolo 14 della Direttiva 2000/31/CE.

Pertanto, come precisato dal secondo comma di tale paragrafo, tali prestatori devono, in linea di principio, ottenere un'autorizzazione dei titolari dei diritti, ad esempio mediante la conclusione di un accordo di licenza, per l'utilizzo, sui loro servizi, di contenuti protetti messi in rete dagli utenti.[529] Tale obbligo è direttamente connesso all'obiettivo generale perseguito all'articolo 17 della Direttiva 2019/790, ossia "*garantire il buon funzionamento e l'equità del mercato per il diritto d'autore*"[530].

4. Il sistema delle autorizzazioni

La prima disposizione degna di nota è contenuta nei paragrafi primo e secondo dell'art. 17 e riguarda il meccanismo delle autorizzazioni che gli OCSSP dovrebbero ottenere per lecitamente procedere nella loro attività di comunicazione al pubblico.

Il Considerando 61 nota, infatti, come negli ultimi anni il funzionamento del mercato dei contenuti online si è fatto sempre più complesso. I servizi di condivisione di contenuti online sono diventati una delle principali fonti di accesso a prodotti tutelati dal diritto d'autore, al contempo fornendo un canale di fruizione alle opere culturali e creative garantendo alle stesse opportunità di sviluppare nuovi modelli di business. Tuttavia, pur

---

«https://curia.europa.eu/juris/document/document.jsf?text=&docid=258261&pageIndex=0&doclang=IT&mode=req&dir=&occ=first&part=1&cid=10742191». (Ultimo accesso: 10 maggio 2022), par. 27. La Corte in tal caso richiama espressamente la sentenza CGUE 22 giugno 2021, C-682/18 e C-683/18, *YouTube e Cyando*, par.102, liberamente accessibile presso: «https://curia.europa.eu/juris/document/document.jsf?text=&docid=243241&pageIndex=0&doclang=IT&mode=lst&dir=&occ=first&part=1&cid=170202» (Ultimo accesso: 10 maggio 2022)

[529] In questo senso si esprime anche l'Avvocato Generale Henrik Saugmandsgaard Øe, conclusioni presentate il 15 luglio 2021 nella Causa C-401/19, Repubblica di Polonia contro Parlamento europeo, Consiglio dell'Unione europea, ricorso presentato ex art. 263 TFUE, cit. liberamente accessibili presso: «https://curia.europa.eu/juris/document/document.jsf?text=&docid=244201&pageIndex=0&doclang=it&mode=lst&dir=&occ=first&part=1&cid=130522» (Ultimo accesso: 10 maggio 2022).

[530] Così, infatti, si esprime il terzo considerando della Direttiva 2019/790 ove afferma che: "*I rapidi sviluppi tecnologici continuano a trasformare il modo in cui le opere e altri materiali sono creati, prodotti, distribuiti e sfruttati, mentre emergono costantemente nuovi modelli di business e nuovi attori. È necessario che la legislazione in materia sia adeguata alle esigenze future, in modo da non limitare l'evoluzione tecnologica. Gli obiettivi e i principi stabiliti dal quadro giuridico dell'Unione sul diritto d'autore rimangono validi. Tuttavia, vi è ancora incertezza giuridica quanto a taluni utilizzi, anche transfrontalieri, delle opere e altri materiali in ambiente digitale, sia per i titolari dei diritti che per gli utilizzatori. In alcuni settori, come indicato nella comunicazione della Commissione del 9 dicembre 2015, dal titolo «Verso un quadro normativo moderno e più europeo sul diritto d'autore», è necessario adeguare e completare l'attuale quadro dell'Unione sul diritto d'autore salvaguardando un elevato livello di protezione del diritto d'autore e dei diritti connessi. La presente direttiva prevede norme miranti ad adeguare talune eccezioni e limitazioni al diritto d'autore e diritti connessi all'ambiente digitale e al contesto transfrontaliero, nonché misure volte a facilitare determinate procedure di concessione delle licenze, in particolare, ma non solo, per la divulgazione di opere fuori commercio e di altri materiali e la disponibilità online di opere audiovisive su piattaforme di video su richiesta, al fine di garantire un più ampio accesso ai contenuti. Essa contiene anche disposizioni volte a rendere più agevole l'utilizzo dei contenuti di pubblico dominio. Per garantire il buon funzionamento e l'equità del mercato per il diritto d'autore sono altresì opportune norme relative ai diritti sulle pubblicazioni, all'uso di opere o altri materiali da parte dei prestatori di servizi online che memorizzano contenuti caricati dagli utenti e vi danno accesso, alla trasparenza dei contratti per autori e artisti (interpreti o esecutori), alla remunerazione di autori e artisti (interpreti o esecutori), nonché a un meccanismo per la revoca dei diritti che autori e artisti (interpreti o esecutori) hanno trasferito in esclusiva.*"

consentendo la varietà e l'accessibilità dei contenuti, simili piattaforme creano anche problemi quando vengono caricati contenuti protetti dal diritto d'autore senza il previo consenso dei titolari dei diritti. Dato che un simile sistema di accesso incide sulla capacità dei titolari dei diritti di stabilire se, e a quali condizioni, le loro opere e altri materiali siano utilizzati, nonché sulla loro capacità di ottenere un'adeguata remunerazione per detto utilizzo, il legislatore europeo ritiene importante promuovere lo sviluppo del mercato della concessione delle licenze tra i titolari di diritti e i prestatori di servizi di condivisione di contenuti online. Tali accordi, secondo quanto disposto dal Considerando 61, dovrebbero essere equi e mantenere un equilibrio ragionevole tra entrambe le parti. I titolari dei diritti dovrebbero ricevere un compenso adeguato per l'utilizzo delle loro opere. Allo stesso tempo, in ogni caso, poiché tali disposizioni non dovrebbero incidere sulla libertà contrattuale, i titolari dei diritti non dovrebbero essere obbligati a rilasciare un'autorizzazione o a concludere accordi di licenza con le piattaforme di cui trattiamo.

In considerazione di quanto affermato quindi, l'art. 17 dispone che un prestatore di servizi di condivisione di contenuti online deve ottenere un'autorizzazione dai titolari dei diritti di cui all'articolo 3, paragrafi 1 e 2, della Direttiva 2001/29/CE, ad esempio mediante la conclusione di un accordo di licenza, al fine di comunicare al pubblico o rendere disponibili al pubblico opere o altri materiali. In aggiunta, il paragrafo secondo dispone che qualora un prestatore di servizi di condivisione di contenuti online ottenga un'autorizzazione, tale autorizzazione includa anche gli atti compiuti dagli utenti dei servizi che rientrano nell'ambito di applicazione dell'articolo 3 della Direttiva 2001/29/CE qualora non agiscano su base commerciale o qualora la loro attività non generi ricavi significativi.

La motivazione dell'introduzione di questa disciplina sulle eque remunerazioni e sulle licenze è principalmente dovuta ad affrontare in sede legislativa il delicato problema del c.d. "*value gap*"[531], ossia la disparità di posizione fra i titolari dei diritti d'autore e le grandi piattaforme di accesso a contenuti online.

È stato fatto notare, infatti, che l'articolo 17 della Direttiva sul diritto d'autore affronta il concetto di "divario di valore", o "value gap", locuzione intesa a significare che le piattaforme di condivisione dei contenuti online ottengono un valore irragionevole consentendo ai propri utenti di mettere a disposizione contenuti protetti da diritto d'autore, senza garantire che i titolari dei diritti ricevano la loro quota del valore o della remunerazione da tale sfruttamento delle loro opere. Al fine di "colmare il divario" (*bridge the gap*), la Direttiva in commento cerca di garantire che i titolari dei diritti ricevano un'adeguata remunerazione per l'utilizzo delle loro opere online promuovendo un mercato delle licenze tra titolari dei diritti e fornitori di servizi di condivisione di contenuti che mantenga un ragionevole equilibrio tra le posizioni di interesse delle parti.[532]

Bridy nota in merito che l'articolo 17 della Direttiva ha lo scopo di affrontare questo divario di valore che consiste essenzialmente nella denuncia di lunga data dell'industria

---

[531] Notazioni dottrinali in merito sono rinvenibili principalmente presso A. BRIDY, *The Price of Closing the 'Value Gap': How the Music Industry Hacked EU Copyright Reform* (June 30, 2019), in *Vanderbilt Journal of Entertainment & Technology Law*, volume 22, 2020, 323-358, liberamente accessibile presso: «https://ssrn.com/abstract=3412249» (Ultimo accesso: 10 maggio 2022) o «http://dx.doi.org/10.2139/ssrn.3412249» (Ultimo accesso: 10 maggio 2022); C. ANGELOPOULOS, J.P. QUINTAIS, *Fixing Copyright Reform: How to Address Online Infringement and Bridge the Value Gap*, in *Kluwer Copyright Blog*, 2018, liberamente accessibile presso: «http://*copyright*blog.kluweriplaw.com/2018/08/30/fixing-*copyright*-reform-address-online-infringement-bridge-value-gap/» (Ultimo accesso: 10 maggio 2022).

[532] Per maggiori riferimenti in merito al value gap, secondo una prospettiva statunitense si veda: United States Copyright Office, *Section 512 of Title 17, A Report Of The Register Of Copyrights*, cit. 61 e ss.

musicale secondo cui *YouTube* sottocompensa i titolari dei diritti musicali per gli *stream* di video caricati dagli utenti che contengono contenuti coperti da *copyright* rivendicati. Come efficacemente ricorda l'autrice, il testo della Direttiva non menziona da nessuna parte *YouTube*, ma chiunque sia esperto nell'economia politica del diritto d'autore digitale sa che l'articolo 17 è stato concepito specificamente per far pagare *YouTube*[533].

Il "divario di valore", o *value gap*, è dunque, in sostanza, uno slogan che i gruppi commerciali dell'industria musicale hanno creato per vendere ai responsabili politici l'idea che i previ "*safe harbors*" del *copyright* non siano una valida scelta politica per Internet, ma una scappatoia legale che consente a *YouTube* di sfruttare ingiustamente il prezioso patrimonio intellettuale dell'industria musicale. In poche parole, si cerca, secondo l'autrice, di ridefinire l'ambito dei *safe harbor* esistenti nell'Unione Europea per escludere *YouTube* dalla loro protezione.

Si può quindi affermare che l'obiettivo dichiarato fosse quello di diminuire la differenza percepita fra il valore che i prestatori di servizi di condivisione online ricavano dalle opere e dai materiali protetti e i proventi che essi riversano ai titolari dei diritti. L'Avvocato Generale Henrik Saugmandsgaard Øe ha anche affermato che "*si deve ricordare che i servizi in questione, tipici del «Web 2.0» interattivo e di cui YouTube, Soundcloud o, ancora, Pinterest sono gli esempi più noti, consentono a chiunque di mettere in rete automaticamente, senza selezione preventiva da parte dei loro prestatori, i contenuti desiderati. I contenuti messi in rete dagli utenti di tali servizi – comunemente designati come «user-generated content» o «user-uploaded content» – possono successivamente essere consultati in streaming (diffusione in flusso continuo) a partire dai siti Internet o dalle applicazioni per dispositivi smart associati a detti servizi – consultazione che è agevolata dalle funzioni di indicizzazione, di ricerca e di raccomandazione ivi generalmente presenti –, e ciò il più delle volte gratuitamente –; i prestatori di questi stessi servizi si remunerano solitamente tramite la vendita di spazi pubblicitari. Una quantità gigantesca di contenuti viene dunque messa a disposizione del pubblico su Internet, inclusa una quota ingente di opere e di altri materiali protetti*[534]".

È per queste ragioni quindi che a partire dal 2015, i titolari dei diritti hanno fatto valere che, mentre tali servizi di condivisione online occupano, nella prassi, una posizione apicale nella distribuzione online di opere ed i loro prestatori ne ricavano introiti pubblicitari considerevoli, allo stesso tempo non retribuiscono in maniera equa detti titolari. "*I proventi che tali prestatori versano a questi stessi titolari sarebbero segnatamente insignificanti rispetto a quelli che i prestatori di servizi di streaming musicale – come Spotify – versano loro, benché questi due tipi di servizi siano spesso percepiti dai consumatori come fonti equivalenti di accesso a detti materiali. Ne risulterebbe parimenti una concorrenza sleale fra detti servizi*[535]*"*.

Il legislatore europeo ha allora deciso di affrontare la questione, anche spinto dall'attività lobbistica verificatasi sin dal 2015, proprio nel costruire un sistema complesso di autorizzazioni o licenze che possono essere divise in due categorie: (a) quelle necessarie per le comunicazioni della piattaforma e (b) quelle necessarie per le comunicazioni degli utenti.

---

[533] A. BRIDY, *The Price of Closing the 'Value Gap': How the Music Industry Hacked EU Copyright Reform,* cit., 332 e ss.
[534] Avvocato Generale Henrik Saugmandsgaard Øe, conclusioni presentate il 15 luglio 2021 nella Causa C-401/19, Repubblica di Polonia contro Parlamento europeo, Consiglio dell'Unione europea, ricorso presentato ex art. 263 TFUE, liberamente accessibili presso «https://curia.europa.eu/juris/document/document.jsf?text=&docid=244201&pageIndex=0&doclang=it&mode=lst&dir=&occ=first&part=1&cid=130522» (Ultimo accesso: 10 maggio 2022).
[535] Avvocato Generale Henrik Saugmandsgaard Øe, conclusioni presentate il 15 luglio 2021 nella Causa C-401/19, Repubblica di Polonia contro Parlamento europeo, Consiglio dell'Unione europea, ricorso presentato ex art. 263 TFUE, cit.

4.1. Le autorizzazioni dell'art. 17 §1

Il paragrafo primo dell'art. 17 dispone che un prestatore di servizi di condivisione di contenuti online deve pertanto ottenere un'autorizzazione dai titolari dei diritti di cui all'articolo 3, paragrafi 1 e 2, della Direttiva 2001/29/CE, ad esempio mediante la conclusione di un accordo di licenza, al fine di comunicare al pubblico o rendere disponibili al pubblico opere o altri materiali.

Le linee guida della Commissione in merito ricordano come il termine "*autorizzazione*" non venga in realtà definito nella Direttiva e suggeriscono che debba essere interpretato alla luce delle finalità della normativa. Sia l'articolo 17, paragrafo 1, sia il Considerando 64 sono infatti formulati in modo aperto e fanno riferimento alla necessità di ottenere un' "*autorizzazione… [anche attraverso] un accordo di licenza*". Gli Stati membri possono prevedere modelli diversi di autorizzazione al fine di "*promuovere lo sviluppo del mercato della concessione delle licenze*"[536]. Il legislatore italiano, in questo caso, afferma all'art. 102-sexies che gli OCSSP devono ottenere un'autorizzazione dai titolari dei diritti, anche mediante la conclusione di un accordo di licenza. Tale autorizzazione, per il legislatore nazionale, può essere ottenuta direttamente o tramite gli organismi di gestione collettiva e le entità di gestione indipendente di cui al decreto legislativo del 15 marzo 2017, n. 35, ossia il decreto di attuazione della Direttiva 2014/26/UE sulla gestione collettiva dei diritti d'autore e dei diritti connessi e sulla concessione di licenze multiterritoriali per i diritti su opere musicali. Infatti, come ricordano anche le linee guida della Commissione, qualora i titolari dei diritti abbiano incaricato un organismo di gestione collettiva di gestire i propri diritti, tale organismo può concludere accordi di licenza con prestatori di servizi di condivisione di contenuti online per il repertorio che rappresenta, in base alle norme stabilite nella Direttiva 2014/26/UE. La concessione di licenze collettive può pertanto agevolare l'ottenimento di autorizzazioni da un'ampia gamma di titolari di diritti[537].

La Commissione ricorda poi che gli Stati membri dovrebbero inoltre mantenere la possibilità per i titolari dei diritti di non concedere l'autorizzazione ai prestatori di servizi di condivisione di contenuti online, come indicato al Considerando 61, in base al quale, tali disposizioni non dovrebbero incidere sulla libertà contrattuale, di tal che i titolari dei diritti non dovrebbero essere obbligati a rilasciare un'autorizzazione o a concludere accordi di licenza.

Gli Stati membri sono inoltre incoraggiati dalle linee guida della Commissione a mantenere o definire meccanismi volontari per facilitare accordi tra i titolari dei diritti e i prestatori di servizi. Secondo la Commissione dovrebbero ad esempio essere presi in considerazione meccanismi volontari di mediazione al fine di sostenere le parti disposte a concludere un accordo ma che incontrano difficoltà nei negoziati. Il legislatore italiano, tuttavia, pare non aver prestato attenzione ad una simile raccomandazione, non avendo previsto alcunché nel suo articolato normativo.

---

536 In questo senso si esprime il Considerando 61 quando afferma che "*È quindi importante promuovere lo sviluppo del mercato della concessione delle licenze tra i titolari di diritti e i prestatori di servizi di condivisione di contenuti online. Tali accordi di licenza dovrebbero essere equi e mantenere un equilibrio ragionevole tra entrambe le parti. I titolari dei diritti dovrebbero ricevere un compenso adeguato per l'utilizzo delle loro opere o di altri materiali. Tuttavia, poiché tali disposizioni non dovrebbero incidere sulla libertà contrattuale, i titolari dei diritti non dovrebbero essere obbligati a rilasciare un'autorizzazione o a concludere accordi di licenza*".

537 Communication From The Commission To The European Parliament And The Council: Guidance on Article 17 of Directive 2019/790 on Copyright in the Digital Single Market COM/2021/288 final, cit.

4.2. Le autorizzazioni dell'art. 17 §2

Maggiormente interessante si dimostra invece il paragrafo secondo dell'art. 17 il quale afferma che, qualora un prestatore di servizi di condivisione di contenuti online ottenga un'autorizzazione, tale autorizzazione debba includere anche gli atti compiuti dagli utenti dei servizi che rientrano nell'ambito di applicazione dell'articolo 3 della Direttiva 2001/29/CE qualora non agiscano su base commerciale o qualora la loro attività non generi ricavi significativi. Il legislatore nazionale non aiuta nell'interpretazione del disposto normativo comunitario, avendo trasposto pressoché *verbatim* quanto previsto in sede europea. Le linee guida della Commissione, tuttavia, ancora una volta, riescono ad esplicare il dettato normativo.

In particolare, l'art. 17 paragrafo secondo richiede che un'autorizzazione concessa ai prestatori di servizi di condivisione di contenuti online deve riguardare anche gli atti compiuti da (i) utenti che non agiscono su base commerciale o (ii) utenti la cui attività non genera ricavi significativi.

Come precedentemente affermato in merito alle "grandi quantità di contenuti" in relazione all'ambito soggettivo di applicazione dell'art. 17, anche in questo caso sarebbe controproducente definire in termini quantitativi cosa siano i "ricavi significativi", preferendosi un'analisi caso per caso delle circostanze concrete.

La prima categoria di utenti quindi, secondo la Commissione, potrebbe riguardare la condivisione di contenuti senza alcuno scopo di lucro, "*ad esempio nel caso di utenti che caricano un video domestico che include musica utilizzata come sottofondo*"[538]. La seconda categoria potrebbe riguardare, invece, "*ad esempio, utenti che caricano tutorial con musica o immagini da cui ottengono ricavi pubblicitari limitati*". Diversamente da queste due ipotesi, gli utenti che, invece, agiscono su base commerciale o ottengono ricavi significativi dai contenuti caricati non rientrano nell'ambito di tale autorizzazione o non sono coperti dalla stessa, salvo diverso accordo delle parti medesime.

Il Considerando 69 della Direttiva aggiunge poi che, se i titolari dei diritti hanno espressamente autorizzato gli utenti a caricare e mettere a disposizione opere o altri materiali su un servizio di condivisione di contenuti online, l'atto di comunicazione al pubblico del prestatore di servizi è permesso nell'ambito dell'autorizzazione concessa dal titolare dei diritti. Tuttavia, i prestatori di servizi di condivisione di contenuti online non dovrebbero poter beneficiare della presunzione che i loro utenti possano lecitamente disporre di tutti i diritti rilevanti. Inoltre, i prestatori di servizi di condivisione di contenuti online non devono ottenere un'autorizzazione distinta quando i titolari dei diritti hanno già autorizzato espressamente gli utenti a caricare contenuti specifici. Come nota la Commissione infatti, in tali casi, l'atto di comunicazione al pubblico è già stato autorizzato nell'ambito dell'autorizzazione concessa agli utenti.

5. Un nuovo meccanismo di responsabilità

Il paragrafo quarto dell'art. 17 è quello che dimostra il maggior interesse ai fini di una corretta analisi del bilanciamento fra diritto d'autore e diritto alla privacy degli utenti. Esso,

[538] Communication From The Commission To The European Parliament And The Council: Guidance on Article 17 of Directive 2019/790 on Copyright in the Digital Single Market COM/2021/288 final, cit.

infatti, introduce nell'ordinamento europeo un nuovo meccanismo di responsabilità che deroga a quello previsto per gli ISP dalla Direttiva e-commerce e si struttura "*in negativo*", elencando delle condizioni che, ove dimostrate, impediscono il verificarsi di una responsabilità diretta in capo ai prestatori di servizi di condivisione di contenuti online.

La Direttiva 2019/790 stabilisce che un *provider* che integri tanto il requisito soggettivo che quello oggettivo, sarà ritenuto responsabile qualora si verifichi una violazione del diritto d'autore sulla sua piattaforma. Il quarto paragrafo è chiaro nel suo *incipit* in quanto dispone che qualora "*non sia concessa alcuna autorizzazione, i prestatori di servizi di condivisione di contenuti online sono responsabili per atti non autorizzati di comunicazione al pubblico, compresa la messa a disposizione del pubblico, di opere e altri materiali protetti dal diritto d'autore*". L'art. 17 tuttavia subito aggiunge che tale responsabilità non si verifica allorché il *provider* dimostri di *"(a) aver compiuto i massimi sforzi per ottenere un'autorizzazione, e (b) aver compiuto, secondo elevati standard di diligenza professionale di settore, i massimi sforzi per assicurare che non siano disponibili opere e altri materiali specifici per i quali abbiano ricevuto le informazioni pertinenti e necessarie dai titolari dei diritti; e in ogni caso, (c) aver agito tempestivamente, dopo aver ricevuto una segnalazione sufficientemente motivata dai titolari dei diritti, per disabilitare l'accesso o rimuovere dai loro siti web le opere o altri materiali oggetto di segnalazione e aver compiuto i massimi sforzi per impedirne il caricamento in futuro conformemente alla lettera b)".*

Dall'articolato normativo emergono chiaramente tre requisiti che procederemo ad analizzare ora partitamente, ossia: la nozione dei massimi sforzi per ottenere una autorizzazione di cui alla lettera a); l'attività di cui alla lettera b), su cui vedremo verificarsi i maggiori punti critici della disciplina in analisi ed infine l'attività di rimozione permanente di cui alla lettera c), in cui si procederà a segnalare le differenze con la controparte statunitense.

5.1. La lettera A): I massimi sforzi per ottenere un'autorizzazione

L'art. 17 della Direttiva in commento distingue chiaramente l'ipotesi in cui l'attività della piattaforma avvenga in presenza di autorizzazione, rispetto a quando tale autorizzazione non vi sia, affermando, in linea di principio, che ove non sia concessa alcuna autorizzazione, i prestatori di servizi di condivisione di contenuti online sono responsabili degli illeciti avvenuti sulla piattaforma. La lettera a) del paragrafo quarto, tuttavia, offre un'ulteriore tutela al *provider* sulla constatazione che, come già affermato, nessuna delle disposizioni della Direttiva dovrebbe incidere sulla libertà contrattuale dei soggetti presi in considerazione, di tal che, come ricordato dal Considerando 61, i titolari dei diritti non dovrebbero essere obbligati a rilasciare un'autorizzazione o a concludere accordi di licenza.

Stante tale constatazione, il legislatore europeo considera che, date anche le altre condizioni di cui alle altre lettere del paragrafo quarto, la dimostrazione di essersi attivati e adoperati al meglio per ottenere una licenza, senza aver avuto successo, legittima un'esclusione di responsabilità per eventuali illecite condivisioni di materiale protetto dal diritto d'autore.

I paragrafi 1 e 4 dell'articolo 17, sono sistematicamente collegati, in quanto il primo stabilisce una responsabilità primaria per atti di comunicazione al pubblico commessi congiuntamente dall'OCSSP e dai suoi utenti, mentre il secondo prevede dei meccanismi atti ad escludere il ricorrere della responsabilità nelle ipotesi in cui l'OCSSP non abbia ottenuto le necessarie licenze[539].

[539] In questo senso si esprimono C. GEIGER, B.J. JÜTTE, *Platform liability under article 17 of the copyright in the Digital Single Market directive, automated filtering and fundamental rights: an impossible match*, 2020, 40, disponibile sul sito:

Cosa integrano i "*massimi sforzi*"[540] non viene affermato dalla Direttiva, probabilmente per evitare di imporre prassi di mercato specifiche e lasciare invece liberi i prestatori di servizi ed i titolari dei diritti d'autore di negoziare liberamente i regimi delle autorizzazioni. Le linee guida della Commissione sul punto affermano che le azioni compiute dai prestatori di servizi per avviare un dialogo con i titolari dei diritti devono essere valutate caso per caso. Secondo la Commissione, in particolare, "*dovrebbero ad esempio essere presi in considerazione elementi quali le specifiche prassi di mercato in settori diversi (valutando ad esempio se la gestione collettiva sia una prassi diffusa o no) o le misure che gli Stati membri possono aver adottato per agevolare le autorizzazioni, ad esempio i meccanismi volontari di mediazione*[541]".

Appare in ogni caso che la richiesta di massimi sforzi si compendi in una proattiva ricerca dell'attuale titolare dei diritti d'autore sull'opera da comunicare al pubblico ed altresì in una attiva ricerca di un dialogo con tali titolari. Chiaramente il legislatore europeo è a conoscenza del fatto che non sempre i titolari del *copyright* sono facilmente identificabili, per questo, anche in relazione al principio di proporzionalità, deve essere presa in considerazione una certa qual ragionevolezza nel richiedere ai *provider* questi sforzi. La Commissione sul punto si mostra aderente alla prospettiva così presentata in quanto ritiene che i prestatori di servizi dovrebbero, come minimo, avviare proattivamente un dialogo con i titolari dei diritti che possono essere facilmente identificati e rintracciati, in particolare quelli che rappresentano un ampio catalogo di opere o altri materiali. Questo coinvolge anche gli organismi di gestione collettiva che agiscono in conformità alla Direttiva 2014/26/UE, i quali sono chiaramente facilmente identificabili, per natura, ed incoraggiati a stipulare accordi di licenza con le piattaforme.

Viceversa, ove un titolare dei diritti d'autore non sia facilmente identificabile o rintracciabile, richiedere un obbligo di risultato nell'ottenere una licenza sarebbe irragionevole e contrario al principio di proporzionalità. In questo senso poi la Commissione incoraggerebbe gli Stati all'istituzione di *"registri dei titolari dei diritti consultabili dai prestatori di servizi di condivisione di contenuti online, nel rispetto delle norme sulla protezione dei dati, se del caso*"[542]. Allo stato dell'arte, non risulta che tali registri siano stati attuati.

Il Considerando 66 poi richiama l'attenzione dell'interprete sul fatto che la valutazione da compiere per comprendere i massimi sforzi posti in essere dagli OCSSP dovrebbe tenere conto delle "*dimensioni dei titolari dei diritti e della tipologia di opera e degli altri materiali*", ma del pari anche delle dimensioni dei *provider* stessi. La Commissione in merito consiglia agli Stati membri, nel recepire la Direttiva, di considerare che "*se da un lato è prevedibile che i grandi prestatori di servizi con un vasto pubblico in diversi o in tutti gli Stati membri contattino un alto numero di titolari dei diritti per ottenere le autorizzazioni, dall'altro è lecito attendersi che i prestatori di servizi più*

«https://digitalcommons.wcl.american.edu/research/64/» (Ultimo accesso: 10 maggio 2022). Essi infatti affermano: "*Article 17(1) and (4) are systematically linked, whereby the former establishes primary liability for acts of communication to the public jointly committed by the OCSSP and its users, which morphs into secondary liability if the OCSSP has failed to obtain the necessary licenses*"

[540] Differenze nella formulazione linguistica dei "massimi sforzi" sono stati evidenziati da: E. ROSATI, *DSM Directive Series #5: Does the DSM Directive mean the same thing in all language versions? The case of 'best efforts' in Article 17(4)(a)*,), in *The IPKat,* 2019, acessibile presso «https://ipkitten.blogspot.com/2019/05/dsm-directive-series-5-does-dsm.html» (Ultimo accesso: 10 maggio 2022), D. LARROYED, *When Translations Shape Legal Systems: How Misguided Translations Impact Users and Lead to Inaccurate Transposition – The Case of 'Best Efforts' Under Article 17 DCDSM*, in *SSRN*, 2020, accessibile presso: «https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3740066» (Ultimo accesso: 10 maggio 2022).

[541] Communication From The Commission To The European Parliament And The Council: Guidance on Article 17 of Directive 2019/790 on Copyright in the Digital Single Market COM/2021/288 final, cit.

[542] Communication From The Commission To The European Parliament And The Council: Guidance on Article 17 of Directive 2019/790 on Copyright in the Digital Single Market COM/2021/288 final, cit.

piccoli, con un pubblico limitato o di livello nazionale, contattino proattivamente solo gli organismi di gestione collettiva competenti ed eventualmente alcuni altri titolari di diritti facilmente identificabili. Questi piccoli prestatori di servizi dovrebbero provvedere affinché gli altri titolari dei diritti possano contattarli facilmente, ad esempio fornendo recapiti chiari o strumenti ad hoc sul loro sito web, e dovrebbero avviare un dialogo con tutti i titolari di diritti che li contattano per offrire una licenza[543]".

L'art. 102-septies della legge sul diritto d'autore italiana, nell'implementare tale disposizione, ricorda poi, del pari di quanto dispone l'art. 17 paragrafo 5, come "*per stabilire, secondo il principio di proporzionalità, se il prestatore di servizi di condivisione di contenuti online è esente da responsabilità, sono presi in considerazione, con valutazione caso per caso, anche la tipologia, il pubblico e la dimensione del servizio e la tipologia di opere o di altri materiali caricati dagli utenti del servizio, nonché la disponibilità di strumenti adeguati ed efficaci e il relativo costo per i prestatori di servizi*".

Non a caso allora il legislatore europeo al paragrafo sesto prevede un regime di responsabilità in parte derogatorio per quei *provider* che abbiano un fatturato annuo inferiore a determinate soglie[544]. Il Considerando 67 infatti tiene conto del caso specifico delle imprese start-up che operano tramite il caricamento degli utenti per sviluppare nuovi modelli di business. Esso afferma che il regime derogatorio applicabile ai nuovi prestatori di servizi con un fatturato e un pubblico ridotti "*dovrebbe andare a vantaggio delle imprese effettivamente nuove e dovrebbe pertanto cessare di applicarsi tre anni dopo la prima disponibilità online dei loro servizi nell'Unione. Questo regime non dovrebbe essere abusato tramite accordi finalizzati ad estenderne i benefici oltre i primi tre anni. In particolare, esso non dovrebbe applicarsi ai servizi nuovamente creati o ai servizi forniti sotto una nuova denominazione, ma che svolgono l'attività di un prestatore di servizi di condivisione di contenuti online già esistente che non potrebbe beneficiare o non potrebbe più beneficiare di questo regime*". Alla luce di questo, l'art. 17 paragrafo sesto prevede che i *provider* i cui servizi sono disponibili al pubblico nell'Unione da meno di tre anni e che hanno un fatturato annuo inferiore a 10 milioni di euro godano di condizioni di responsabilità privilegiate. In particolare, le condizioni in virtù del regime di responsabilità di cui al paragrafo 4 sono limitate alla conformità alla lettera a) e alla circostanza di aver agito tempestivamente, in seguito alla ricezione di una segnalazione sufficientemente motivata, per disabilitare l'accesso o rimuovere dai loro siti web tali opere. Si aggiunge poi che, se il numero medio di visitatori unici mensili di tali prestatori di servizi supera i 5 milioni, calcolati sulla base del precedente anno civile, essi devono dimostrare altresì di aver compiuto i massimi sforzi per impedire l'ulteriore caricamento di opere o di altri materiali oggetto della segnalazione per i quali i titolari dei diritti abbiano fornito informazioni pertinenti e necessarie.

In sostanza dunque per questi *provider* vale la disciplina derogatoria che prevede che: (a) se hanno meno di 5 milioni di visitatori unici, i "nuovi" prestatori di servizi sono tenuti a adoperarsi al meglio per ottenere un'autorizzazione (articolo 17, paragrafo 4, lettera a)) e devono rispettare l'obbligo di "segnalazione e rimozione" di cui alla prima parte dell'articolo 17, paragrafo 4, lettera c); (b)se hanno più di 5 milioni di visitatori unici, tali "nuovi" prestatori di servizi, oltre ad essere soggetti agli stessi obblighi di adoperarsi al meglio per ottenere un'autorizzazione e di "notifica e rimozione" che gravano sui prestatori di servizi con un

[543] Communication From The Commission To The European Parliament And The Council: Guidance on Article 17 of Directive 2019/790 on Copyright in the Digital Single Market COM/2021/288 final, cit.

[544] Per maggiori informazioni in merito si veda J. P. QUINTAIS, P. MEZEI, I. HARKAI, J. C. MAGALHÃES, C. KATZENBACH, S. F. SCHWEMER, & T. RIIS, *Final Report on mapping of EU legal framework and intermediaries' practices on copyright content moderation and removal*, 2022, cit., 59 e ss.; M. L. MONTAGNANI, *A New Interface between Copyright Law and Technology: How User-Generated Content Will Shape the Future of Online Distribution*, in *Bocconi Legal Studies Research Paper* No. 1275326, 2009, liberamente accessibile presso: «https://ssrn.com/abstract=1275326» o «http://dx.doi.org/10.2139/ssrn.1275326» (Ultimo accesso: 10 maggio 2022).

pubblico più ridotto, devono anche rispettare l'obbligo di impedire futuri caricamenti di opere oggetto di segnalazione a norma della seconda parte dell'articolo 17, paragrafo 4, lettera c). Rimane che, in ogni caso, a nessuna delle due categorie di prestatori di servizi si applica l'obbligo di adoperarsi al meglio per assicurare che non siano disponibili contenuti non autorizzati, previsto all'articolo 17, paragrafo 4, lettera b).

La Commissione, nelle sue linee guida, introduce una sorta di velata presunzione in questo campo in quanto afferma che "*qualora un prestatore di servizi contatti un titolare dei diritti ma quest'ultimo rifiuti di avviare negoziati per la concessione di un'autorizzazione relativa a contenuti di cui è titolare, o rigetti offerte ragionevoli fatte in buona fede, si dovrebbe ritenere che il prestatore di servizi abbia rispettato l'obbligo di diligenza di cui all'articolo 17, paragrafo 4, lettera a). Tuttavia, per non incorrere in responsabilità qualora il contenuto non autorizzato sia disponibile sul suo servizio, il prestatore di servizi dovrebbe comunque dimostrare di essersi adoperato al meglio ai fini dell'articolo 17, paragrafo 4, lettere b) e c)*[545]*"*.

Per concludere, un punto che lascia perplessi riguarda il rapporto fra tale esenzione di responsabilità ed il Considerando 61. A norma di quest'ultimo infatti, come già richiamato, gli accordi di licenza dovrebbero essere equi e mantenere un equilibrio ragionevole tra entrambe le parti contraenti. Questo significa che i titolari dei diritti dovrebbero ricevere un compenso adeguato per l'utilizzo delle loro opere o di altri materiali. Quindi, ci si chiede, il concetto di "massimi sforzi" di cui alla lettera a) dovrebbe comprendere anche l'equità dei compensi? *Quid iuris* nel caso in cui tale equità non venisse rinvenuta nei negoziati, pur intervenuti, fra le parti? La Commissione afferma sul punto che, a suo avviso, il concetto di massimi sforzi "*dovrebbe comprendere anche gli sforzi […] per condurre negoziati in buona fede e concludere accordi di licenza equi. A tal fine, i prestatori di servizi dovrebbero essere trasparenti con i titolari dei diritti per quanto riguarda i criteri che intendono utilizzare per identificare e remunerare i contenuti oggetto dell'accordo, in particolare quando utilizzano tecnologie per il riconoscimento dei contenuti al fine di rendere conto degli utilizzi di contenuti oggetto di licenze, e dovrebbero raggiungere, ove possibile, un accordo con i titolari dei diritti*". Le linee guida aggiungono poi, sempre sul punto, che "*si può ritenere che i prestatori di servizi che rifiutano di concludere un accordo di licenza che prevede condizioni eque e mantiene un ragionevole equilibrio tra le parti non si siano adoperati al meglio per ottenere un'autorizzazione. I prestatori di servizi non dovrebbero invece essere tenuti ad accettare offerte per la conclusione di accordi che non siano equi e non mantengano un equilibrio tra le parti. La valutazione di ciò che si intende per condizioni eque e un ragionevole equilibrio tra le parti sarà effettuata caso per caso*"[546]. Il punto, comunque, che rimane non detto è quali siano le conseguenze in questo caso. Si potrebbe allora immaginare che un sindacato sull'equità o meno delle proposte di licenze potrebbe portare ad una affermazione di responsabilità dei *provider*, non ritenendo integrati i "massimi sforzi". Sul punto si auspica quindi un intervento chiarificatore della giurisprudenza della Corte di Giustizia, potendo comportare incertezze nell'applicazione di questo articolo.

5.2. La lettera B): I meccanismi di filtraggio

Ove si verifichino le condizioni previste dalla lettera a) del paragrafo quarto dell'art. 17, l'analisi volta a verificare l'assenza di responsabilità del *provider* si deve concentrare sulla lettera b). Ricordando quanto affermato, essa richiede di dimostrare di "*aver compiuto, secondo elevati standard di diligenza professionale di settore, i massimi sforzi per assicurare che non siano disponibili*

[545] Communication From The Commission To The European Parliament And The Council: Guidance on Article 17 of Directive 2019/790 on Copyright in the Digital Single Market COM/2021/288 final, cit.
[546] Communication From The Commission To The European Parliament And The Council: Guidance on Article 17 of Directive 2019/790 on Copyright in the Digital Single Market COM/2021/288 final, cit.

opere e altri materiali specifici per i quali abbiano ricevuto le informazioni pertinenti e necessarie dai titolari dei diritti".

Questa disposizione è sicuramente la più controversa e, a parere di chi scrive, quella che maggiormente mette in evidenza i profili critici dell'*enforcement* del dritto d'autore nel panorama digitale, in particolare con riferimento alla tutela dei dati personali degli utenti, della loro libertà di espressione e di autodeterminazione. Checché ne dica il legislatore europeo, questa disposizione obbliga i *provider* ad una sorveglianza del web e ad un monitoraggio costante delle attività online compiute dagli utenti, non avendo alcun valore le declamazioni di principio in senso contrario[547], se poi nei fatti si richiede una simile sorveglianza[548]. Senza voler anticipare tuttavia quanto diffusamente sarà oggetto del proseguo del presente capitolo, la base di partenza del ragionamento è quella riguardante il significato della disposizione di cui alla lettera b), in modo da fugare ogni dubbio sulla sua possibile portata.

La disposizione normativa è innanzitutto formulata secondo un impreciso periodo ipotetico in cui la protasi dello stesso è data dall'aver ricevuto le informazioni pertinenti e necessarie, mentre l'apodosi dalla dimostrazione di aver compiuto i massimi sforzi richiesti dalla normativa. Quindi prima evidente condizione di applicabilità della disciplina è data dalla definizione di cosa si intenda per queste "*informazioni pertinenti e necessarie*". Il Considerando 66 esplica sul punto che "*i titolari dei diritti dovrebbero fornire ai prestatori di servizi le informazioni pertinenti e necessarie tenendo conto, tra l'altro, delle dimensioni dei titolari dei diritti e della tipologia di opera e degli altri materiali*". Ne consegue evidentemente che, confermati nell'interpretazione anche dalla Commissione europea, qualora i titolari dei diritti non forniscano tali informazioni volte a soddisfare i requisiti di cui all'articolo 17, paragrafo 4, i prestatori di servizi di condivisione di contenuti online non sono responsabili dei caricamenti non autorizzati. È quindi coessenziale al funzionamento di questo meccanismo di responsabilità una collaborazione fra OCSSP e titolare dei diritti d'autore.

Non serve poi sottolineare che, ovviamente, la fattispecie della lettera b) richiede che le "informazioni pertinenti e necessarie" siano fornite in anticipo, pena l'inutilizzabilità dello strumento. La valutazione poi della pertinenza e della necessarietà non potrebbe essere fatta a priori e in modo uguale per ogni situazione, essendo invece consigliabile adottarne una lettura caso per caso, anche alla luce, come vedremo, delle singole richieste di dati provenienti dal funzionamento tecnico delle tecnologie adottabili per adempiere ai "massimi sforzi" richiesti dalla Direttiva.

Ad avviso della Commissione, le informazioni in questione devono essere precise per consentire ai prestatori di servizi di condivisione di contenuti online di intervenire con gli strumenti tecnici necessari. In questo senso, ciò che può costituire un'informazione "pertinente" varierà a seconda delle opere interessate e delle circostanze relative alle opere o

---

[547] Il riferimento è all'art 17 paragrafo 8 che dispone, paradossalmente, "*L'applicazione del presente articolo non comporta alcun obbligo generale di sorveglianza*".

[548] Trattando della proposta di Direttiva Laura Camarella, in L. CAMARELLA, *La responsabilità dell'Internet Service Provider alla luce della nuova Direttiva sul diritto d'autore nel mercato unico digitale*, cit., si esprime affermando "*L'articolo 15 della direttiva e-commerce vieta agli Stati membri di imporre ai fornitori obblighi generali di controllo anche delle informazioni che trasmettono o archiviano, come ad esempio obblighi generali di ricerca attiva di fatti o circostanze indicanti attività illegali. Questo presenta un problema per la proposta, poiché le "tecnologie di riconoscimento dei contenuti efficaci" richiedono, per definizione, proprio questa tipologia di monitoraggio: diversamente, come sarebbe possibile "riconoscere efficacemente" i contenuti in violazione su una piattaforma tramite uno strumento tecnologico senza la supervisione della totalità dei contenuti su quella piattaforma? Al fine di "riconoscere" l'indesiderato contenuto all'interno di una più vasta raccolta di contenuti si deve, logicamente, esaminare ogni contenuto di quella raccolta*".

agli altri materiali specifici. Secondo la Commissione, "*le informazioni dovrebbero, come minimo, essere precise per quanto riguarda i diritti di proprietà dell'opera o del materiale in questione. Ciò che può essere considerato "necessario" varia a seconda delle soluzioni utilizzate dai prestatori di servizi e dovrebbe consentire ai prestatori di servizi di applicare efficacemente le soluzioni tecnologiche che decidono di utilizzare. Ad esempio, qualora si faccia ricorso al fingerprinting, i titolari dei diritti possono essere invitati a fornire un'impronta digitale elettronica dell'opera/del materiale specifico in questione o un file che lo stesso prestatore di servizi sottoporrà a fingerprinting, unitamente a informazioni sulla titolarità dei diritti. Quando si utilizzano soluzioni basate su metadati, le informazioni fornite possono riguardare, ad esempio, il titolo, l'autore/produttore, la durata, la data o altre informazioni pertinenti e necessarie affinché i prestatori di servizi di condivisione di contenuti online possano intervenire. In tale contesto è importante che i metadati forniti dai titolari dei diritti non siano successivamente rimossi*[549]".

Le linee guida ricordano poi come il concetto di "informazioni pertinenti e necessarie" presupponga che i prestatori di servizi tengano conto della natura e della qualità delle informazioni che i titolari dei diritti possono realisticamente fornire. A tale riguardo, la Commissione segnala poi che i titolari dei diritti possono scegliere di identificare i contenuti specifici protetti dal diritto d'autore e dai diritti connessi la cui disponibilità online non autorizzata potrebbe arrecare loro un notevole danno economico. Per la Commissione, infatti, l'identificazione preventiva di tali contenuti da parte dei titolari dei diritti può essere un fattore di cui tenere conto nel valutare se i prestatori di servizi di condivisione di contenuti online si siano adoperati al meglio per garantire che tali contenuti specifici non siano disponibili. La possibilità di identificare quei contenuti che potrebbero comportare un significativo danno economico non è una disposizione ben delineata dalle linee guida, tuttavia appare preoccupante. Si afferma infatti che "*i prestatori di servizi dovrebbero prestare particolare attenzione e diligenza nell'adempimento del loro obbligo di adoperarsi al meglio prima di caricare contenuti che potrebbero causare un danno economico significativo ai titolari dei diritti. […] Al fine di garantire il giusto equilibrio tra i diversi diritti fondamentali in gioco, segnatamente la libertà di espressione degli utenti, il diritto di proprietà intellettuale dei titolari dei diritti e il diritto dei prestatori alla libertà d'impresa, tale maggiore attenzione ai contenuti la cui disponibilità potrebbe causare un danno economico significativo dovrebbe essere limitata ai casi di elevato rischio di danni economici significativi, che dovrebbero essere adeguatamente giustificati dai titolari dei diritti*"[550].

Tuttavia, come ricorda l'Avvocato Generale Henrik Saugmandsgaard Øe, si darebbe in questo modo la possibilità di "riservare" i materiali la cui messa in rete non autorizzata sia idonea a causare un danno economico significativo. Viene inoltre indicato che i *provider* non adempirebbero ai loro obblighi di massimi sforzi qualora consentissero la messa in rete di contenuti che riproducono questi stessi materiali nonostante siffatte riserve. L'Avvocato Generale ritiene che se ciò dovesse essere inteso nel senso che questi stessi prestatori dovrebbero "*bloccare ex ante taluni contenuti dietro la mera allegazione di un rischio di danno economico importante da parte dei titolari dei diritti – fermo restando che gli orientamenti non contengono altri criteri che limitino in maniera oggettiva il meccanismo di «riserva» a taluni casi particolari –,quand'anche tali contenuti non fossero manifestamente contraffatti, la disposizione mostrerebbe incompatibilità con i diritti fondamentali previsti dall'ordinamento europeo*". [551]

[549] Communication From The Commission To The European Parliament And The Council: Guidance on Article 17 of Directive 2019/790 on Copyright in the Digital Single Market COM/2021/288 final, cit.
[550] Communication From The Commission To The European Parliament And The Council: Guidance on Article 17 of Directive 2019/790 on Copyright in the Digital Single Market COM/2021/288 final, cit.
[551] Avvocato Generale Henrik Saugmandsgaard Øe, conclusioni presentate il 15 luglio 2021 nella Causa C-401/19, Repubblica di Polonia contro Parlamento europeo, Consiglio dell'Unione europea, ricorso presentato ex art. 263 TFUE, cit.

In ogni caso, se da parte dei titolari dei diritti d'autore si impone un onere di fornire le informazioni "pertinenti e necessarie", dall'altra parte, in capo alle piattaforme di condivisione dei contenuti online si chiede un'obbligazione più particolare, che il legislatore europeo, ma anche la Commissione ed il legislatore nazionale, dicono e non dicono allo stesso tempo, ossia la sottendono, meno velatamente dello sperato. Questo obbligo consiste nell'adozione di soluzioni tecnologiche di riconoscimento e filtraggio dei contenuti, quelle tecnologie che abbiamo già avuto modo di incontrare nel capitolo precedente.

Il Considerando 66 infatti chiede che, nel valutare se un prestatore di servizi di condivisione di contenuti online abbia compiuto i massimi sforzi nel rispetto di elevati standard di diligenza professionale di settore, si debba considerare se il prestatore di servizi abbia adottato tutte le misure che un operatore diligente adotterebbe per ottenere il risultato di impedire la disponibilità di opere o altri materiali non autorizzati sul suo sito web. In questo, secondo il Considerando 66, si dovrebbe tener conto delle migliori pratiche del settore e dell'efficacia delle misure adottate.

Le linee guida della Commissione poi affermano che l'articolo 17, paragrafo 4, lettera b), dovrebbe essere attuato in modo tecnologicamente neutro e tale da rispondere alle esigenze future. Gli Stati membri non dovrebbero pertanto prescrivere, nelle rispettive leggi di attuazione, l'uso di una soluzione tecnologica né imporre soluzioni tecnologiche specifiche ai prestatori di servizi come condizione per dimostrare di essersi adoperati al meglio. Il legislatore italiano si è perfettamente adeguato a quanto raccomandato sul punto, preferendo non prevedere nulla e non fornire alcuna indicazione in merito.

Il legislatore europeo quindi, nel fornire indicazioni sui massimi sforzi che gli OCSSP devono compiere, ritiene che si debbano prendere in considerazione una serie di elementi, quali le dimensioni del servizio, l'evoluzione dello stato dell'arte dei mezzi esistenti, compresi i potenziali sviluppi futuri, per evitare la disponibilità di diversi tipi di contenuti e il costo di tali mezzi per i prestatori di servizi. Ciò comprende chiaramente un'analisi delle principali pratiche adoperate nel settore per raggiungere il fine di impedire che materiali protetti dal diritto d'autore, privi di autorizzazione al loro utilizzo, siano messi a disposizione del pubblico. Secondo la Commissione europea, è particolarmente importante esaminare le pratiche di settore vigenti sul mercato in un dato momento. In merito alle misure tecnologiche che dovrebbero essere adottate si afferma che prestatori di servizi di condivisione di contenuti online dovrebbero tuttavia rimanere liberi di scegliere la tecnologia o la soluzione più adatta per adempiere l'obbligo di diligenza nelle rispettive situazioni concrete.

La Commissione ricorda che il dialogo con le parti interessate aveva fatto emergere che la tecnologia di riconoscimento dei contenuti è oggi comunemente utilizzata per gestire l'uso dei contenuti protetti dal diritto d'autore, almeno da parte dei principali prestatori di servizi di condivisione di contenuti online e per quanto riguarda determinati tipi di contenuti. La tecnologia di riconoscimento dei contenuti basata sul *fingerprinting,* come visto anche nel precedente capitolo, sembra essere quella più utilizzata. Il capitolo terzo, infatti, aveva portato esempi quali il *Content ID* di *Youtube*, i sistemi di *Audible Magic* o di *Facebook Rights Manager*, tutti basati principalmente, anche se non esclusivamente, sul sistema di *Automatic Content Recognition* rappresentato dal *fingerprinting.* La Commissione europea allo stesso tempo afferma tuttavia che tale particolare tecnologia non dovrebbe essere necessariamente considerata come lo standard del mercato, in particolare per i piccoli prestatori di servizi.

Sul punto il Considerando 66 esplicita che "*mezzi diversi per evitare la disponibilità di contenuti non autorizzati protetti dal diritto d'autore potrebbero essere appropriati e proporzionati a seconda*

del tipo di contenuto e non è pertanto da escludersi che in alcuni casi la disponibilità dei contenuti non autorizzati possano essere evitati solo previa notifica dei titolari dei diritti. Qualsiasi misura adottata dai prestatori di servizi dovrebbe essere efficace rispetto agli obiettivi perseguiti, ma non dovrebbero andare oltre quanto necessario per raggiungere l'obiettivo di evitare e interrompere la disponibilità di opere e altri materiali non autorizzati".

In questo senso poi la Commissione nota che, nella pratica, ciò significa che non è ragionevole attendersi che i prestatori di servizi di condivisione di contenuti online applichino le soluzioni più costose o sofisticate qualora ciò risulti sproporzionato nel loro caso specifico. Ciò vale anche per i contenuti che i titolari dei diritti pertinenti hanno identificato come contenuti la cui disponibilità potrebbe arrecare loro un danno significativo. Inoltre, come spiegato al Considerando 66, non si può escludere che in alcuni casi la disponibilità di contenuti non autorizzati possa essere evitata solo a seguito di una segnalazione da parte dei titolari dei diritti. Ciò può risultare proporzionato, ad esempio, per i contenuti in relazione ai quali la tecnologia non è prontamente disponibile sul mercato o non è sviluppata in un determinato momento.

Per queste ragioni appare ragionevole, secondo le linee guida della Commissione, che i prestatori di servizi di maggiori dimensioni e con un pubblico più ampio "*utilizzino soluzioni/tecnologie più avanzate rispetto ad altri prestatori di servizi con un pubblico e risorse limitati*". Del pari appare più ragionevole pensare che "*i piccoli prestatori di servizi ricorrano a soluzioni più semplici (come i metadati o la ricerca di parole chiave) purché tali soluzioni non comportino un blocco eccessivo dei contenuti, che sarebbe contrario a quanto previsto dai paragrafi 7 e 9*[552]".

Senza voler anticipare quanto verrà diffusamente esposto in merito alla tutela dei dati personali in relazione a questi sistemi tecnologici di sorveglianza, si segnala solo che la Commissione, con una vuota petizione di principio, ritiene che, teoricamente "*l'uso di tecnologie come il riconoscimento dei contenuti non dovrebbe di per sé rendere necessaria l'identificazione degli utenti che caricano i loro contenuti; se però questo è il caso, devono essere rispettate le pertinenti norme in materia di protezione dei dati, compresi i principi di minimizzazione dei dati e limitazione delle finalità*[553]". Si avrà modo, dunque, di vedere se effettivamente tali principi sono rispettati nei fatti. Rimandando al seguito dell'elaborato ulteriori indicazioni sul punto, si è quindi compreso che ove gli OCSSP vogliano andare esenti da responsabilità dovranno dimostrare non solo di aver compiuto i massimi sforzi per ottenere una licenza, ma anche aver implementato nelle proprie piattaforme i più opportuni sistemi tecnologici, secondo le migliori prassi del mercato, al fine di bloccare tutti quei contenuti protetti dal diritto d'autore di cui i titolari dello stesso abbiano fornito le informazioni identificative.

5.3. La lettera C): "Notice and take down" o "Notice and stay down"?

La terza condizione segnalata dall'art. 17 paragrafo quarto per andare esenti da responsabilità si compendia nel dimostrare di *"aver agito tempestivamente, dopo aver ricevuto una segnalazione sufficientemente motivata dai titolari dei diritti, per disabilitare l'accesso o rimuovere dai loro siti web le opere o altri materiali oggetto di segnalazione e aver compiuto i massimi sforzi per impedirne il caricamento in futuro conformemente alla lettera b)".*

[552] Communication From The Commission To The European Parliament And The Council: Guidance on Article 17 of Directive 2019/790 on Copyright in the Digital Single Market COM/2021/288 final, cit.
[553] Communication From The Commission To The European Parliament And The Council: Guidance on Article 17 of Directive 2019/790 on Copyright in the Digital Single Market COM/2021/288 final, cit.

Questa disposizione segnala una prospettiva innovativa nel panorama delle fattispecie di responsabilità dei *provider* andando a modificare il tradizionale meccanismo di "*notice and take down*", come accennato nel capitolo secondo, e procedendo ad imporre invece, in ambito europeo, un procedimento di "*notice and stay down*"[554]. Tale distinzione consente oggi di affermare che non sarà sufficiente per il *provider* agire disabilitando l'accesso o rimuovendo i contenuti in violazione del diritto d'autore dalla propria piattaforma, su segnalazione del titolare dei diritti d'autore, sarà invece altresì necessario impedire il futuro caricamento da parte degli utenti del medesimo contenuto.

Anche questo, come vedremo, del pari della lettera b), comporta un obbligo di sorveglianza e di monitoraggio costante del web, proprio alla ricerca non solo di tutti quei materiali potenzialmente lesivi di cui alla lettera b), ma altresì di tutti quei materiali in precedenza segnalati e rimossi per i quali si deve aver cura che non siano ricaricati.

Prima di procedere all'analisi della disciplina europea introduttiva di questo meccanismo di responsabilità, si rende necessario procedere ad una visione comparata del modello del *notice and take down* al fine di tratteggiare le differenze più significative fra i due sistemi.

5.3.2. Notice and take down

Come illustrato nel secondo capitolo, trattando della responsabilità degli *Internet Service Provider* si è avuto modo di affermare che la statunitense 17 U.S.C §512 (c)(3) introduce un interessante meccanismo di esclusione della responsabilità ove il *provider* riesca a dimostrare di aver proceduto a rimuovere o disabilitare l'accesso a quei contenuti in violazione del diritto d'autore che gli siano stati correttamente segnalati dal titolare del diritto d'autore.

---

554 Notazioni dottrinali rinvenibili presso: G. CASSANO, F. BUFFA, *Responsabilità del content provider e dell'host provider,* in *Il Corriere giuridico*, fasc. 1, 2003, 77-81, liberamente consultabile presso: «https://www.altalex.com/documents/news/2005/07/19/responsabilita-del-content-provider-e-dell-host-provider» (Ultimo accesso: 10 maggio 2022); M. LEISTNER, *European Copyright Licensing and Infringement Liability Under Art. 17 DSM-Directive Compared to Secondary Liability of Content Platforms in the U.S. – Can We Make the New European System a Global Opportunity Instead of a Local Challenge?,* in *Zeitschrift für Geistiges Eigentum/Intellectual Property Journal (ZGE/IPJ)*, 2020, liberamente accessibile presso: «https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3572040» (Ultimo accesso: 10 maggio 2022). Sulla comparazione fra sistemi statunitensi ed europei si veda altresì J. GINSBURG, *A United States Perspective on Digital Single Market Directive Art. 17, EU COPYRIGHT LAW: A COMMENTARY*, in I. STAMATOUDI, P. TORREMANS, eds., (2d ed. Edward Elgar, 2020), in *Columbia Public Law Research Paper* No. 14-654, liberamente accessibile presso: «https://ssrn.com/abstract=3579076» (Ultimo accesso: 10 maggio 2022). Ulteriori notazioni dottrinali rinvenibili presso: M. L. MONTAGNANI, *A New Interface between Copyright Law and Technology: How User-Generated Content Will Shape the Future of Online Distribution*, in *Bocconi Legal Studies Research Paper* No. 1275326, 2009, liberamente accessibile presso: «https://ssrn.com/abstract=1275326» (Ultimo accesso: 10 maggio 2022) o «http://dx.doi.org/10.2139/ssrn.1275326» (Ultimo accesso: 10 maggio 2022); M. L. MONTAGNANI, A. TRAPOVA, *New Obligations for Internet Intermediaries in the Digital Single Market — Safe Harbors in Turmoil?*, in *Journal of Internet Law*, Jan 2019, Vol. 22 Issue 7, p3-11. 9p., 2019, liberamente accessibile presso: «https://ssrn.com/abstract=3361073» (Ultimo accesso: 10 maggio 2022) o «http://dx.doi.org/10.2139/ssrn.3361073» (Ultimo accesso: 10 maggio 2022); M. L. MONTAGNANI, *A New Liability Regime for Illegal Content in the Digital Single Market Strategy*, in *SSRN*, liberamente accessibile presso: «https://ssrn.com/abstract=3398160» (Ultimo accesso: 10 maggio 2022) o «http://dx.doi.org/10.2139/ssrn.3398160» (Ultimo accesso: 10 maggio 2022); M. L. MONTAGNANI, *Virtues and Perils Of Algorithmic Enforcement and Content Regulation in The EU – A Toolkit For A Balanced Algorithmic Copyright Enforcement*, in *Case Western Reserve Journal of Law, Technology & the Internet*, Vol. 11, No. 1, 2020, *Bocconi Legal Studies Research Paper* No. 3767008, 2020, liberamente accessibile presso: «https://ssrn.com/abstract=3767008». (Ultimo accesso: 10 maggio 2022)

Come già affermato, i c.d "*hosting providers*"[555] possono andare esenti da responsabilità ove (i) non siano a conoscenza effettiva che il materiale o un'attività che utilizza il materiale sul sistema o sulla rete stia violando il *copyright*; (ii) in assenza di tale effettiva conoscenza, non sia a conoscenza di fatti o circostanze da cui risulti un'attività illecita; o (iii) dopo aver acquisito tale conoscenza o consapevolezza, agisca tempestivamente per rimuovere o disabilitare l'accesso al materiale. È inoltre necessario che tale *provider* (B) non percepisca un vantaggio finanziario direttamente attribuibile all'attività illecita, nel caso in cui il prestatore di servizi abbia il diritto e la capacità di controllare tale attività; e (C) alla notifica della presunta violazione, risponda tempestivamente per rimuovere, o disabilitare l'accesso al materiale che si ritiene essere in violazione del *copyright* o essere oggetto di attività illecita.

I *Safe Harbor* statunitensi, quindi, chiedono al *provider* di non essere a conoscenza dell'attività dell'utente attuata in violazione del diritto d'autore e quindi di attivarsi prontamente nel momento stesso in cui ricevono una notifica che indichi l'avvenuta violazione del *copyright*. La conoscenza da parte del *provider* è, come visto nel capitolo secondo, solitamente rinvenuta attraverso il c.d "*red flag test*". Esso si compone di una parte "oggettiva" ed una "soggettiva": la prima analizza se la violazione avrebbe potuto apparire evidente ad una persona ragionevole, la seconda guarda invece alla concreta conoscenza del *provider* dei fatti o delle circostanze. Ne consegue che il punto cruciale è quello di come e quanto il *provider* si curi dei contenuti sulla propria piattaforma: se non se ne cura non vi sarà alcuna responsabilità[556].

Nel capitolo secondo avevamo deciso di soprassedere rispetto al funzionamento tecnico del meccanismo di *notice and take down* per ragioni di economia espositiva. Tuttavia, ora si rende necessario ritornare sui nostri passi e analizzare il sistema americano da questa privilegiata visuale.

---

[555] 17 U.S.C. §512 (c), nel testo originale dispone che: "*A Service Provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the Service Provider, if the Service Provider— (A) (i) does not have actual knowledge that the material or an activity using the material on the system or network is infringing; (ii) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or (iii) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material; (B) does not receive a financial benefit directly attributable to the infringing activity, in a case in which the Service Provider has the right and ability to control such activity; and (C) upon notification of claimed infringement as described in paragraph (3), responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity".*

[556] Riferimento alla giurisprudenza sul punto può essere rinvenuto nei casi: 7 v. Corbis Corp. v. Amazon.com, Inc., 351 F. Supp. 2d 1090, (W.D. Wash. 2004), liberamente accessibile presso: «https://casetext.com/case/corbis-corporation-v-amazoncom-2» (Ultimo accesso: 10 maggio 2022); Perfect 10, Inc. v. CCBill LLC, 448. F.3d 1102 (9th Cir. 2007), liberamente accessibile presso: «https://casetext.com/case/perfect-10-inc-v-ccbill-llc» (Ultimo accesso: 10 maggio 2022); UMG Recordings, Inc. v. Veoh Networks, Inc., 665 F. Supp. 2d 1099, (C.D. Cal. 2009), liberamente accessibile presso: «https://casetext.com/case/umg-recordings-56» (Ultimo accesso: 10 maggio 2022); Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19, (2d Cir. 2012), liberamente accessibile presso: «https://cyber.harvard.edu/people/tfisher/cx/2012_Viacom.pdf» (Ultimo accesso: 10 maggio 2022). In questo ultimo caso la giurisprudenza ha affermato che vi è dunque *actual knowledge* quando il *provider* ha una conoscenza soggettiva di una specifica violazione, mentre vi è *red flag knowledge* quando la conoscenza dovrebbe derivare da fatti dai quali un soggetto ragionevole potrebbe oggettivamente comprendere la presenza di una violazione.

La notifica richiesta dai *Safe Harbor*, per essere efficace, deve contenere una serie di elementi[557]. In particolare, una notifica di presunta violazione deve essere una comunicazione scritta che include sostanzialmente quanto segue: (i) una firma fisica o elettronica di una persona autorizzata ad agire per conto del titolare di un diritto esclusivo presumibilmente violato; (ii) l'identificazione dell'opera protetta da *copyright* che si ritiene sia stata violata o, se più opere protette da *copyright* in un unico sito online sono coperte da un'unica notifica, un elenco rappresentativo di tali opere in quel sito; (iii) l'identificazione del materiale che si presume illecito o sia oggetto di attività illecita e che deve essere rimosso o l'accesso al quale deve essere disabilitato, e informazioni ragionevolmente sufficienti per consentire al fornitore di servizi di individuare il materiale; (iv) informazioni ragionevolmente sufficienti per consentire al fornitore di servizi di contattare la parte reclamante, come un indirizzo, un numero di telefono e, se disponibile, un indirizzo di posta elettronica al quale la parte reclamante può essere contattata; (v) una dichiarazione secondo cui la parte reclamante crede in buona fede che l'uso del materiale nel modo lamentato non sia autorizzato dal titolare del *copyright* o dalla legge; (vi) una dichiarazione che le informazioni contenute nella notifica sono esatte e, a pena di falsa testimonianza, che la parte attrice è autorizzata ad agire per conto del titolare di un diritto esclusivo presumibilmente violato.

La §512(c)(3)(B)(i) specifica che se tali requisiti non sono rispettati, la notifica non rileverà ai fini della determinazione della "effettiva conoscenza" dell'illecito. La § 512 (c)(3)(B)(ii) tuttavia chiarisce che, nel caso in cui la notifica non rispetti sostanzialmente tutte le condizioni, ma rispetti sostanzialmente le clausole (ii), (iii) e (iv) del comma (A), la clausola (B)(i) si applica solo se il fornitore di servizi ha prontamente cercato di contattare la persona che effettua la notifica o adotta altre misure ragionevoli per ricevere una notifica rispettosa di tutte le disposizioni della lettera (A). [558] Se dunque, anche a fronte di una notifica incompleta, il *provider* non si attiva per contattare l'istante, anche tale notifica incompleta sarà idonea a creare una *actual* o *apparent knowledge* del *provider* e di comportare la sua esclusione dai *Safe Harbor*[559].

---

[557] Nel testo della legislazione statunitense si legge: "*(A) To be effective under this subsection, a notification of claimed infringement must be a written communication provided to the designated agent of a Service Provider that includes substantially the following:*
(i) A physical or electronic signature of a person authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.
(ii) Identification of the copyrighted work claimed to have been infringed, or, if multiple copyrighted works at a single online site are covered by a single notification, a representative list of such works at that site.
(iii) Identification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the Service Provider to locate the material.
(iv) Information reasonably sufficient to permit the Service Provider to contact the complaining party, such as an address, telephone number, and, if available, an electronic mail address at which the complaining party may be contacted.
(v) A statement that the complaining party has a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law".
(vi) A statement that the information in the notification is accurate, and under penalty of perjury, that the complaining party is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed".

[558] "*(i) Subject to clause (ii), a notification from a copyright owner or from a person authorized to act on behalf of the copyright owner that fails to comply substantially with the provisions of subparagraph (A) shall not be considered under paragraph (1)(A) in determining whether a service provider has actual knowledge or is aware of facts or circumstances from which infringing activity is apparent.*
(ii) In a case in which the notification that is provided to the service provider's designated agent fails to comply substantially with all the provisions of subparagraph (A) but substantially complies with clauses (ii), (iii), and (iv) of subparagraph (A), clause (i) of this subparagraph applies only if the service provider promptly attempts to contact the person making the notification or takes other reasonable steps to assist in the receipt of notification that substantially complies with all the provisions of subparagraph (A)".

[559] In questo senso si esprime anche L. CAMARELLA, *La responsabilità dell'Internet Service Provider alla luce della nuova Direttiva sul diritto d'autore nel mercato unico digitale*, cit.; ulteriori informazioni rinvenibili altresì presso: G. CASSANO;

Una volta dunque ricevuta la notifica, corredata di tutti gli elementi richiesti dalla normativa in commento, il *provider*, per poter beneficiare della copertura dei *safe harbors*, deve attivarsi per disabilitare l'accesso al contenuto o rimuovere lo stesso: quella parte della definizione che va sotto il nome di "*take down*". Rimosso il materiale, il *provider* deve rendere edotto l'utente il cui contenuto è stato cancellato della avvenuta operazione, consentendo quindi allo stesso di procedere con una eventuale "*counternotification*", opponendosi alla rimozione.

La Section §512 (g)(3)[560] in merito dispone che per essere efficace una contro-notifica deve essere una comunicazione scritta che include sostanzialmente quanto segue: (A) una firma fisica o elettronica dell'abbonato (B) l'identificazione del materiale che è stato rimosso o al quale è stato disabilitato l'accesso e il luogo in cui il materiale è apparso prima che fosse rimosso o l'accesso ad esso fosse disabilitato (C) una dichiarazione sotto pena di falsa testimonianza che l'abbonato ritiene in buona fede che il materiale sia stato rimosso o disattivato a causa di un errore o di un'identificazione errata del materiale da rimuovere o disabilitare (D) il nome, l'indirizzo e il numero di telefono dell'abbonato e una dichiarazione che l'abbonato acconsente alla giurisdizione del tribunale distrettuale federale per il distretto giudiziario in cui si trova l'indirizzo, o se l'indirizzo dell'abbonato è al di fuori degli Stati Uniti, per qualsiasi distretto giudiziario in cui si trova il fornitore di servizi e che l'abbonato accetterà la notifica del processo dalla persona che ha fornito la notifica ai sensi della sottosezione (c)(1)(C).

Ricevuta l'eventuale *counternotification* il *provider* dovrà trasmetterne copia al titolare dei diritti d'autore, contestualmente avvisando lo stesso del rispristino del materiale oggetto di contro-notifica. Nelle more del rispristino del materiale il titolare del diritto d'autore può tuttavia presentare un'azione giudiziale contro l'utente per ottenere l'affermazione del proprio diritto e la conseguente cessazione dell'illecito perpetrato, ove accertato tale[561].

La procedura di *notice and take down* prevista dal DMCA, tuttavia, è da più parti vista come obsoleta. In questo, un recente contributo ha affermato proprio che rispetto al momento dell'adozione di questa disciplina, "*Internet è cresciuto ed è cambiato in un modo che il Congresso non avrebbe potuto facilmente prevedere all'epoca dell'approvazione del DMCA. Google è stato lanciato nel 1998, anno in cui è stata approvata la § 512. Napster nacque nel 1999, con altre reti peer-to-*

F. BUFFA, *Responsabilità del content provider e dell'host provider*, cit., 77-81; M. LEISTNER, *European Copyright Licensing and Infringement Liability Under Art. 17 DSM-Directive Compared to Secondary Liability of Content Platforms in the U.S. – Can We Make the New European System a Global Opportunity Instead of a Local Challenge?*, cit.

560 "*To be effective under this subsection, a counter notification must be a written communication provided to the service provider's designated agent that includes substantially the following:*
(A) A physical or electronic signature of the subscriber.
(B) Identification of the material that has been removed or to which access has been disabled and the location at which the material appeared before it was removed or access to it was disabled.
(C) A statement under penalty of perjury that the subscriber has a good faith belief that the material was removed or disabled as a result of mistake or misidentification of the material to be removed or disabled.
(D) The subscriber's name, address, and telephone number, and a statement that the subscriber consents to the jurisdiction of Federal District Court for the judicial district in which the address is located, or if the subscriber's address is outside of the United States, for any judicial district in which the service provider may be found, and that the subscriber will accept service of process from the person who provided notification under subsection (c)(1)(C) or an agent of such person".

561 J.M. URBAN, J. KARAGANIS, B.L. SCHOFIELD, *Notice and takedown in everyday practice, Version 2*, in *SSRN*, 2017, disponibile al link «https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2755628» (Ultimo accesso: 10 maggio 2022); Per un dettagliato approfondimento dei meccanismi di *notice and action* si faccia riferimento ad A. KUCZERAWY, *From 'Notice and take down' to 'Notice and Stay Down': Risks and Safeguards for Freedom of Expression* (dicembre 19, 2018) in G. FROSIO (ed), The Oxford Handbook of Intermediary Liability Online, 2019, liberamente accessibile presso: «https://ssrn.com/abstract=3305153» (Ultimo accesso: 10 maggio 2022).

peer, un modello tecnologico non previsto né prevedibile dal DMCA. Successivamente sono emersi Facebook e altri social network, insieme a YouTube e altre piattaforme. Per i principali titolari di diritti che affrontano violazioni su vasta scala, anche l'enforcement del copyright è cambiato. Questi grandi titolari dei diritti hanno cominciato ad utilizzare procedimenti automatizzati per rilevare infrazioni e generare automaticamente avvisi di rimozione. L'automazione è sicuramente un aspetto inevitabile di fronte a violazioni su vasta scala, ma anche i processi decisionali basati su macchine sollevano domande sulla qualità e sull'adeguatezza degli avvisi. E mentre i titolari di diritti di grandi dimensioni possono permettersi di ricorrere a questi metodi per gestire le violazioni online, i titolari di diritti più piccoli possono avere difficoltà a farli valere"[562].

Nel 2020 il Copyright Office statunitense, commentando in merito alla §512 del DMCA riporta che per la maggior parte dei titolari di copyright, la sezione 512 non fornisce in realtà un mezzo efficace per arginare le attività illecite sul web. In questo senso, alcuni commentatori sottolineano gli oneri e le inefficienze sostanziali derivanti dalla necessità di generare e inviare un numero enorme di avvisi di rimozione agli ISP. Per esempio, la MPAA osservava che "*nell'anno solare 2015, i [suoi] membri hanno inviato avvisi in merito a oltre 104,2 milioni di URL illeciti*". La Copyright Alliance descrive il numero di avvisi di rimozione come "*sbalorditivo, e . . . in costante aumento*", poiché le parti interessate sono "*alle prese con decine di milioni di avvisi all'anno*". Sony Music riferiva poi che le sue registrazioni erano state oggetto di oltre 5,7 milioni di avvisi di rimozione nel 2015. Allo stesso modo, Songwriters of North America ("SONA") cita un rapporto del 2013 che indicava che i titolari dei diritti d'autore inviavano avvisi di rimozione ogni mese "per oltre 6,5 milioni di file illeciti, disponibili su oltre 30.000 siti Web"[563].

Stante l'inefficienza del Sistema statunitense, da più parti declamata, alcune recenti proposte vorrebbero far propendere anche il Congresso statunitense per una riforma che viri verso un meccanismo di "notice and stay down". Il Copyright Office in particolare ricorda che l'argomentazione principale dei titolari di diritti a favore dell'adozione di un requisito di "stay down" è che un tale approccio è necessario per affrontare il c.d "*whack-a-mole problem*": la ricomparsa su un servizio (spesso in breve tempo) di contenuti che erano già stati oggetto di un avviso di rimozione. Il presupposto da cui parte l'analisi è quella di imporre un requisito di "stay down" attraverso mezzi tecnologici, sia tramite un sistema di filtraggio dei contenuti *sui generis* sviluppato da tale ISP, come il *Content ID* di *YouTube* o con tecnologie di filtraggio standard, come quella offerta da Audible Magic.[564]

Il modello del *notice and stay down* pare allora essere stato preso ad ispirazione per il confezionamento dell'art. 17 della Direttiva 2019/790. L'ordinamento europeo, prima dell'avvento della Direttiva in commento, prevedeva nel sistema creato dalla Direttiva e-commerce un meccanismo simile al *notice and take down*, sebbene meno particolareggiato e dettagliato della procedura statunitense.

Il Considerando 46 della Direttiva e-commerce stabiliva in merito proprio che per godere di una limitazione della responsabilità, un *provider* dovesse agire immediatamente per rimuovere le informazioni o per disabilitare l'accesso alle medesime non appena fosse stato informato o si rendesse conto delle attività illecite. La rimozione delle informazioni o la disabilitazione dell'accesso alle medesime avrebbero dovuto essere effettuate nel rispetto del

---

562 L. CAMARELLA, *La responsabilità dell'Internet Service Provider alla luce della nuova Direttiva sul diritto d'autore nel mercato unico digitale*, cit., 211 e ss.

563 Per maggiori riferimenti in merito si veda: United States Copyright Office, *Section 512 of Title 17, A Report Of The Register Of Copyrights*, cit., 79 e ss, ove sono rinvenibili ulteriori dati statistici di riferimento.

564 Per maggiori riferimenti in merito alla proposta statunitense di passare ad un sistema di notice and stay down si veda: United States Copyright Office, *Section 512 of Title 17, A Report Of The Register Of Copyrights*, cit., 164 e ss.

principio della libertà di espressione e delle procedure all'uopo previste a livello nazionale. Il più volte ricordato art. 14 chiedeva poi agli *hosting provider* di agire "*immediatamente per rimuovere le informazioni o per disabilitarne l'accesso*" ove si fosse riscontrata una attività illecita ed il *provider* avesse voluto andare esente da responsabilità.

Pare allora necessario indagare quali novità investono il panorama europeo ove siano coinvolte le attività di cui alla lettera c) del paragrafo quarto dell'art. 17, ricordando comunque che esso non pregiudica la possibile applicazione dell'articolo 14, paragrafo 1, della Direttiva 2000/31/CE a tali prestatori di servizi per finalità che non rientrano nell'ambito di applicazione della Direttiva in commento.

5.3.3. Notice and stay down

L'art. 17 chiede sicuramente di agire tempestivamente, dopo aver ricevuto una segnalazione sufficientemente motivata dai titolari dei diritti, per disabilitare l'accesso o rimuovere dai loro siti web le opere illecitamente condivise, in ciò in linea con il sistema di *notice and take down* previamente richiesto. Aggiunge tuttavia un ulteriore obbligo giuridico in capo al *provider* consistente nel compiere i massimi sforzi per impedirne il caricamento in futuro, ossia imponendo un obbligo di "*rimozione permanente*".

Un sistema di *notice and stay down*, come nota parte della dottrina, propone una forma responsabilità del fornitore di servizi volta ad assicurare che sia impedita la ricomparsa dello stesso o di un simile contenuto già ritenuto e segnalato come illecito. In un quadro di questo genere, un avviso di rimozione da parte di un titolare dei diritti generalmente comporterebbe l'obbligo per il fornitore di servizi di identificare e rimuovere proattivamente tutti i contenuti illeciti e prevenire quindi caricamenti futuri. I fornitori di servizi, in questo, dovrebbero chiaramente fare affidamento sulla tecnologia, come vari sistemi di filtraggio, per adempiere agli obblighi imposti dalla normativa.[565]

La Commissione, nelle sue linee guida, individua una serie di possibili scenari in cui un tale obbligo giuridico potrebbe sorgere. Il primo caso è quello in cui "*i titolari dei diritti non hanno fornito in anticipo ai prestatori di servizi di condivisione di contenuti online le informazioni "pertinenti e necessarie" di cui all'articolo 17, paragrafo 4, lettera b), per evitare che i contenuti non autorizzati siano resi disponibili. Agiscono ex post, una volta che un determinato contenuto è diventato disponibile, per chiederne la rimozione permanente*". Una seconda possibilità è quando "*i prestatori di servizi di condivisione di contenuti online si sono adoperati al meglio per assicurare che non siano disponibili contenuti non autorizzati a norma dell'articolo 17, paragrafo 4, lettera b), ma nonostante tali sforzi i contenuti non autorizzati sono divenuti disponibili per ragioni oggettive, ad esempio nel caso in cui alcuni contenuti non possano essere riconosciuti a causa di limitazioni tecnologiche intrinseche".* Infine, in alcuni casi specifici ci si può attendere che i prestatori di servizi di condivisione di contenuti online agiscano solo una volta ricevuta la segnalazione da parte dei titolari dei diritti. Questi casi sono per esempio quelli

[565] Per maggiori riferimenti in merito all'analisi dei sistemi di notice and stay down, con riferimenti comparati al sistema statunitense del Notice and Take down si veda: United States Copyright Office, *Section 512 of Title 17, A Report Of The Register Of Copyrights*, cit. 42 e ss., in cui si afferma che: "*A notice-and-staydown system essentially collapses the steps discussed above under the other notice systems into a single responsibility of the service provider to prevent the reappearance of the same or similar infringing content. Under a notice-and-staydown framework, a takedown notice from a rightsholder generally triggers a duty for the service provider to proactively identify and remove all instances of the infringing content and prevent future uploads. Service providers have depended on technology, such as various filtering systems, in order to meet the obligations under this duty.*"

indicati al Considerando 66, ossia le ipotesi in cui manchino, per avventura, tecnologie idonee per arginare simili condivisioni su quei particolari contenuti, allo stato dell'arte[566].

Anche in questo caso, affinché l'obbligazione di rimozione permanente si possa verificare, al pari della lettera b), anche la lettera c) richiede che vengano fornite al *provider* sufficienti informazioni per adempiere. Le linee guida della Commissione sul punto affermano che nell'attuare l'articolo 17, paragrafo 4, lettera c), "*gli Stati membri devono differenziare chiaramente il tipo di informazioni che i titolari dei diritti forniscono in una "segnalazione sufficientemente motivata" per la rimozione dei contenuti (la parte relativa alla "rimozione" di cui alla lettera c)) dalle "informazioni pertinenti e necessarie" che forniscono per impedire futuri caricamenti di opere oggetto di segnalazione (la parte relativa alla "rimozione permanente" di cui alla lettera c), che rinvia alla lettera b))*".

La Commissione, nel valutare quali siano le informazioni necessarie a questi fini compie un rimando ad una propria precedente raccomandazione[567], affermandone la applicabilità, *per relationem*, anche al caso di specie. In particolare, ai sensi di tale comunicazione, le segnalazioni dovrebbero essere adeguatamente motivate e sufficientemente precise da consentire al *provider* di prendere una decisione coscienziosa e informata riguardo ai contenuti cui si riferisce la segnalazione, in particolare per stabilire se tali contenuti debbano essere considerati illegali e debbano essere rimossi o se l'accesso ai medesimi debba essere disabilitato. Tali segnalazioni allora, secondo la Commissione, dovrebbero contenere una spiegazione dei motivi per i quali l'autore della stessa ritiene che i contenuti in questione siano illegali e una chiara indicazione circa l'ubicazione di tali contenuti. *Per relationem*, si potrebbe affermare anche che il *provider*, qualora sia a conoscenza dei recapiti dell'autore della segnalazione, dovrebbe inviare una conferma di ricevimento all'autore della segnalazione e informarlo senza indebito ritardo e in modo proporzionato della propria decisione relativa ai contenuti cui si riferisce la segnalazione.

Il punto principale della disposizione è tuttavia quello concernente l'obbligo di "rimozione permanente", previsto dalla seconda parte dell'articolo 17, paragrafo 4, lettera c). Questo impone ai prestatori di servizi di adoperarsi al meglio per impedire il futuro caricamento di opere o altri materiali segnalati dai titolari dei diritti. Questa disposizione compie un rimando alla lettera b) dello stesso paragrafo; ciò significa che, come segnala la Commissione, per permettere ai prestatori di servizi di adoperarsi al meglio per evitare futuri caricamenti a norma di tale disposizione, i titolari dei diritti devono fornire loro lo stesso tipo di informazioni "pertinenti e necessarie" utilizzate per dare applicazione alla lettera b). Ciò implica ad esempio che, se un prestatore di servizi utilizza tecnologie di *fingerprinting* per evitare futuri caricamenti di opere oggetto di segnalazione, il fatto di ricevere unicamente le informazioni fornite nella segnalazione non sarebbe sufficiente[568].

La Corte di Giustizia, pronunciandosi recentemente sulla validità dell'articolo 17 della direttiva in commento, ha altresì colto l'occasione per confermare la lettura data dell'obbligo

---

[566] Communication From The Commission To The European Parliament And The Council: Guidance on Article 17 of Directive 2019/790 on Copyright in the Digital Single Market COM/2021/288 final, cit.

[567] Comunicazione della Commissione del 1° marzo 2018, disponibile all'indirizzo: «https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32018H0334&from=IT» (Ultimo accesso: 10 maggio 2022).

[568] Communication From The Commission To The European Parliament And The Council: Guidance on Article 17 of Directive 2019/790 on Copyright in the Digital Single Market COM/2021/288 final, cit.; si veda altresì: M. LEISTNER, *European Copyright Licensing and Infringement Liability Under Art. 17 DSM-Directive Compared to Secondary Liability of Content Platforms in the U.S. – Can We Make the New European System a Global Opportunity Instead of a Local Challenge?*, cit.

di *notice and stay down*. In particolare la Corte ha osservato che "*gli obblighi incombenti ai fornitori di servizi di condivisione di contenuti online non si limitano all'obbligo previsto all'inizio dell'articolo 17, paragrafo 4, lettera c), della direttiva 2019/790, corrispondente a quello che incombeva loro già in applicazione dell'articolo 14, paragrafo 1, lettera b), della direttiva 2000/31 e consistente nel dovere di agire immediatamente, non appena ricevuta una segnalazione sufficientemente motivata dai titolari di diritti, per disabilitare l'accesso ai contenuti protetti oggetto della segnalazione o per ritirarli dalle loro piattaforme*". La Corte nota, infatti, che oltre alla sussistenza di un obbligo di *notice and take down*, sussiste un obbligo in capo ai provider di, "*in applicazione dell'articolo 17, paragrafo 4, lettera c), in fine, della direttiva 2019/790, compiere «i massimi sforzi per impedirne il caricamento in futuro conformemente alla lettera b)» di tale disposizione*", riferendo simile obbligo a quei "contenuti protetti che sono stati oggetto, a seguito della loro messa a disposizione del pubblico, di una segnalazione sufficientemente motivata da parte dei titolari dei diritti"[569].

In ogni caso, anche qui le declamazioni di tutela degli utenti e dei loro dati non si fanno attendere. Il legislatore europeo costantemente ricorda che gli Stati membri dovrebbero tenere presente che l'applicazione dell'articolo 17 non deve comportare alcun obbligo generale di sorveglianza, come stabilito al paragrafo 8 dello stesso. Eppure, i meccanismi di *Automatic Content Recognition*, come visto nel capitolo precedente, impongono una sorveglianza del web, in grado, come tale, di incidere sui diritti degli utenti.

6. La necessità di bilanciamento: inquadramento dei problemi

Il quesito che deve porsi l'interprete dinnanzi alla disciplina così delineata dall'art.17 della Direttiva 2019/790 concerne la sua compatibilità con due aspetti essenziali ai fini della presente opera. Sin dalle prime pagine del presente elaborato, la dimensione del *copyright* si è sempre affermato dovesse essere bilanciata con altrettante esigenze e diritti. Anche in questo caso le considerazioni devono essere del medesimo tenore,

Come ricordano Giorgio Resta e Guido Alpa, in più occasioni la Corte di Giustizia ha affermato che ove si applichi il diritto dell'UE si applicano anche i diritti fondamentali che esso garantisce. Gli autori ricordano in particolare la sentenza resa nel caso Åkerberg Fransson[570] in cui la Corte ha confermato che, dato che i diritti fondamentali garantiti dalla Carta devono essere rispettati quando una normativa nazionale rientra nell'ambito di applicazione del diritto dell'Unione, non possono esistere casi rientranti nel diritto dell'Unione senza che tali diritti fondamentali trovino applicazione. Questo significa quindi che l'applicabilità del diritto dell'Unione implica quella dei diritti fondamentali garantiti dalla Carta. [571] Le medesime conclusioni sono rafforzate, nell'ambito dell'analisi dell'articolo 17 in commento dal fatto che è la stessa Direttiva ad imporre all'interprete di ragionare in chiave di bilanciamento.

---

[569] CGUE 26 aprile 2022, C-401/2019, Repubblica di Polonia contro Parlamento europeo, Consiglio dell'Unione europea, par. 50-52 liberamente accessibile presso: «https://curia.europa.eu/juris/document/document.jsf?text=&docid=258261&pageIndex=0&doclang=IT&mode=req&dir=&occ=first&part=1&cid=10742191». (Ultimo accesso: 10 maggio 2022).

[570] CGUE 26 febbraio 2013, C-617/10, *Åkerberg Fransson*, liberamente accessibile presso: «https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:62010CJ0617&from=IT» (Ultimo accesso: 10 maggio 2022).

[571] Per maggiori informazioni sulle decisioni algoritmiche ed il rapporto che queste istaurano con la normativa a tutela dei dati personali si veda G. ALPA, G. RESTA, *Le persone e la Famiglia 1, Le persone fisiche e i diritti della personalità*, cit., 116.

È possibile affermare questo sulla base innanzitutto del Considerando 84 della Direttiva in cui si afferma, retoricamente, che "*la presente Direttiva rispetta i diritti fondamentali e osserva i principi riconosciuti segnatamente dalla Carta. Di conseguenza essa andrebbe interpretata e applicata conformemente a tali diritti e principi*". Al di là della petizione di principio di un supposto rispetto dei diritti fondamentali stabiliti dalla Carta di Nizza, l'interprete è tenuto ad indagare se sia veramente il caso di affermare una compatibilità della disciplina. Lo stesso art.17, al decimo paragrafo, ripropone la stessa considerazione, affermando che "*nel discutere le migliori prassi, si tiene specialmente conto, tra l'altro, della necessità di pervenire a un equilibrio tra i diritti fondamentali e il ricorso a eccezioni e limitazioni. Ai fini del dialogo con le parti interessate, le organizzazioni di utenti hanno accesso a informazioni adeguate fornite dai prestatori di servizi di condivisione di contenuti online sul funzionamento delle loro prassi in relazione al paragrafo 4*". Tale istanza è confermata poi anche dal Considerando 70 che, nell'affermare che gli utenti dovrebbero avere la possibilità di godere delle eccezioni e limitazioni al diritto d'autore, giunge a statuire che questo sia importante proprio al fine di "*raggiungere un equilibrio tra i diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea («Carta»), in particolare la libertà di espressione e la libertà delle arti, e il diritto di proprietà, inclusa la proprietà intellettuale*".

Il raggiungimento di un equilibrio fra diritti fondamentali che viene quindi copiosamente richiesto dalla Direttiva stessa deve essere letto alla luce del paragrafo quinto dell'art. 17 che, nel fare riferimento al principio di proporzionalità, indirettamente richiama l'attenzione dell'interprete all'art. 52 della Carta di Nizza[572]. Quest'ultimo, nel definire la "portata dei diritti" garantiti dalla Carta medesima afferma che "*eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla presente Carta devono essere previste dalla legge e rispettare il contenuto essenziale di detti diritti e libertà. Nel rispetto del principio di proporzionalità, possono essere apportate limitazioni solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui*". Le condizioni di tali possibili limitazioni devono quindi essere indagate nel presente elaborato.

Si consideri in ogni caso che, sulla base dell'articolo 51 della Carta, tutte le sue disposizioni si applicano alle Istituzioni e agli Organi dell'Unione nel rispetto del principio di sussidiarietà, come pure agli Stati membri esclusivamente nell'attuazione del diritto dell'Unione. Pertanto, i suddetti soggetti devono rispettarne i diritti, osservarne i principi e promuoverne l'applicazione secondo le rispettive competenze.

In secondo luogo, o meglio, in specificazione di questo primo punto, l'analisi qui proposta deve indagare non solo la compatibilità con i diritti fondamentali previsti dalla Carta, tra cui, ex artt. 7 ed 8 della stessa, il diritto alla vita privata, ma anche una loro specifica estrinsecazione costituita dalla compatibilità della presente disciplina con quella in merito al trattamento dei dati personali contenuta nel Regolamento UE 679/2018.

Anche in questo secondo punto siamo incoraggiati nella nostra analisi dalla Direttiva stessa la quale al Considerando 85 si pronuncia nel senso che "*qualsiasi trattamento dei dati personali a norma della presente Direttiva dovrebbe rispettare i diritti fondamentali, compresi il diritto al rispetto della vita privata e della vita familiare e il diritto alla protezione dei dati di carattere personale di cui agli articoli 7 e 8 della Carta e deve essere conforme alla Direttiva 2002/58/CE e al regolamento (UE) 2016/679*". Tale presa di posizione viene ribadita anche dal Considerando 70 che stabilisce

[572] Per una attenta analisi del delicato bilanciamento in commento ed un chiaro riferimento alla casistica euro-italiana si faccia riferimento a C. SGANGA, *A Decade of Fair Balance Doctrine, and How to Fix It: Copyright Versus Fundamental Rights Before the CJEU from Promusicae to Funke Medien, Pelham and Spiegel Online,* cit.. Si veda inoltre C. SGANGA, *A New Era for EU Copyright Exceptions and Limitations? Judicial Flexibility and Legislative Discretion in the Aftermath of the CDSM Directive and the Trio of the Grand Chamber of the CJEU,* cit.

proprio che la cooperazione fra titolari dei diritti d'autore e gli OCSSP non dovrebbe comportare l'identificazione dei singoli utenti né il trattamento dei loro dati personali, salvo conformemente alla Direttiva 2002/58/CE e al Regolamento (UE) 2016/679, nella sostanza riproponendo il medesimo fraseggio del nono paragrafo dell'articolo 17.

L'interprete quindi, nell'interrogarsi su questi punti controversi, dovrebbe essere anche consapevole delle possibili conseguenze di una normativa non conforme a quanto delineato dalla Carta o dai Trattati, che, per inciso, si ricordano avere lo stesso valore[573].

Il Trattato sul Funzionamento dell'Unione Europea prevede in questo senso almeno due norme che si attagliano rigorosamente alla situazione in esame. L'art. 263 TFUE in questo senso dispone che la Corte di Giustizia dell'Unione europea esercita un controllo di legittimità sugli atti legislativi destinati a produrre effetti giuridici nei confronti di terzi, potendo pronunciarsi, in particolare, sulla violazione delle forme sostanziali, violazione dei trattati o di qualsiasi regola di diritto relativa alla loro applicazione. Tali ricorsi possono essere proposti da uno Stato membro, dal Parlamento europeo, dal Consiglio o dalla Commissione, non quindi dal cittadino comune. Ai sensi dell'articolo seguente poi, se il ricorso è fondato, la Corte di Giustizia dell'Unione europea dichiara nullo e non avvenuto l'atto impugnato, eventualmente precisando gli effetti dello stesso che devono essere considerati definitivi.

L'alternativa a tale previsione è data dal rinvio pregiudiziale alla Corte di Giustizia ex art. 267 del TFUE, in particolare sotto il rispetto della lettera b) del citato articolo, comprendente le censure di "*validità e l'interpretazione degli atti compiuti dalle istituzioni, dagli organi o dagli organismi dell'Unione*".

Anticipando quanto farà seguito al presente paragrafo, probabilmente l'art. 17, almeno per come oggi è formulato, mostra dei profili di decisa incompatibilità con il resto del panorama europeo, potendosi paventare una censura di invalidità dello stesso in merito alla violazione dei diritti fondamentali degli utenti. Tale articolo è stato criticato già da molta parte della dottrina[574] e non è un caso che uno degli Stati membri europei abbia già

---

[573] Così infatti dispone il TUE, come riformato in seguito al Trattato di Lisbona, il cui articolo sesto oggi stabilisce in merito che "1. *L'Unione riconosce i diritti, le libertà e i principi sanciti nella Carta dei diritti fondamentali dell'Unione europea del 7 dicembre 2000, adattata il 12 dicembre 2007 a Strasburgo, che ha lo stesso valore giuridico dei trattati. Le disposizioni della Carta non estendono in alcun modo le competenze dell'Unione definite nei trattati.*
I diritti, le libertà e i principi della Carta sono interpretati in conformità delle disposizioni generali del titolo VII della Carta che disciplinano la sua interpretazione e applicazione e tenendo in debito conto le spiegazioni cui si fa riferimento nella Carta, che indicano le fonti di tali disposizioni.
2. L'Unione aderisce alla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali. Tale adesione non modifica le competenze dell'Unione definite nei trattati.
3. I diritti fondamentali, garantiti dalla Convenzione europea per la salvaguardia dei diritti del- l'uomo e delle libertà fondamentali e risultanti dalle tradizioni costituzionali comuni agli Stati membri, fanno parte del diritto dell'Unione in quanto principi generali."

[574] Si vedano per esempio F. ROMERO MORENO, '*Upload filters' and human rights: implementing Article 17 of the Directive on Copyright in the Digital Single Market*, 34(2) International Review of Law, Computers & Technology (2020), 153-182, liberamente accessibile presso «https://www.tandfonline.com/doi/full/10.1080/13600869.2020.1733760» (Ultimo accesso: 10 maggio 2022); C. ANGELOPOULOS, & J. P. QUINTAIS, *Fixing Copyright Reform: A Better Solution to Online Infringement,* 10(2) Journal of Intellectual Property, Information Technology and E-Commerce Law (2019), 147-172,, M. LEISTNER, *European Copyright Licensing and Infringement Liability Under Art. 17 DSM-Directive Compared to Secondary Liability of Content Platforms in the U.S. – Can We Make the New European System a Global Opportunity Instead of a Local Challenge?*, cit., J. REDA, J. SELINGER, & M. SERVATIUS, *Article 17 of the Directive on Copyright in the Digital Single Market: a Fundamental Rights Assessment (Study for Gesellschaft für Freiheitsrechte*), (December 2020), liberamente accessibile presso «https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3732223» (Ultimo accesso: 10 maggio 2022); M. SENFTLEBEN, & C. ANGELOPOULOS, *The Odyssey of the Prohibition on General Monitoring Obligations on the Way to the Digital Services Act: Between Article 15 of the E- Commerce Directive and Article 17 of the Directive on Copyright in the Digital Single Market* (October 22, 2020), liberamente accessibile presso:

provveduto a censurare l'articolo in commento, proponendo un ricorso per nullità dell'art. 17 della Direttiva dinnanzi alla Corte di Giustizia europea[575]. La Corte, tuttavia, con motivazione apodittica e priva di un efficace riscontro con la realtà tecnologica ed economica di cui si darà contezza nelle pagine seguenti, ha recentemente deciso il ricorso ribadendo la piena validità dell'articolo in commento, senza tuttavia che pregnanti considerazioni giuridiche siano state addotte a giustificazione di una presa di posizione che pare voler salvare a tutti i costi una disciplina giuridica, quale l'articolo 17 in commento, che, per ciò che sottende e prevedibilmente comporterà sul piano pratico, appare più pericolosa che utile[576].

La questione che si dimostra più critica, come vedremo sulla base delle considerazioni che seguiranno, è data dal fatto che, sebbene l'articolo 17 affermi al paragrafo ottavo che "*l'applicazione del presente articolo non comporta alcun obbligo generale di sorveglianza*", così non pare essere nei fatti. Le parole del legislatore europeo vengono tradite dallo stesso quando chiede alle piattaforme di condivisione di contenuti online di compiere i massimi sforzi per impedire che opere protette dal diritto d'autore vengano condivise sulle proprie piattaforme in assenza di autorizzazione. Tale obbligazione, esplicazione delle istanze di *enforcement* del diritto d'autore, non può estrinsecarsi in altro modo, come ampiamente affermato, se non per mezzo di meccanismi di filtraggio dei contenuti che per loro stessa natura impongono nei fatti un obbligo di monitoraggio costante del web. È una contraddizione insolvibile nel testo della legge che porta, interpretativamente, ad essere abbastanza sicuri quando si afferma che il paragrafo 8 è vuoto di significato.

Una parte della dottrina ha ritenuto altresì istruttivo esaminare la storia legislativa dell'art. 17 per meglio comprendere il suo rapporto con gli artt. 14 e 15 della Direttiva sul commercio elettronico. Il *Council's Legal Service*, in commento alla proposta di direttiva, aveva infatti osservato che non esisterebbe alcuna gerarchia tra atti legislativi secondari, quali gli articoli richiamati delle direttive in commento, ed il loro rapporto sarebbe disciplinato secondo i principi della *"lex specialis derogat legi generali"* e *"lex posteriori derogat legi priori"*. Sulla base di questa logica aveva ritenuto che l'introduzione delle misure previste dall'allora art. 13 della proposta della Commissione non fossero giuridicamente problematiche, e che avrebbero dovuto essere considerate come una *lex specialis*. Il *Council's Legal Service* sembrava, tuttavia, secondo parte della dottrina, evitare il principio secondo il quale anche la *lex posteriori* o la *lex specialis* deve trovare un giusto equilibrio tra diritti fondamentali concorrenti[577].

«https://ssrn.com/abstract=3717022» (Ultimo accesso: 10 maggio 2022), ALAI, DRAFT OPINION on certain aspects of the implementation of Article 17 of Directive (EU) 2019/790 of 17 April 2019 on *copyright* and related rights in the digital single market, liberamente accessibile presso: «https://www.alai.org/en/assets/files/resolutions/200330-opinion-article-17- directive-2019_790-en.pdf» (Ultimo accesso: 10 maggio 2022); ALAI, DRAFT OPINION on certain aspects of the implementation of Article 17 of Directive (EU) 2019/790 of 17 April 2019 on *copyright* and related rights in the digital single market, liberamente accessibile presso: «https://www.alai.org/en/assets/files/resolutions/200330-opinion-article-17-directive- 2019_790-en.pdf» (Ultimo accesso: 10 maggio 2022).

[575]Ricorso proposto il 24 maggio 2019 — Repubblica di Polonia/Parlamento europeo e Consiglio dell'Unione europea (Causa C-401/19), liberamente consultabile presso: «https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:62019CN0401&from=EN» (Ultimo accesso: 10 maggio 2022).

[576] CGUE 26 aprile 2022, C-401/2019, Repubblica di Polonia contro Parlamento europeo, Consiglio dell'Unione europea, cit.

[577] J. P. QUINTAIS, P. MEZEI, I. HARKAI, J. C. MAGALHÃES, C. KATZENBACH, S. F. SCHWEMER, & T. RIIS, *Final Report on mapping of EU legal framework and intermediaries' practices on copyright content moderation and removal*, 2022, cit., 58.

Come visto nel capitolo secondo, la Corte di Giustizia, con i casi Scarlet Extended v. Sabam[578] e Sabam v. Netlog[579], aveva messo fuori gioco nel panorama europeo qualsiasi obbligo di monitoraggio da parte degli Internet Service Provider, avendo ritenuto che una simile obbligazione fosse contraria al diritto europeo ed in particolare incompatibile con i diritti fondamentali sanciti dalla Carta di Nizza[580]. Tre erano stati i punti toccati da questa giurisprudenza: la libertà di impresa dei *provider*, la libertà di espressione degli utenti e la tutela della privacy degli stessi. Per rispetto, e per un certo qual ossequio nei confronti del legislatore europeo, non è intenzione di questo elaborato accusarlo velatamente di codardia; tuttavia, sicuramente gli si può contestare un'opacità nel formalmente chinare il capo dinnanzi alle statuizioni della Corte di Giustizia, proclamando a chiare lettere l'insussistenza di qualsiasi obbligo di sorveglianza, per poi però farlo riemergere nella disciplina del paragrafo quarto dell'articolo 17. Tanto è confermato dallo stesso Avvocato Generale Henrik Saugmandsgaard Øe che si esprime affermando: "*non vedo con quali mezzi, se non con l'utilizzo di uno strumento di riconoscimento automatico che consente loro di filtrare i contenuti caricati sui loro servizi, tali prestatori potrebbero ragionevolmente «assicurare che non siano disponibili» opere e materiali protetti identificati dai titolari dei diritti e «impedirne il caricamento in futuro» […] Mi sembra che le disposizioni […] effettivamente obblighino i prestatori di servizi di condivisione, in numerose situazioni, ad utilizzare tali strumenti di riconoscimento di contenuto. A mio avviso, il legislatore dell'Unione ha semplicemente cambiato metodo fra la proposta di direttiva e la sua adozione quale direttiva 2019/790. Piuttosto che prevedere direttamente un obbligo di predisporre tali strumenti, esso li ha imposti indirettamente, tramite le condizioni di esenzione da responsabilità previste a tali disposizioni*".[581]

7. Compatibilità con i diritti fondamentali

Si è più volte avuto modo di dimostrare, nel corso dei capitoli precedenti, che il diritto d'autore non è assoluto, nel senso di non poter essere compresso, ma anzi che esso debba costantemente fare i conti con interessi e diritti di pari valore. Questa considerazione pare doversi riproporre anche con riguardo all'art. 17, essendovi gli estremi per attuare un attento giudizio di proporzionalità, che altro non è che, in termini europei, un sinonimo di attento bilanciamento.

Il test di proporzionalità europeo, infatti, si compone di tre passaggi. Innanzitutto, si deve verificare se la misura contestata sia in sé appropriata alla luce delle finalità che si propone, considerando se essa sia idonea a raggiungere la finalità che si propone e se tale finalità sia in sé legittima. In secondo luogo, la misura legislativa soggetta al vaglio di proporzionalità deve essere necessaria, ossia essere la misura che impone il minor sacrificio

[578] CGUE 24 novembre 2011, Causa C-70/10, *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, liberamente accessibile presso: «https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:62010CJ0070&from=EN» (Ultimo accesso: 10 maggio 2022).

[579] CGUE 16 febbraio 2012, C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV*, liberamente consultabile presso: «https://curia.europa.eu/juris/document/document.jsf?docid=119512&doclang=IT» (Ultimo accesso: 10 maggio 2022).

[580] Per riferimenti dottrinali si veda S. F. SCHWEMER; J. SCHOVSBO, *What is Left of User Rights? – Algorithmic Copyright Enforcement and Free Speech in the Light of the Article 17 Regime* (December 20, 2019), in Paul Torremans (ed), *Intellectual Property Law and Human Rights*, 4th edition (Wolters Kluwer, 2020, 569-589, liberamente accessibile presso: «https://ssrn.com/abstract=3507542» o «http://dx.doi.org/10.2139/ssrn.3507542» (Ultimo accesso: 10 maggio 2022).

[581] Avvocato Generale Henrik Saugmandsgaard Øe, conclusioni presentate il 15 luglio 2021 nella Causa C-401/19, Repubblica di Polonia contro Parlamento europeo, Consiglio dell'Unione europea, ricorso presentato ex art. 263 TFUE, cit.

possibile agli altri diritti protetti. In terzo luogo, deve essere confrontata con gli altri interessi ad essa opposti[582].

Gli interessi che si oppongono all'*enforcement* del diritto d'autore per mezzo di meccanismi automatici di filtraggio sono già stati affermati in precedenza richiamando le sentenze Scarlet Extended v. Sabam e Sabam v. Netlog.

La libertà di espressione, la libertà di impresa, la tutela della privacy, sono tutti diritti che vengono ristretti significativamente se gli obblighi imposti ai *provider* dall'art. 17 possono essere rispettati solo per il tramite di un filtraggio automatico dei contenuti[583]. Alcuni autori hanno infatti notato che il filtraggio automatizzato porta all'inaccessibilità dei contenuti condivisi sulle piattaforme disciplinate dall'art. 17, vanificando così in modo significativo i diritti degli utenti. Inoltre, gli utenti che caricano contenuti, catturati da meccanismi di filtraggio automatizzati, sarebbero limitati nel loro diritto di trasmettere informazioni, comprese quelle che potrebbero essere legalmente rese disponibili in base a un'eccezione o limitazione al diritto d'autore. Questi usi legittimi come ad esempio per citazioni, critiche, revisioni o parodia beneficiano di una fortissima giustificazione dei diritti fondamentali che la Direttiva altrimenti intende esplicitamente salvaguardare (art. 17, par. 7). Pertanto, ogni filtraggio automatizzato inevitabilmente indotto dall'art. 17 che non fosse in grado di riconoscere e rispettare tali usi legittimi violerebbe non solo la volontà esplicita del legislatore, ma anche diritti importanti in una società democratica[584].

In aggiunta, si può notare che obbligando i *provider* ad adottare un ruolo proattivo nell'*enforcement* del diritto d'autore sul web si chiede che gli stessi investano pesantemente le proprie risorse finanziarie per adattarsi alle richieste legislative dell'art. 17, così ponendo serie limitazioni alla libertà di impresa come tutelata dall'art. 16 della Carta di Nizza.

L'enforcement automatizzato dei diritti d'autore richiede necessariamente il trattamento dei dati personali e l'applicazione delle violazioni del diritto d'autore richiede la divulgazione di tali informazioni alle parti lese o alle forze dell'ordine. I dati degli utenti, ovvero quando e cosa caricano e scaricano su e dalle piattaforme di condivisione dei contenuti online, sono tutelati dal diritto alla protezione dei dati personali e dal rispetto della vita privata e familiare. In caso di presunte violazioni del diritto d'autore, questi diritti sono in conflitto con il diritto di proprietà intellettuale. Su questo punto il bilanciamento, come vedremo, oltre ad

---

582 In questo senso si esprimono C. GEIGER, B.J. JÜTTE, *Platform liability under article 17 of the copyright in the Digital Single Market directive, automated filtering and fundamental rights: an impossible match*, 2020, liberamente accessibile presso: «https://digitalcommons.wcl.american.edu/research/64/» (Ultimo accesso: 10 maggio 2022). Per un'attenta analisi del delicato bilanciamento in commento e dei risvolti in tema di proporzionalità europea si faccia riferimento a C. SGANGA, *A Decade of Fair Balance Doctrine, and How to Fix It: Copyright Versus Fundamental Rights Before the CJEU from Promusicae to Funke Medien, Pelham and Spiegel Online,* cit.; si veda inoltre C. SGANGA, *A New Era for EU Copyright Exceptions and Limitations? Judicial Flexibility and Legislative Discretion in the Aftermath of the CDSM Directive and the Trio of the Grand Chamber of the CJEU,* cit., 311-339.

583 Per notazioni dottrinali sul tema si facia riferimento a S. F. SCHWEMER; J. SCHOVSBO, *What is Left of User Rights? – Algorithmic Copyright Enforcement and Free Speech in the Light of the Article 17 Regime,* cit. 569-589.

584 In questo senso si esprimono C. GEIGER, B.J. JÜTTE, *Platform liability under article 17 of the copyright in the Digital Single Market directive, automated filtering and fundamental rights: an impossible match*, cit., 6-7, quando affermano che "*Automated filtering leads to the inaccessibility of content shared on online content-sharing platforms, thereby frustrating the rights of users in a significant manner. Furthermore, users uploading content, which is caught by automated filtering mechanisms, would be restricted in their right to impart information, including such information that could be lawfully made available under an exception or limitation to copyright. These legitimate uses such as e.g. for quotations, criticism, review or parody purposes benefit from a very strong fundamental rights justification which the directive otherwise explicitly aims to safeguard (Art 17 (7)). Thus, any automated filtering inevitably induced by Art. 17 that would be incapable of recognizing and respecting these legitimate uses would not be only violating the explicit will of the legislature but also important rights in a democratic society".*

interessarci maggiormente, dati i fini dichiarati di questo elaborato, si mostra come particolarmente complesso.

In sostanza allora, l'obbligo imposto agli OCSSP ai sensi dell'articolo 17, paragrafo 4, renderà inevitabile che le piattaforme monitorino e filtrino i contenuti caricati dai loro utenti con mezzi automatizzati. Questo è il risultato di una redazione giuridica che non riesce a determinare l'equilibrio tra i diritti fondamentali pertinenti a livello dell'UE, nonché costituisce il motivo per cui, come vedremo, la Polonia ha deciso di esercitare le prerogative dell'articolo 263 TFUE avverso l'articolo 17, paventandone censure di illegittimità[585], forse tuttavia erroneamente respinte dalla Corte di Giustizia[586].

7.1. Libertà di informazione e di espressione

Il primo punto di scontro con l'*enforcement* del diritto d'autore è dato dagli artt. 10 ed 11 della Carta di Nizza che tutelano la libertà di espressione ed il diritto di informare ed essere informati[587]. In particolare, l'art. 10 dispone che ogni individuo ha diritto alla libertà di pensiero, di coscienza e di religione, mentre l'articolo 11 completa la precedente disposizione confermando che ogni individuo ha diritto alla libertà di espressione e che tale diritto include la libertà di opinione e la libertà di ricevere o di comunicare informazioni o idee senza che vi possa essere ingerenza da parte delle autorità pubbliche e senza limiti di frontiera. A queste due disposizioni si lega a doppio filo quella prevista dall'art. 13 della Carta di Nizza, la quale prevede che le arti e la ricerca scientifica siano libere, e del pari che la libertà accademica sia rispettata. In aggiunta, anche l'articolo 11 CEDU dispone che ogni persona ha diritto alla libertà d'espressione e che tale diritto include la libertà d'opinione e la libertà di ricevere o di comunicare informazioni o idee senza che vi possa essere ingerenza da parte delle autorità pubbliche e senza limiti di frontiera.

Sicuramente sia la Corte di Giustizia[588] che la Corte Europea dei diritti dell'uomo hanno riconosciuto che la tutela dei diritti menzionati può essere compressa in determinate occasioni ai fini della tutela della proprietà intellettuale; tuttavia, con il limite che tali restrizioni siano assolutamente necessarie in una società democratica e nel rispetto del

---

585 Ricorso proposto il 24 maggio 2019 — Repubblica di Polonia/Parlamento europeo e Consiglio dell'Unione europea (Causa C-401/19), liberamente consultabile presso: «https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:62019CN0401&from=EN» (Ultimo accesso: 10 maggio 2022).

586 CGUE 26 aprile 2022, C-401/2019, Repubblica di Polonia contro Parlamento europeo, Consiglio dell'Unione europea, cit.

587 Per maggiori informazioni sul bilanciamento fra diritti fondamentali ed il nuovo articolo 17 in commento si faccia riferimento a J. P. QUINTAIS, P. MEZEI, I. HARKAI, J. C. MAGALHÃES, C. KATZENBACH, S. F. SCHWEMER, & T. RIIS, *Final Report on mapping of EU legal framework and intermediaries' practices on copyright content moderation and removal*, 2022, cit., 65 e ss.

588 Si veda ad esempio CGEU 12 giugno 2003, C-112/00, *Eugen Schmidberger, Internationale Transporte und Planzüge contro Republik Österreich*, liberamente accessibile presso: «https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A62000CJ0112» (Ultimo accesso: 10 maggio 2022). Per maggiori informazioni sulla libertà di espressione nel panorama giurisprudenziale europeo si veda anche: O. POLLICINO, M. BASSINI, *Free Speech, Defamation and the Limits to Freedom of Expression in the EU: A Comparative Analysis (2014)*, in A. SAVIN, J. TRZASKOWSKI (eds), in *Research Handbook on EU Internet Law*, 2014, Bocconi Legal Studies Research Paper No. 2706112, liberamente accessibile presso: «https://ssrn.com/abstract=2706112» (Ultimo accesso: 10 maggio 2022); O. POLLICINO, *Right to Internet Access: Quid Iuris?*, in A. VON ARNAULD, K. VON DER DECKEN, M. SUSI (eds), *The Cambridge Handbook on New Human Rights. Recognition, Novelty, Rhetoric, Cambridge*, 2019, liberamente accessibile presso: «https://ssrn.com/abstract=3397340» (Ultimo accesso: 10 maggio 2022); O. POLLICINO, L. SOMAINI, *Online Disinformation and Freedom of Expression in the Electoral Context: The European and Italian Responses*, in S. BAUME, V. BOILLET, V. MARTENET (eds), in *Misinformation in referenda*, liberamente accessibile presso: «https://ssrn.com/abstract=3552680» (Ultimo accesso: 10 maggio 2022).

principio di proporzionalità. Allo stesso tempo si conferma l'importanza della libertà di espressione anche su Internet[589].

Proprio con riferimento al contesto della libertà di espressione sul web la Corte di Giustizia ha recentemente confermato un indirizzo interpretativo inaugurato già dalla Corte Europea dei Diritti dell'Uomo. Infatti, secondo tale giurisprudenza, "*l'articolo 10 della CEDU garantisce la libertà di espressione e d'informazione a chiunque e riguarda non soltanto il contenuto delle informazioni, ma anche i mezzi della loro diffusione; qualsiasi limitazione apportata a tali mezzi incide sul diritto di ricevere e di comunicare informazioni*". La giurisprudenza in merito, infatti, rileva che "*Internet è oggi divenuto uno dei principali strumenti di esercizio, da parte degli individui, del loro diritto alla libertà di espressione e d'informazione. I siti Internet, e in particolare le piattaforme di condivisione di contenuti online, grazie alla loro accessibilità e alla loro capacità di conservare e di diffondere grandi quantità di dati, contribuiscono notevolmente a migliorare l'accesso del pubblico all'attualità e, in via generale, ad agevolare la comunicazione delle informazioni; la possibilità, per i singoli individui, di esprimersi su Internet costituisce uno strumento senza precedenti per esercitare la libertà di espressione*"[590].

In riferimento all'art. 13 della Carta poi, un meccanismo come quello richiesto agli OCSSP dall'articolo 17 introdurrebbe il rischio di minare la creatività online dato che la massima protezione di alcune forme di creatività intellettuale andrebbe a scapito di altre forme di creatività che sono anche positive per la società. A questo proposito l'importanza del modo in cui l'arte è comunicata deve essere evidenziata. In particolare, le moderne forme di espressione digitale creativa sono diffuse prevalentemente al pubblico tramite piattaforme online, come quelle soggette a regolamentazione ai sensi dell'articolo 17 della Direttiva. La regolamentazione dei canali di diffusione può quindi costituire una restrizione al diritto alla libertà artistica, che necessita di giustificazione e di bilanciamento

La dimensione toccata dall'art. 17 che mostra un particolare interesse è quella che compendia le tecnologie di filtraggio alle eccezioni e limitazioni previste per il diritto d'autore. Infatti, l'art. 17 paragrafo settimo sostiene che la cooperazione tra i prestatori di servizi di condivisione di contenuti online e i titolari dei diritti non deve impedire la disponibilità delle opere o di altri materiali caricati dagli utenti, che non violino il diritto d'autore o i diritti connessi, anche nei casi in cui tali opere o altri materiali siano oggetto di un'eccezione o limitazione. In particolare, le eccezioni necessariamente da tenere in considerazioni sono quelle di (a) citazione, critica, rassegna e (b) utilizzi a scopo di caricatura, parodia o *pastiche*. Tale disposizione normativa è da leggere in combinato disposto con il paragrafo nono che, ribadendo il concetto, stabilisce che la Direttiva 2019/790 non incide in alcun modo sugli utilizzi legittimi, quali quelli oggetto delle eccezioni o limitazioni previste dal diritto dell'Unione.

Le linee guida della Commissione fanno poi notare che le eccezioni o limitazioni di cui alla Direttiva 2001/29/CE sono facoltative e rivolte a tutti gli utenti. Per contro, "*le eccezioni e limitazioni particolari di cui all'articolo 17, paragrafo 7, sono di attuazione obbligatoria per gli Stati membri, si applicano specificamente e solo all'ambiente online e a tutti gli utenti al momento del caricamento*

589 In questo senso si esprimono C. GEIGER, B.J. JÜTTE, *Platform liability under article 17 of the copyright in the Digital Single Market directive, automated filtering and fundamental rights: an impossible match*, cit., 1 e ss.

590 CGUE 26 aprile 2022, C-401/2019, Repubblica di Polonia contro Parlamento europeo, Consiglio dell'Unione europea, cit., par. 46. La Corte richiama in particolare la giurisprudenza della Corte EDU: Corte EDU, 1° dicembre 2015, Cengiz e a. c. Turchia, par. 52; nonché Corte EDU, 23 giugno 2020, Vladimir Kharitonov c. Russia, par. 33 e giurisprudenza ivi citata.

e della messa a disposizione di contenuti generati dagli utenti su servizi di condivisione di contenuti online, senza che siano previste ulteriori condizioni per la loro applicazione"[591].

Il Considerando 70 esplicitamente afferma che le misure adottate dai prestatori di servizi di condivisione di contenuti online in cooperazione con i titolari dei diritti non dovrebbero pregiudicare l'applicazione di eccezioni o limitazioni al diritto d'autore, in particolare quelle intese a garantire la libertà di espressione degli utenti, mostrando proprio la stretta relazione allora fra i meccanismi di filtraggio e le possibili compressioni alla libertà di espressione. Il Considerando poi afferma, come visto, che garantire le eccezioni e limitazioni al diritto d'autore "*è particolarmente importante al fine di raggiungere un equilibrio tra i diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea («Carta»), in particolare la libertà di espressione e la libertà delle arti, e il diritto di proprietà, inclusa la proprietà intellettuale*". La richiesta di raggiungere questo equilibrio, infatti, richiede di bilanciare attentamente l'*enforcement* del diritto d'autore con la libertà di espressione.

Questa libertà, secondo parte della dottrina, sarebbe limitata se si impedissero usi che rientrano nell'ambito di una delle eccezioni elencate, e certamente anche altre eccezioni disponibili ai sensi delle rispettive legislazioni nazionali mediante filtraggio generale o specifico. L'importanza di alcuni tipi di espressione, in particolare il discorso di natura politica, peserebbe proprio sull'applicazione di filtri di contenuto da parte degli OCSSP che creerebbero inevitabilmente effetti collaterali sul discorso lecito[592].

Per quanto riguarda gli utilizzi legittimi, tutelati dal paragrafo nono, essi sono definiti dalle linee guida della Commissione come quegli usi che non violano il diritto d'autore o i diritti connessi e che possono comprendere "a*) gli usi oggetto di eccezioni e limitazioni, b) gli usi da parte di coloro che detengono o hanno acquistato i diritti sui contenuti da essi caricati o gli usi contemplati dall'autorizzazione di cui all'articolo 17, paragrafo 2, e c) gli usi di contenuti non coperti dal diritto d'autore o dai diritti connessi, in particolare per quanto riguarda le opere di dominio pubblico o, ad esempio, i contenuti che non raggiungono la soglia di originalità o non soddisfano qualsiasi altro requisito relativo alla soglia di protezione*[593]". Se tuttavia si considera la difficoltà, ancora oggi, di comprendere quando un'opera sia originale o meno e se sia meritevole del diritto d'autore, sorprende quantomeno la cieca fiducia che la Commissione dimostra avere nei confronti delle soluzioni tecnologiche. Di questa fiducia tuttavia è possibile, se non doveroso, dubitare[594].

---

591 Communication From The Commission To The European Parliament And The Council: Guidance on Article 17 of Directive 2019/790 on Copyright in the Digital Single Market COM/2021/288 final, cit.

592 In questo senso si esprimono C. GEIGER, B.J. JÜTTE, *Platform liability under article 17 of the copyright in the Digital Single Market directive, automated filtering and fundamental rights: an impossible match*, cit.; si veda altresì P. SAMUELSON, *Pushing Back on Stricter Copyright ISP Liability Rules,* in *Michigan Technology Law Review,* 2020, accessibile presso: «https://ssrn.com/abstract=3630700» (Ultimo accesso: 10 maggio 2022).

593 Communication From The Commission To The European Parliament And The Council: Guidance on Article 17 of Directive 2019/790 on Copyright in the Digital Single Market COM/2021/288 final, cit.

594 Si veda ad esempio la sentenza CGUE 29 luglio 2019, C-469/17, *Funke Medien NRW GmbH / Bundesrepublik Deutschland,* consultabile presso: «https://curia.europa.eu/juris/document/document.jsf?text=&docid=207024&pageIndex=0&doclang=it&mode=lst&dir=&occ=first&part=1&cid=1467839» (Ultimo accesso: 10 maggio 2022); Laura Camarella, in L. CAMARELLA, *La responsabilità dell'Internet Service Provider alla luce della nuova Direttiva sul diritto d'autore nel mercato unico digitale*, cit., 161, si esprime affermando: "*i rischi persistono in capo agli utenti: inutile soffermarsi sul grado di imprecisione che tali software di riconoscimento hanno nell'individuazione e distinzione del materiale protetto da quello che non lo è. La situazione si complica ulteriormente quando del materiale protetto può poi essere utilizzato rientrando nelle varie ipotesi di eccezioni e limitazioni le quali già sono difficilmente scindibili in un giudizio di legalità ex post, men che meno potranno essere decise con certezza da algoritmi automatici che agiscono ex ante. Il rischio è quello di sfociare non solo nella rimozione di contenuti in realtà leciti, ma anche nell'impossibilità di caricare contenuti leciti in seguito al vaglio preventivo di tali software, con gravi ripercussioni sulle libertà di informazione ed espressione di cui all'art. 11 della Carta*".

Sembra comunque che possa sussistere una sorta di gerarchia di importanza fra il paragrafo settimo ed il paragrafo quarto, cosa che è stata anche confermata dalla Commissione europea durante la sua udienza[595] dinnanzi alla Corte di Giustizia nel contesto della censura mossa dalla Polonia.

Sebbene dunque sia previsto così dall'art. 17 paragrafo settimo, i precedenti paragrafi suggeriscono comunque che gli OCSSP dovrebbero monitorare i caricamenti in relazione a tutte le opere e altri materiali per i quali non sia stato possibile ottenere alcuna autorizzazione ai sensi dell'articolo 17 paragrafi primo e secondo. Pare quindi che gli OCSSP debbano monitorare tutti i caricamenti da parte degli utenti in relazione ai quali vengono fornite informazioni (necessarie e pertinenti) dai titolari dei diritti, e questo anche se in realtà tali caricamenti non costituirebbero violazioni dei diritti d'autore. Infatti, il caricamento può costituire un uso pienamente legittimo, perché coperto da un'eccezione e limitazione al diritto d'autore, valutazione che può essere di per sé molto complessa[596].

La discussione sulla capacità dell'articolo 17 di combattere le violazioni del diritto d'autore e sul ruolo che il filtraggio automatizzato dovrebbe svolgere in questo contesto si basa, secondo parte della dottrina, sull'idea sbagliata che la tecnologia sia in grado di risolvere tutti i problemi di applicazione dell'art. 17. Il legislatore dell'UE sembra presumere che l'OCSSP possa utilizzare filtri "intelligenti" che identificano i contenuti illeciti consentendo al contempo il caricamento e la messa a disposizione di contenuti leciti[597].

Anche le linee guida della Commissione dimostrano la consapevolezza da parte della stessa dell'impossibilità del funzionamento di un simile sistema, cosa che invece non pare trasparire dal dettato legislativo dell'art. 17 che impone ai *provider* un obbligo di risultato. La Commissione, infatti, afferma che "*allo stato attuale delle conoscenze tecniche, nessuna tecnologia è in grado di raggiungere gli standard richiesti dalla legge nel valutare se il caricamento di contenuti che un utente desidera effettuare costituisca un uso legittimo o lesivo del diritto d'autore o dei diritti connessi. La tecnologia di riconoscimento dei contenuti può tuttavia individuare un contenuto specifico protetto dal diritto d'autore in relazione al quale i titolari dei diritti hanno fornito ai prestatori di servizi le informazioni pertinenti e*

---

595 Per riferimenti in merito si veda P. KELLER, *CJEU hearing in the Polish challenge to Article 17: Not even the supporters of the provision agree on how it should work*, in *Kluwer Copyright Blog*, liberamente accessibile presso: «http://copyrightblog.kluweriplaw.com/2020/11/11/cjeu-hearing-inthe-polish-challenge-to-article-17-not-even-the-supporters-of-the-provision-agree-onhow-it-should-work/» (Ultimo accesso: 10 maggio 2022).

596 Per maggiori informazioni si veda: J.QUINTAIS, G. FROSIO, S. GOMPEL, P.B. HUGENHOLTZ, M. HUSOVEC, B.J. JÜTTE, M. SENFTLEBEN, *Safeguarding User Freedoms in Implementing Article 17 of the Copyright in the Digital Single Market Directive: Recommendations From European Academics,* in *Journal of Intellectual Property, Information Technology and E-Commerce Law (JIPITEC*), 2019, liberamente accessibile presso: «https://www.jipitec.eu/issues/jipitec-10-3-2019/5042» (Ultimo accesso: 10 maggio 2022); G. FROSIO, *The Death of 'No Monitoring Obligations': A Story of Untameable Monsters,* 8(3) *Journal of Intellectual Property, Information Technology and E-Commerce Law (JIPITEC*) 212, 2017 liberamente accessibile presso: «https://ssrn.com/abstract=2980786» (Ultimo accesso: 10 maggio 2022).

597 In questo senso si esprimono C. GEIGER, B.J. JÜTTE, *Platform liability under article 17 of the copyright in the Digital Single Market directive, automated filtering and fundamental rights: an impossible match*, cit. 45 e ss. Gli autori citano altresì numerosa altra dottrina in merito che si procede a riportare per veloci riferimenti a tesi dottrinali adiacenti a quella presentata: in particolare si veda T. SPOERRI, *On Upload-Filters and other Competitive Advantages for Big Tech Companies under Article 17 of the Directive on Copyright in the Digital Single Market,* 10(2) *Journal of Intellectual Property, Information Technology and E-Commerce Law* (2019), liberamente accessibile presso: «https://www.jipitec.eu/issues/jipitec-10-2-2019/4914/JIPITEC_10_2_2019_173_Spoerri» (Ultimo accesso: 10 maggio 2022). Si segnala nello stesso senso anche uno studio condotto nel 2019 che sottolinea come il *Content ID* di *YouTube* non sia in grado di distinguere fra un uso lecito od illecito: S. JACQUES, K. GARSTKA, M. HVIID, J. STREET, *An Empirical Study of the Use of Automated Anti-Piracy Systems and Their Consequences for Cultural Diversity*, 15(2) *SCRIPTed* (2018), 277-312, liberamente accessibile presso: «https://script-ed.org/article/an-empirical-study-of-the-use-of-automated-anti-piracy-systems-and-their-consequences-for-cultural-diversity/» (Ultimo accesso: 10 maggio 2022).

necessarie". Per ovviare a questa *impasse*, per la Commissione, il blocco automatizzato dovrebbe in linea di principio essere limitato ai caricamenti "*manifestamente lesivi del diritto d'autore o dei diritti connessi*", mentre gli altri caricamenti dovrebbero essere consentiti ed eventualmente soggetti ad "*una verifica umana ex post qualora i titolari dei diritti si oppongano inviando una segnalazione*", in conformità al paragrafo 9[598].

La Commissione tenta, ad avviso di chi scrive inefficacemente, di fornire dei criteri per stabilire quando le tecnologie dovrebbero bloccare i contenuti o meno. Innanzitutto, afferma che i contenuti che i titolari dei diritti non hanno espressamente chiesto di bloccare non dovrebbero essere considerati manifestamente lesivi del diritto d'autore o dei diritti connessi. Poi aggiunge che "*fra i criteri utili per individuare nella pratica i caricamenti manifestamente lesivi del diritto d'autore […] potrebbero figurare la lunghezza/le dimensioni dei contenuti identificati utilizzati nel caricamento, la proporzione del contenuto corrispondente/identificato in relazione all'intero caricamento (ad esempio se il contenuto corrispondente è utilizzato separatamente o in combinazione con altri contenuti) e il livello di modifica dell'opera (ad esempio se il caricamento corrisponde solo in parte al contenuto identificato perché è stato modificato dall'utente*) [599] ". Un esempio di caricamento che, secondo la Commissione, generalmente non dovrebbe essere considerato manifestamente lesivo del diritto d'autore o dei diritti connessi potrebbe essere quello che "*comprende brevi estratti che rappresentano una piccola parte dell'intera opera identificata dai titolari dei diritti (tale uso può essere coperto dall'eccezione prevista per le citazioni). Questo potrebbe essere il caso di un video generato da un utente comprendente un estratto di un lungometraggio o di una canzone*[600]".

Il rischio di un "*over-enforcement*" è chiaramente in agguato quando si prendono in considerazioni queste disposizioni. Richiamando un'opinione espressa da Senftleben, alcuni autori hanno sostenuto proprio che la disposizione in commento prevede implicitamente che la valutazione legale sottostante che dovranno compiere i *provider* è probabile che sia cauta e difensiva, ed allo stesso tempo ricordano come un'interpretazione generosa delle limitazioni del *copyright* al servizio della libertà di espressione sembri improbabile. In altre parole, vi è il rischio di un'applicazione eccessiva, un "*over-enforcement*" appunto.[601]

Rendendosi conto tuttavia della pratica impossibilità di adottare un sistema di filtraggio così intelligente da poter distinguere le sfumature contestuali di un caricamento, la Commissione ricorre poi ad affermare che "*può essere necessaria, ove proporzionato e possibile, una rapida verifica umana ex ante, da parte dei prestatori di servizi di condivisione di contenuti online, dei caricamenti che includano contenuti la cui disponibilità potrebbe causare un danno economico significativo*

---

[598] Per maggiori informazioni ed una attenta analisi dei meccanismi procedurali di salvaguardia delle pretese degli utenti si veda J. P. QUINTAIS, P. MEZEI, I. HARKAI, J. C. MAGALHÃES, C. KATZENBACH, S. F. SCHWEMER, & T. RIIS, *Final Report on mapping of EU legal framework and intermediaries' practices on copyright content moderation and removal*, 2022, cit., 63.

[599] Communication From The Commission To The European Parliament And The Council: Guidance on Article 17 of Directive 2019/790 on Copyright in the Digital Single Market COM/2021/288 final, cit.

[600] Communication From The Commission To The European Parliament And The Council: Guidance on Article 17 of Directive 2019/790 on Copyright in the Digital Single Market COM/2021/288 final, cit.

[601] Per maggiori informazioni si veda J. P. QUINTAIS, P. MEZEI, I. HARKAI, J. C. MAGALHÃES, C. KATZENBACH, S. F. SCHWEMER, & T. RIIS, *Final Report on mapping of EU legal framework and intermediaries' practices on copyright content moderation and removal*, 2022, cit., 64. Gli autori in merito citano altresì, per riferimenti, J. M. URBAN; J. KARAGANIS; B. SCHOFIELD, '*Notice and Takedown:Online Service Provider and Rightsholder Accounts of Everyday Practi*ce' (2017) 64 J. *Copyright Soc'y* 371; K. ERICKSON; M. KRETSCHMER, 'Empirical Approaches to Intermediary Liability' in Giancarlo Frosio (ed), *Oxford Handbook on Intermediary Liability Online* (OUP 2019), liberamente acessibile presso: «https://papers.ssrn.com/abstract=3400230» (Ultimo accesso: 10 maggio 2022); S. BAR-ZIV; N. ELKIN-KOREN, Behind the Scenes of Online Copyright Enforcement: Empirical Evidence on Notice & Takedown' (2017), 50 *Connecticut Law Review*, liberamente accessibile presso: «https://papers.ssrn.com/abstract=3214214». (Ultimo accesso: 10 maggio 2022).

identificati da uno strumento automatizzato di riconoscimento dei contenuti". Ciò si applicherebbe, ad avviso della Commissione, a quei contenuti particolarmente "sensibili al fattore tempo" ad esempio anteprime di musica o film o momenti salienti di trasmissioni recenti di eventi sportivi.

Ciò che è evidente a questo punto è che i filtri automatizzati che il legislatore europeo nei fatti impone alle piattaforme di adottare, non sono in grado di riconoscere le sfumature che concernono ogni singolo caricamento di un materiale, in quanto queste ultime, spesso, dipendono dal contesto di caricamento, il che è tuttavia necessario per distinguere le violazioni del diritto d'autore dagli usi che rientrano nell'ambito di un'eccezione. Geiger e Jutte in merito ricordano che tale distinzione sarebbe necessaria per differenziare tra la semplice riproduzione di una parte di un'opera, e la riproduzione della stessa parte per un uso parodistico o che costituisce una citazione consentita. Entrambe le situazioni dovrebbero, ad avviso degli autori, essere valutate nel contesto in cui avviene l'uso di un'opera protetta e si basano su considerazioni contestuali come l'intento di umorismo o lo spirito satirico[602].

7.2. Libertà di impresa

Come più volte ricordato, già nel 2012 la Corte di Giustizia con i casi Sabam[603] riteneva che l'imposizione di un obbligo di sorveglianza avrebbe comportato un'indebita compressione della libertà di impresa. In tale contesto la Corte di Giustizia aveva affermato che una simile obbligazione avrebbe causato "*una grave violazione della libertà di impresa […], poiché l'obbligherebbe a predisporre un sistema informatico complesso, costoso, permanente e unicamente a suo carico, il che risulterebbe peraltro contrario alle condizioni stabilite dall'art. 3, n. 1, della Direttiva 2004/48, il quale richiede che le misure adottate per assicurare il rispetto dei diritti di proprietà intellettuale non siano inutilmente complesse o costose*".

La libertà di impresa è tutelata nel sistema normativo europeo principalmente dall'art. 16 della Carta di Nizza, il quale proclama che "*è riconosciuta la libertà d'impresa, conformemente al diritto comunitario e alle legislazioni e prassi nazionali*".

In due casi relativi ad *access provider*, la CGUE ha ulteriormente determinato i parametri per le interferenze con la libertà di svolgere un'attività nel contesto del monitoraggio e del blocco delle informazioni. Nella causa Mc Fadden[604], ha in particolare chiarito che un requisito che obbligasse un fornitore di accesso ad adeguare le opzioni tecniche a sua disposizione non sarebbe arrivato al punto di sconfinare nell'essenza stessa della libertà di condurre un'impresa. Ma in questo caso il provvedimento richiesto sembrava assolutamente necessario per tutelare l'essenza di un altro diritto fondamentale, che a sua volta giustificava

---

602 In questo senso si esprimono C. GEIGER, B.J. JÜTTE, *Platform liability under article 17 of the copyright in the Digital Single Market directive, automated filtering and fundamental rights: an impossible match*, cit. 48 e ss.

603 CGUE 24 novembre 2011, Causa C-70/10, *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*; CGUE 16 febbraio 2012, causa C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV*.

604 Sentenza CGUE 15 settembre 2016, C-484/14, *Tobias Mc Fadden contro, Sony Music Entertainment Germany GmbH,* liberamente consultabile presso: «https://curia.europa.eu/juris/document/document.jsf?text=&docid=183363&pageIndex=0&doclang=IT&mode=req&dir=&occ=first&part=1» (Ultimo accesso: 10 maggio 2022).

una moderata restrizione del diritto di cui all'articolo 16, tuttavia, l'obbligo di monitoraggio del traffico Internet è stato chiaramente respinto nella specie[605].

Tale domanda era stata presentata nell'ambito di una controversia tra il sig. Tobias Mc Fadden e la Sony Music Entertainment Germany GmbH avente ad oggetto l'eventuale responsabilità del primo nell'utilizzo, da parte di un terzo, della rete locale senza fili gestita dal sig. Mc Fadden al fine di mettere a disposizione del pubblico, senza autorizzazione, un fonogramma prodotto dalla Sony Music.

Il sig. Mc Fadden gestiva infatti un'impresa che vendeva o noleggiava materiali d'illuminazione e audio. Nella sua attività egli sfruttava una rete locale senza fili che offriva, nei dintorni della sua impresa, un accesso gratuito e anonimo a Internet. L'accesso a detta rete era deliberatamente non protetto al fine di attirare l'attenzione dei clienti dei negozi adiacenti, dei passanti e dei vicini sulla sua attività. Nel settembre 2010 un'opera musicale venne gratuitamente messa a disposizione del pubblico su Internet, senza il consenso dei titolari dei relativi diritti, attraverso la rete locale senza fili gestita dal sig. Mc Fadden. Quest'ultimo affermava di non aver commesso l'asserita violazione, ma di non poter escludere che fosse stata commessa da uno degli utenti della sua rete.

Con lettera del 29 ottobre 2010, la Sony Music intimava al sig. Mc Fadden di rispettare i suoi diritti su detto fonogramma. In seguito a tale diffida, il sig. Mc Fadden proponeva dinanzi al giudice del rinvio un'azione di accertamento negativo, a fronte della quale la Sony Music replicava formulando varie domande riconvenzionali volte ad ottenere dal sig. Mc Fadden, non solo il risarcimento dei danni a titolo della sua responsabilità diretta nella violazione dei propri diritti su detto fonogramma, ma anche la cessazione della violazione dei suoi diritti.

Nella sua domanda di pronuncia pregiudiziale, il giudice del rinvio osservava di essere propenso a ritenere che la violazione dei diritti della Sony Music non fosse stata commessa personalmente dal sig. Mc Fadden, bensì da un utente sconosciuto della sua rete. Tuttavia, detto giudice prospettava l'insorgenza di una responsabilità indiretta del sig. Mc Fadden, non avendo quest'ultimo protetto la rete mediante la quale era stato possibile commettere in modo anonimo la violazione di cui trattasi. Sorgendo un dubbio interpretativo circa la portata della responsabilità stabilita dalla Direttiva e-commerce, il giudice a quo sospendeva il procedimento rinviando pregiudizialmente alla Corte di Giustizia numerose questioni.

Quella più interessante ai nostri fini riguarda la prospettazione di una ingiunzione in capo al signor Mc Fadden. Il giudice si chiedeva se il diritto comunitario ostasse all'adozione di un'ingiunzione che avesse imposto ad un *ISP,* a pena del pagamento di una penalità, di impedire a terzi di rendere disponibile al pubblico una specifica opera protetta dal diritto d'autore o parti di essa, qualora il fornitore avesse la possibilità di scegliere le misure tecniche da adottare per conformarsi a tale ingiunzione. Secondo la Corte, le sole misure che il *provider* poteva sostanzialmente adottare consistevano (a) nel chiudere la connessione a Internet (b) nel proteggerla mediante password o (c) nell'esaminare tutte le informazioni trasmesse attraverso tale connessione.

La Corte in merito a queste affermava, anzitutto, che la paventata sorveglianza dell'insieme delle informazioni trasmesse dovesse essere da subito esclusa, in quanto contraria all'articolo 15, paragrafo 1, della Direttiva 2000/31 ai sensi del quale è vietato

[605] Per notazioni dottrinali circa la rilevanza giurisprudenziale dei casi citati ai fini del presente bilanciamento si veda C. GEIGER, B.J. JÜTTE, *Platform liability under article 17 of the copyright in the Digital Single Market directive, automated filtering and fundamental rights: an impossible match*, cit. 26 e ss.

imporre un obbligo generale di sorveglianza sulle informazioni che i *provider* trasmettono. Riguardo, poi, alla misura consistente nel chiudere completamente la connessione a Internet, la Corte di Giustizia constatava che la sua attuazione avrebbe comportato una grave violazione della libertà di impresa del soggetto che persegua un'attività economica volta a fornire un accesso a Internet, vietandogli totalmente, di fatto, di proseguire tale attività al fine di porre rimedio a una violazione limitata del diritto d'autore senza prevedere l'adozione di misure meno restrittive di tale libertà. Infine, per quanto riguarda la misura consistente nel proteggere la connessione a Internet mediante una password, la Corte sottolineava che essa era idonea a restringere sia il diritto alla libertà d'impresa del prestatore che fornisce un servizio di accesso a una rete di comunicazione, sia il diritto alla libertà d'informazione dei destinatari di tale servizio. Tuttavia, quest'ultimo poteva essere compresso da una misura volta ad imporre di inserire una password di accesso alla rete, mentre sarebbe stata totalmente ingiustificata una misura di sorveglianza di massa.

La Corte, per quanto qui interessa, affermava che si deve constatare che "*la suddetta ingiunzione, là dove, da un lato, accolla a detto fornitore di accesso un obbligo idoneo ad incidere sulla sua attività economica e, dall'altro, è atta a limitare la libertà dei destinatari di un tale servizio di beneficiare di un accesso a Internet, viola il diritto alla libertà d'impresa del primo, tutelato ai sensi dell'articolo 16 della Carta, nonché il diritto alla libertà d'informazione dei secondi, la cui protezione è sancita dall'articolo 11 della Carta*".

Similmente, nella causa UPC Telekabel[606], la Corte ha stabilito che un'ingiunzione del tribunale che ha ordinato a un *access provider* di bloccare l'accesso a uno specifico sito Web non violava la sostanza stessa del diritto fondamentale. La questione pregiudiziale che veniva posta nel caso di specie era essenzialmente se i diritti fondamentali riconosciuti dall'UE dovessero essere interpretati nel senso che ostano a che sia vietato, con un'ingiunzione pronunciata da un giudice, a un fornitore di accesso ad Internet di concedere l'accesso ad un sito che mette in rete materiali protetti senza il consenso dei titolari dei diritti, qualora tale ingiunzione non specifichi quali misure tale fornitore d'accesso deve adottare e quest'ultimo possa evitare le sanzioni per la violazione di tale ingiunzione, dimostrando di avere comunque adottato tutte le misure ragionevoli.

Sebbene l'ingiunzione possa rappresentare un costo significativo per il fornitore di accesso, il fatto che la scelta di quale misura attuare per ottenere un determinato risultato fosse stata lasciata al fornitore di servizi, tenuto conto delle sue capacità, ha pesato a favore di un equilibrio adeguato.

In particolare, la Corte nota che, per quanto riguarda la libertà d'impresa, va constatato che l'adozione di un'ingiunzione quale quella di cui al procedimento principale limita tale libertà. Infatti, il diritto alla libertà d'impresa comprende segnatamente il diritto di ogni impresa di poter disporre liberamente, nei limiti della responsabilità per le proprie azioni, delle risorse economiche, tecniche e finanziarie di cui dispone. Secondo la Corte quindi non vi è dubbio che un'ingiunzione similare farebbe pesare in capo al suo destinatario un obbligo che limita il libero utilizzo delle risorse a sua disposizione, in quanto imporrebbe di adottare misure che possono rappresentare un costo notevole per lo stesso, avere un impatto considerevole sull'organizzazione delle sue attività o richiedere soluzioni tecniche difficili e complesse.

---

[606] CGUE 27 marzo 2014, C-314/12, *UPC Telekabel Wien GmbH contro Constantin Film Verleih GmbH e Wega Filmproduktionsgesellschaft mbH*, liberamente consultabile presso «https://curia.europa.eu/juris/document/document.jsf?text=&docid=149924&pageIndex=0&doclang=it&mode=lst&dir=&occ=first&part=1&cid=288334» (Ultimo accesso: 10 maggio 2022).

Tuttavia, secondo la Corte, una tale ingiunzione non risulta pregiudicare la sostanza stessa del diritto alla libertà d'impresa di un fornitore di accesso ad Internet, potendo quindi essere sacrificata in luce del bilanciamento con le esigenze di tutela del diritto d'autore.

Quello che ci interessa più da vicino è che in realtà tale corretto bilanciamento, che consente di comprimere la libertà di impresa, è giustificato nel caso di specie da condizioni particolari, che non si rinvengono con riferimento all'articolo 17 della Direttiva 2019/790. Da un lato, un'ingiunzione, quale quella di cui al caso Telekabel, lascerebbe al suo destinatario l'onere di determinare le misure concrete da adottare per raggiungere il risultato perseguito, con la conseguenza che quest'ultimo potrebbe scegliere di adottare misure che più si adattino alle risorse e alle capacità di cui dispone e che siano compatibili con gli altri obblighi e sfide cui deve far fronte nell'esercizio della propria attività. Dall'altro lato, tale ingiunzione consentirebbe al suo destinatario di sottrarsi alla propria responsabilità qualora dimostri di aver adottato tutte le misure ragionevoli. Orbene, tale possibilità di esenzione dalla responsabilità ha, ovviamente, la conseguenza che il destinatario di tale ingiunzione non sarà tenuto a fare sacrifici insostenibili, circostanza che appare in particolare giustificata alla luce del fatto che quest'ultimo non è l'autore della violazione del diritto fondamentale della proprietà intellettuale che ha dato luogo alla pronuncia della suddetta ingiunzione.

Dall'analisi casistica così determinata emergono almeno due considerazioni utili al bilanciamento fra la libertà di impresa e quanto previsto dall'art. 17. In primo luogo, la Corte di Giustizia si ritiene pronta ad affermare che il diritto di cui all'art. 16 della Carta di Nizza può essere facilmente compresso in ipotesi in cui vi sia una violazione del diritto d'autore. Tuttavia, tale limitazione deve essere soggetta ad un attento vaglio di proporzionalità e ragionevolezza per cui, seppur sacrificabile, la "sostanza", il "nucleo essenziale" di tale libertà deve essere mantenuto. Questo si traduce nella tipologia di intervento che può essere richiesto ad un *provider*. Il caso Mc Fadden ha posto in luce come fra varie possibili strategie di *enforcement* al diritto d'autore, solo le meno invasive della libertà di impresa, nonché le meno costose, potrebbero essere ritenute ragionevoli, escludendo quindi categoricamente che una tale misura possa essere integrata dalla sorveglianza o dal monitoraggio delle attività degli utenti. Tale misura infatti rappresenterebbe un costo notevole per il *provider* ed avrebbe un impatto considerevole sull'organizzazione delle sue attività, richiedendo soluzioni tecniche difficili e complesse.

Una seconda considerazione deriva poi dal caso Telekabel che, confermando il primo punto, afferma altresì che una limitazione della libertà di impresa sarebbe lecita e proporzionata solo ove lasci al suo destinatario l'onere di determinare le misure concrete da adottare per raggiungere il risultato perseguito, con la conseguenza che quest'ultimo potrebbe scegliere di adottare misure che più si adattino alle risorse e alle capacità della propria attività. Ebbene, salvo una limitazione parziale ex art. 17 paragrafo sesto per alcuni *provider* minori, pare che il testo dell'art. 17 lasci poco spazio alle scelte gestorie delle piattaforme, dovendo, nei fatti, adottare delle tecnologie di filtraggio, eventualmente lasciando la libertà, che libertà non è, di scegliere fra tecnologie equipollenti disponibili. La richiesta di conformarsi ad "elevati standard di diligenza professionale di settore", alle migliori prassi applicative disponibili sul mercato, va a finire con l'imporre un'irragionevole limitazione alla libertà di impresa[607].

Alla luce di queste considerazioni sorprende allora che la Corte di Giustizia, nel pronunciarsi sul ricorso ex art 263 TFUE per l'annullamento dell'art 17, abbia invece

[607] In senso conforme si segnala altresì: C. GEIGER, B.J. JÜTTE, *Platform liability under article 17 of the copyright in the Digital Single Market directive, automated filtering and fundamental rights: an impossible match*, cit. 29 e ss.

considerato la libertà di impresa non tanto come ostativa alla validità della disposizione normativa in commento, quanto invece confermativa della sua perdurante efficacia. Richiamando la giurisprudenza citata, ed in particolare il caso Telekabel, la Corte ribadisce che "*al fine di rispettare la libertà d'impresa di detti fornitori di servizi [..] e il giusto equilibrio tra essa, il diritto alla libertà di espressione e d'informazione degli utenti dei loro servizi […] e il diritto di proprietà intellettuale dei titolari di diritti, protetto all'articolo 17, paragrafo 2, della Carta*" sia essenzialmente necessario "*lasciare a detti fornitori di servizi l'onere di determinare le misure concrete da adottare per raggiungere il risultato perseguito, con la conseguenza che questi ultimi possono scegliere di adottare misure che più si adattino alle risorse e alle capacità di cui dispongono e che siano compatibili con gli altri obblighi e le sfide cui devono far fronte nell'esercizio della loro attività*"[608]. Ebbene questa affermazione dovrebbe essere letta con una attenzione alla pratica ed alle concrete possibilità di scelta lasciate al provider, da quel privilegiato punto di vista che si rivolge al mondo della realtà economica e tecnologica che, come vedremo, la Corte tende invece ad ignorare ed a dimenticare. Va infatti ribadito che l'articolo 17 lascia ben poco margine di scelta agli OCSSP, costringendoli nei fatti ad adottare sistemi di filtraggio automatico dei contenuti caricati online. Se la Corte non avesse, per preconcetto, voluto salvare l'articolo 17, si sarebbe infatti accorta di quanto contraddittoria in sé una simile affermazione potesse essere e del fatto che la libertà di impresa milita non già a favore della conservazione della disciplina in commento, quanto invece nel senso della sua illegittimità.

7.3. Privacy e vita privata

Il diritto alla privacy ed al rispetto della vita privata sono protetti, nell'ordinamento europeo, dagli articoli 7 ed 8 della Carta di Nizza, i quali a loro volta rimandano all'art. 8 CEDU. In particolare, mentre l'articolo 7 dispone che ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni, l'articolo 8 è espressione tipica dell'era digitale, affermando che "*Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica".*

L'articolo 8 della CEDU a sua volta, dopo aver ribadito che ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza, aggiunge che "*non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui*".

Tali diritti, come debitamente analizzato nella presente dissertazione, entrano spesso in conflitto con altre esigenze, quali quelle alla proprietà intellettuale od a un rimedio effettivo contro le violazioni di altri diritti. In questo punto l'*enforcement* del diritto d'autore mostra le più peculiari capacità di restringere l'ambito di tutela delle disposizioni sopra esaminate, per cui è necessario rinvenire nella normativa se un corretto bilanciamento con queste istanze può essere rinvenuto nell'art. 17 o meno.

[608] CGUE 26 aprile 2022, C-401/2019, Repubblica di Polonia contro Parlamento europeo, Consiglio dell'Unione europea, cit., par. 75

Alcuni autori hanno anche tentato di evidenziare "*una scarsa coordinazione tra i vari settori in cui può operare l'UE nella valutazione delle varie conseguenze, poiché esiste una connessione tra la protezione dei dati personali degli utenti e il complesso delle libertà di espressione all'interno di una società: probabilmente la consapevolezza che le proprie attività online sono monitorate può avere un effetto inibitorio sull'esercizio della libertà di espressione, incentivando così un eccesso di conformità da parte dei non trasgressori che desiderano evitare l'attenzione*"[609].

Come già visto in sede di capitolo secondo, la Corte di Giustizia non appare sempre cristallina nel definire quale debba essere il corretto bilanciamento fra l'*enforcement* del diritto d'autore e la tutela della privacy degli utenti, lasciando spesso al legislatore od alle Corti nazionali l'arduo compito di rinvenirlo nel caso concreto. In questo senso si esprimeva la Corte nel caso Promusicae quando affermava che "*il diritto comunitario richiede che i detti Stati, in occasione della trasposizione di queste direttive, abbiano cura di fondarsi su un'interpretazione delle medesime tale da garantire un giusto equilibrio tra i diversi diritti fondamentali tutelati dall'ordinamento giuridico comunitario. Poi, in sede di attuazione delle misure di trasposizione delle dette direttive, le autorità e i giudici degli Stati membri devono non solo interpretare il loro diritto nazionale in modo conforme a tali direttive, ma anche evitare di fondarsi su un'interpretazione di esse che entri in conflitto con i detti diritti fondamentali o con gli altri principi generali del diritto comunitario, come il principio di proporzionalità*".

Raramente la Corte di Giustizia ha affermato a chiare lettere che il diritto alla tutela della vita privata potesse soccombere quasi totalmente alle esigenze di *enforcement* del diritto d'autore. È l'esempio del caso Bastei Lübbe [610] in cui la Corte giunse a garantire l'identificazione di alcuni utenti, tuttavia argomentando nel senso che sarebbe stato l'unico modo per tutelare i diritti d'autore del loro titolare, essendo impossibile procedere altrimenti.

La richiesta di rinvio pregiudiziale era stata presentata nell'ambito di una controversia tra la Bastei Lübbe GmbH & Co. KG, una casa editrice, e il sig. Michael Strotzer, relativamente ad una domanda di risarcimento per violazione del diritto d'autore mediante condivisione di un audiolibro i cui diritti d'autore appartenevano alla Bastei Lübbe.

Il sig. Michael Strotzer era titolare di una connessione Internet per mezzo della quale, l'8 maggio 2010, il suddetto audiolibro era stato condiviso entro una piattaforma Internet di condivisione (peer-to-peer).

Con lettera del 28 ottobre 2010, la Bastei Lübbe procedeva ad intimare al sig. Strotzer di porre fine alla violazione del diritto d'autore constatata. Risultata vana tale intimazione, la Bastei Lübbe citava in giudizio il sig. Strotzer, in qualità di titolare dell'indirizzo IP da cui era principiata la violazione del diritto d'autore, dinanzi all'Amtsgericht München (Tribunale circoscrizionale, Monaco, Germania) per ottenere un risarcimento in denaro.

Il sig. Strotzer, nel giudizio dinnanzi ai giudici nazionali, negava tuttavia di aver violato, egli stesso, il diritto d'autore. Inoltre, egli adduceva che anche i suoi genitori, con lui conviventi, avevano accesso a tale connessione, ma che, per quanto a sua conoscenza, non disponevano sul loro computer dell'opera in questione, ne ignoravano l'esistenza e non utilizzavano alcun software di piattaforme di condivisione online. In più, il computer dell'interessato sarebbe stato spento al momento in cui avrebbe avuto luogo la violazione del diritto d'autore di cui trattasi. Il punto controverso era dato dal fatto che, secondo la

[609] L. CAMARELLA, *La responsabilità dell'Internet Service Provider alla luce della nuova Direttiva sul diritto d'autore nel mercato unico digitale*, cit., 160 e ss.

[610] CGUE 18 ottobre 2018, Causa C-149/17, *Bastei Lübbe GmbH & Co. KG contro Michael Strotzer*, liberamente consultabile presso: «https://curia.europa.eu/juris/document/document.jsf?text=&docid=206891&pageIndex=0&doclang=IT&mode=lst&dir=&occ=first&part=1&cid=293064» (Ultimo accesso: 10 maggio 2022).

giurisprudenza del Bundesgerichtshof (Corte federale di giustizia), sul titolare della connessione Internet incombe un onere probatorio secondario che può essere soddisfatto dichiarando che altre persone, di cui egli specifichi eventualmente l'identità, avevano un accesso autonomo alla sua connessione Internet e, quindi, avrebbero potuto essere gli autori della violazione del diritto d'autore lamentata. Nell'ipotesi in cui un familiare del titolare della connessione Internet abbia avuto accesso a tale connessione, detto titolare non è tuttavia tenuto a fornire ulteriori precisazioni quanto al momento in cui tale connessione è stata utilizzata e alla natura dell'utilizzo di essa, alla luce della tutela del matrimonio e della famiglia garantita dall'articolo 7 della Carta dei diritti fondamentali dell'Unione europea e dalle pertinenti disposizioni del diritto costituzionale tedesco.

Data la difficoltà della soluzione del caso, con le sue questioni pregiudiziali, il giudice del rinvio chiedeva alla Corte di Giustizia se, da un lato, l'articolo 8, paragrafi 1 e 2, della Direttiva 2001/29, in combinato disposto con l'articolo 3, paragrafo 1, della stessa e, dall'altro, l'articolo 3, paragrafo 2, della Direttiva 2004/48 dovessero essere interpretati nel senso che essi ostano ad una normativa nazionale ai sensi della quale il titolare di una connessione Internet possa non essere considerato responsabile qualora indichi almeno un suo familiare che avesse la possibilità di accedere alla connessione, senza fornire ulteriori precisazioni quanto al momento in cui la medesima connessione è stata utilizzata da tale familiare e alla natura dell'utilizzo che quest'ultimo ne ha fatto.

La Corte di Giustizia, nell'analisi del caso, notava sicuramente come gli Stati membri debbano consentire efficacemente alla parte lesa di ottenere gli elementi di prova necessari a sostegno delle sue affermazioni che si trovino nella disponibilità della controparte, a condizione che la produzione di tali elementi di prova garantisca la tutela delle informazioni riservate. La Corte, tuttavia, notava che il rispetto del diritto fondamentale alla tutela della vita familiare configura un ostacolo che impedisce alla parte lesa di ottenere dalla controparte le prove necessarie per sostenere le proprie affermazioni.

Ad avviso della Corte allora la domanda di pronuncia pregiudiziale sollevava la questione della necessaria conciliazione tra le esigenze inerenti alla tutela di diversi diritti fondamentali, ossia il diritto ad un ricorso effettivo e il diritto di proprietà intellettuale, da una parte, e il diritto al rispetto della vita privata e familiare, dall'altra

La Corte di Giustizia rilevava che "*l'articolo 52, paragrafo 1, della Carta precisa, segnatamente, che eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla Carta devono rispettare il contenuto essenziale di detti diritti e libertà e che dalla giurisprudenza della Corte si evince che una misura che comporti una violazione grave di un diritto tutelato dalla Carta deve considerarsi non conforme all'esigenza di garantire un giusto equilibrio tra i diritti fondamentali che devono essere conciliati*".

La Corte ne ricavava che "*si deve ritenere che, se in situazioni come quelle di cui al procedimento principale la normativa nazionale, nell'interpretazione datane dai giudici nazionali competenti, produce l'effetto di ostacolare la facoltà, da parte del giudice nazionale adito mediante un'azione per responsabilità, di esigere su richiesta dell'attore la produzione e l'ottenimento di elementi di prova relativi ai familiari della controparte, l'accertamento dell'asserita violazione del diritto di autore nonché l'identificazione dell'autore della stessa sono resi impossibili e, conseguentemente, vengono violati in modo grave i diritti fondamentali ad un ricorso effettivo e quelli di proprietà intellettuale, che spettano al titolare del diritto d'autore e, pertanto, l'esigenza di assicurare un giusto equilibrio tra i diversi diritti fondamentali in questione non è rispettata".*

Per queste ragioni, offrendo una protezione quasi assoluta ai familiari del titolare di una connessione Internet, la normativa nazionale non può, in contrasto con quanto prescritto dall'articolo 8, paragrafo 1, della Direttiva 2001/29, essere considerata sufficientemente

efficace e idonea a garantire che, in ultima analisi, all'autore della suddetta violazione sia inflitta una sanzione efficace e dissuasiva.

Quanto sin qui affermato dalla Corte desterebbe sospetto alla luce dell'ampia giurisprudenza citata nel capitolo secondo, considerando che sicuramente una ingerenza nella privacy del sig. Strotzer vi era stata, anche solo al momento della raccolta del suo indirizzo IP, che, è bene ribadire, è sempre un dato personale. Tuttavia, la Corte di Giustizia sottolinea una considerazione che si dimostra essenziale nella nostra analisi, ossia afferma che l'esito del caso "*sarebbe tuttavia diverso se, per evitare un'ingerenza ritenuta inammissibile nella vita familiare, i titolari di diritti potessero disporre di un'altra forma di ricorso effettivo, che in un simile caso consentisse loro, in particolare, di far riconoscere la responsabilità civile del titolare della connessione Internet di cui trattasi*". Emerge chiaramente dunque dalle parole della Corte che la considerazione dell'impossibilità di tutelare il diritto d'autore senza sacrificare almeno in parte il diritto alla privacy non sarebbe possibile. È quindi solo la totale impossibilità ed il totale sacrificio che altrimenti deriverebbe all'*enforcement* del diritto d'autore a far propendere per un bilanciamento di questo genere, altrimenti necessitandosi di rinvenire soluzioni più proporzioniate che non vanifichino nel nucleo essenziale alcuno dei due diritti.

Trasposta la rilevanza del caso nell'ambito dell'art. 17 della Direttiva 2019/790 si comprende come un sacrificio alla tutela della vita privata degli utenti sarebbe lecito ove fosse il solo modo per garantire l'*enforcement* del diritto d'autore e quindi apparisse come l'unica soluzione proporzionata per garantire la giustiziabilità di pretese soggettive. La sorveglianza massiccia richiesta tuttavia dal paragrafo quarto, lettere b) e c) dell'art. 17, non pare integrare i requisiti richiesti dalla sentenza Bastei Lübbe.

La CGUE ha sottolineato in Scarlet Extended[611] che un obbligo generale di filtrare i contenuti illeciti violerebbe il diritto alla protezione dei dati personali. Ciò è dovuto al fatto che il filtraggio automatizzato delle informazioni e il suo utilizzo per identificare i "*pirati della rete*" porta inevitabilmente ad un trattamento dei dati personali e, conseguentemente, consentirebbe l'identificazione dei singoli utenti.

In particolare, nel caso Scarlet, come visto, la Corte di Giustizia si pronunciava affermando che gli effetti di una ingiunzione volta ad imporre un obbligo di sorveglianza, sarebbe stata idonea a ledere anche i diritti fondamentali dei clienti di un *provider*, ed in particolare il loro diritto alla tutela dei dati personali e la loro libertà di ricevere o di comunicare informazioni come tutelati dagli artt. 8 e 11 della Carta.

La Corte si pronuncia nel senso che "*Da un lato, infatti, è pacifico che l'ingiunzione di predisporre il sistema di filtraggio controverso implicherebbe un'analisi sistematica di tutti i contenuti, nonché la raccolta e l'identificazione degli indirizzi IP degli utenti all'origine dell'invio dei contenuti illeciti sulla rete, indirizzi che costituiscono dati personali protetti, in quanto consentono di identificare in modo preciso i suddetti utenti*". A questo poi aggiunge, come abbiamo visto, che "*Dall'altro, detta ingiunzione rischierebbe di ledere la libertà di informazione, poiché tale sistema potrebbe non essere in grado di distinguere adeguatamente tra un contenuto lecito ed un contenuto illecito, sicché il suo impiego potrebbe produrre il risultato di bloccare comunicazioni aventi un contenuto lecito. Infatti, è indiscusso che la questione della liceità di una trasmissione dipende anche dall'applicazione di eccezioni di legge al diritto di autore che variano da uno Stato membro all'altro. Inoltre, in certi Stati membri talune opere possono rientrare nel pubblico dominio o possono essere state messe in linea gratuitamente da parte dei relativi autori*".

[611] CGUE 24 novembre 2011, Causa C-70/10, *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* cit.

La Corte di Giustizia per queste ragioni riconosceva che l'imposizione di un obbligo di filtraggio o di sorveglianza non avrebbe rispettato l'obbligo di garantire un giusto equilibrio fra i diritti fondamentali.

Un'attenta lettura della giurisprudenza indica dunque che i diritti di cui agli articoli 7 e 8 della Carta di Nizza possono essere limitati solo per consentire l'applicazione del diritto d'autore a condizioni rigorose e spesso solo quando è necessaria una restrizione per preservare l'essenza del diritto di proprietà. Ciò lascia spazio al presupposto che il trattamento dei dati personali, e certamente la loro divulgazione, costituiscano restrizioni agli articoli 7 e 8 della Carta molto difficili da giustificare[612].

Geiger e Jütte si esprimono in merito nel senso che il bilanciamento dei diritti fondamentali in relazione all'applicazione del diritto d'autore online dimostra una riluttanza da parte della Corte di Giustizia a dare priorità alla protezione della proprietà intellettuale rispetto ad altri importanti diritti. Diventa evidente che il quadro giuridico che fornisce ai titolari dei diritti strumenti di *enforcement* deve essere rispettoso degli altri diritti fondamentali, come esaminati, le cui restrizioni devono essere sempre esaminate rigorosamente[613].

Gli autori notano poi che rispetto al nuovo meccanismo di responsabilità per gli OCSSP, va tenuto presente che il diritto degli utenti e dei gestori della piattaforma, il diritto alla privacy e alla libertà di espressione, il diritto al giusto processo e a un rimedio effettivo e la libertà di condurre un'impresa, devono essere presi sul serio e che qualsiasi responsabilità della piattaforma deve essere attuata nel rispetto di un giusto equilibrio dei diritti coinvolti. Per quanto legittima sia l'applicazione dei diritti esclusivi protetti dalla legge sul diritto d'autore nel mondo online, non può comportare violazioni significative e sproporzionate degli altri diritti fondamentali. Ne consegue quindi che, secondo gli autori, i titolari dei diritti non possono aspettarsi di essere trattati in modo più favorevole degli utenti e degli operatori di piattaforma[614].

Come segnalato in plurime occasioni, il punto controverso e di maggiore frizione è proprio quello relativo al filtraggio automatico dei contenuti. L'articolo 17 dispone al paragrafo quarto che, per tutti quei contenuti per cui i *provider* non dispongono di una specifica autorizzazione, devono compiere i massimi sforzi per impedirne il caricamento, o, come reazione ad una segnalazione, impedire *pro futuro* il verificarsi di ulteriori violazioni, secondo lo schema del "*notice and stay down*".

---

612 In questo senso si esprimono C. GEIGER, B.J. JÜTTE, *Platform liability under article 17 of the copyright in the Digital Single Market directive, automated filtering and fundamental rights: an impossible match*, cit. 30 e ss.

613 Riprendendo GEIGER C., JÜTTE B.J., *ibidem, 38-39*: "*The balancing of* FR *in relation to online copyright enforcement demonstrates a reluctance on part of the CJEU to give priority to property protection over other important* FR*. It becomes apparent that the legal framework that provides rightholders with enforcement tools needs to be respectful of the* FR *of others, restrictions to which must be always strictly scrutinized. Although the Court does not determine the balance to be struck with finality, it has provided guidelines with which domestic court have to apply national transpositions of the EU rules".*

614Riprendendo GEIGER C., JÜTTE B.J., *ibidem, 38,* "*With respect to the new liability mechanism for OCSSPs, which will be further described and analyzed below, it must be borne in mind that the right of users and platform operators, the right to privacy and freedom of expression, the right to due process and to an effective remedy, and the freedom to conduct a business respectively, have to be taken seriously and that any platform liability must be implemented in compliance with a fair balance of the rights involved. No matter how legitimate the enforcement of exclusive rights protected by copyright law is in the online world, it cannot result in significant and disproportionate infringements of the rights of others and rightholders cannot expect to be treated more favorably than users and platform operators. Therefore, any liability regime for platforms must be designed in a* FR*-compliant manner and safeguards must be included to make* FR *a reality in its practical implementation*".

Alcune tesi dottrinali, tra cui quelle di Senftleben e Angelopuolos,[615] sostengono che l'articolo 17 non richiede agli OCSSP di impegnarsi nel monitoraggio automatizzato di tutti i contenuti notificati dai titolari dei diritti.

Gli autori notano infatti come l'articolo 15 della Direttiva e-commerce disponga che gli Stati membri non possono imporre ai prestatori un obbligo *generale* di sorveglianza sulle informazioni che trasmettono o memorizzano né un obbligo *generale* di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite.

L'argomentazione principale portata avanti da questa dottrina riposa nella considerazione dell'attributo "*generale*" connesso alla sorveglianza, procedendo a distinguere lo stesso, anche troppo sottilmente forse, da un obbligo invece "*specifico*" di sorveglianza, come tale non compreso dalla norma.

Gli autori richiamano tre interpretazioni di ciò che costituisce "monitoraggio generale": (1) un'interpretazione di base che definisce il monitoraggio generale come una situazione in cui tutto il contenuto di una piattaforma è monitorato, anche se solo in relazione a opere specifiche; (2) una situazione in cui è consentito il monitoraggio di tutti i contenuti in relazione a specifiche violazioni ai sensi di un'ingiunzione del tribunale e (3) una situazione in cui è consentito il monitoraggio di tutti i contenuti in relazione a specifiche violazioni ai sensi di una notifica di un'ingiunzione del tribunale da parte di, ad esempio, il titolare del diritto. Quest'ultimo approccio considera l'obbligo di monitorare tutte le informazioni gestite da un intermediario, qualora questo sia stato ordinato da un tribunale per far fronte a un'illegittimità "specifica" e/o tale illegittimità "specifica" sia stata precedentemente portata all'attenzione dell'intermediario tramite una notifica, per esempio dal titolare del diritto[616].

Tuttavia, nella Direttiva e-commerce non viene fornita alcuna definizione di monitoraggio generale. Il Considerando 47 fornisce un'indicazione in questo senso quando afferma che "*gli Stati membri non possono imporre ai prestatori un obbligo di sorveglianza di carattere generale. Tale disposizione non riguarda gli obblighi di sorveglianza in casi specifici e, in particolare, lascia impregiudicate le ordinanze emesse dalle autorità nazionali secondo le rispettive legislazioni*". Del pari, gli autori segnalano anche la rilevanza del Considerando 45, il quale dispone la possibilità di imporre ai *provider* misure inibitorie che obblighino a porre fine a una violazione o impedirla, anche con la rimozione dell'informazione illecita o la disabilitazione dell'accesso alla medesima.

Secondo gli autori, "*sebbene possano essere previste diverse modalità di azione preventiva, l'opzione più ovvia è l'adozione di sistemi di filtraggio, ovvero tecnologie di riconoscimento automatico dei contenuti che*

---

615 M. SENFTLEBEN, C. ANGELOPOULOS, *The Odyssey of the Prohibition on General Monitoring Obligations on the Way to the Digital Services Act: Between Article 15 of the ECommerce Directive and Article 17 of the Directive on Copyright in the Digital Single Market*, cit., 2 e ss.

616M. SENFTLEBEN, C. ANGELOPOULOS, *The Odyssey of the Prohibition on General Monitoring Obligations on the Way to the Digital Services Act: Between Article 15 of the ECommerce Directive and Article 17 of the Directive on Copyright in the Digital Single Market*, cit. 2 e ss., "*(1) Interpretative Option A – 'basic' interpretation: The ban on general monitoring prohibits the imposition of any obligation to monitor all or most of the information handled by an intermediary in general. (2) Interpretative Option B – 'basic minus' interpretation: The ban on general monitoring prohibits the imposition of any obligation to monitor all or most of the information handled by an intermediary only in order to detect and prevent any unlawful activity in general. This interpretation leaves room for the imposition of monitoring obligations concerning all or most of the information handled by the intermediary, if this general monitoring is carried out in search of infringements of a specific right. In other words, according to this approach, the generality or specificity of the monitoring is not determined by what is being monitored, but by the generality or specificity of the subject matter which the monitoring seeks to identify in uploaded content. (3) B2: basic interpretation minus injunctions minus notifications ('basic double minus'): This approach would permit obligations to monitor all the information handled by an intermediary, if that has been ordered by a court to address a 'specific' illegality and/or such a 'specific' illegality has previously been brought to the intermediary's attention via a notification, e.g. by the rightholder."*

elaborano i contenuti gestiti da un intermediario prima o dopo che sono stati pubblicati dall'utente finale, al fine di rilevare ed escludere contenuti illeciti"[617].

L'art. 17 della Direttiva richiede che gli OCSSP garantiscano l'indisponibilità di contenuti protetti da *copyright* o diritti connessi per i quali non dispongano di un'autorizzazione. Come già affermato, a questi fini, i titolari dei diritti devono collaborare con gli OCSSP fornendo le informazioni "pertinenti e necessarie" in relazione a tali lavori, in modo che gli operatori della piattaforma possano adempiere ai propri obblighi.

In una certa misura, preventivamente o come reazione a precedenti violazioni, gli OCSSP dovranno monitorare e filtrare automaticamente lavori specifici. Senftleben e Angelopuolos sostengono quindi che, per queste ragioni, l'articolo 17 non richiede agli OCSSP di impegnarsi nel monitoraggio automatizzato di tutti i contenuti caricati sulla piattaforma.

Ciò significa che il monitoraggio di tutte le informazioni gestite dall'intermediario può essere, per gli autori, "specifico", purché sia mirato alla ricerca di contenuti illegali *pre-identificati*. Questo approccio dispensa dall'obbligo di un'ingiunzione del tribunale e abbraccia qualsiasi notifica, indipendentemente dall'autorità di provenienza (includendo sia l'organo giurisdizionale che i titolari dei diritti), in quanto idonea a far sorgere l'obbligo di monitorare, in tutto o in parte, i contenuti trattati da un intermediario[618].

La tesi proposta dagli autori citati tuttavia non sembra convincente, quantomeno nel contesto di cui trattasi. Sarebbe infatti pretestuoso affermare che il monitoraggio diventa "specifico" per il sol fatto che avverrebbe esclusivamente in ipotesi in cui siano state fornite informazioni dai titolari dei diritti d'autore. Se per avventura tutti i titolari di diritti d'autore esistenti fornissero le informazioni richieste dalla disciplina, si avrebbero ancora i presupposti, o l'audacia, di affermare che il monitoraggio non è generale? Anche non fosse questo il caso, gli insegnamenti dei casi Scarlet Extended v. Sabam[619] e Sabam v. Netlog[620] non verrebbero meno nel caso specifico. Si ricordi infatti che le richieste della Sabam consistevano nel domandare la condanna, a pena di ammenda, a far cessare le violazioni del diritto d'autore sulle proprie opere, rendendo impossibile o bloccando qualsiasi forma di

---

617 M. SENFTLEBEN, C. ANGELOPOULOS, *The Odyssey of the Prohibition on General Monitoring Obligations on the Way to the Digital Services Act: Between Article 15 of the ECommerce Directive and Article 17 of the Directive on Copyright in the Digital Single Market*, cit. 2 e ss., il cui testo originale dispone: "*While a variety of ways of taking preventive action can be envisaged, the most obvious option is the adoption of filtering systems, i.e. automatic content recognition technologies that process content managed by an intermediary either before or after it has been posted by the end user, in order to detect and exclude unlawful conten*t".

618 In questo senso si esprimono M. SENFTLEBEN, C. ANGELOPOULOS, *The Odyssey of the Prohibition on General Monitoring Obligations on the Way to the Digital Services Act: Between Article 15 of the ECommerce Directive and Article 17 of the Directive on Copyright in the Digital Single Market*, cit. 2 e ss., ove affermano che "*This means that the monitoring of all of the information handled by the intermediary may still be 'specific', as long as it is targeted at searching for pre-identified illegal content. This approach dispenses with the requirement of a court order and embraces any notification, regardless of the authority of the origin (including both courts and rightholders), as capable of triggering an obligation to monitor all or most of the content handled by an intermediary*".

619 CGUE 24 novembre 2011, Causa C-70/10, *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM).*

620 CGUE 16 febbraio 2012, causa C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV*, liberamente consulatbile presso: «https://curia.europa.eu/juris/document/document.jsf?docid=119512&doclang=IT» (Ultimo accesso: 10 maggio 2022).

invio o di ricezione da parte dei suoi clienti, mediante programmi *peer-to-peer*, senza autorizzazione dei titolari dei diritti.

Secondo la Corte, l'attuazione di un simile sistema di filtraggio presupponeva (a) che il *provider* identificasse, in primo luogo, nell'insieme delle comunicazioni elettroniche di tutti i suoi clienti, i file che appartenevano al traffico peer-to-peer (b) che esso identificasse, in secondo luogo, nell'ambito di tale traffico, i file che contenevano opere sulle quali i titolari dei diritti di proprietà intellettuale affermavano di vantare diritti; (c) in terzo luogo, che esso determinasse quali tra questi file sono scambiati in modo illecito e, (d) in quarto luogo, che procedesse al blocco degli scambi di file che esso stesso qualificava come illeciti.

In tutta verità, eccetto il punto (a) che non può, per natura, attagliarsi al caso dei prestatori di servizi di condivisione online, ponendo questi in essere una attività intrinsecamente diversa da quella degli *access provider*s, tutti gli altri punti verrebbero invece integrati anche dai sistemi di monitoraggio previsti dall'art. 17. Come notato nel capitolo terzo, un sistema di *Automatic Content Recognition*, basato principalmente sul *fingerprinting*, dato che appare essere la misura che allo stato dell'arte è più diffusa, dovrebbe compiere esattamente quanto sarebbe stato richiesto alla Scarlet.

Come affermato infatti, il processo di *fingerprinting* ha due fasi separate: una prima di generazione dell'impronta, ed una seconda di "confronto" delle impronte digitali. La generazione delle impronte digitali utilizza un peculiare software per analizzare ed estrarre caratteristiche riconoscibili e altre informazioni dal contenuto, quindi, generare una stringa di valori che descrivono le caratteristiche e le informazioni estratte e memorizzare le impronte generate in un database di riferimento. Nell'ambito dell'articolo 17 lettera b) ciò viene compiuto tramite le informazioni "necessarie e pertinenti" che i titolari dei diritti d'autore devono fornire. Sulla base dell'impronta generata, si procede con la fase di confronto delle impronte digitali. Nel fare ciò si analizza ogni singolo contenuto nuovo o sconosciuto dal sistema al fine di generare un'impronta digitale anche di questi. L'impronta digitale generata viene confrontata con tutte le impronte memorizzate nel database di riferimento per vedere se sovviene una corrispondenza. A questo punto l'articolo 17 richiederebbe di bloccare il contenuto o utilizzare altri strumenti, comunque, al fine di impedire la violazione del diritto d'autore. Premesso questo, cosa distingue questa forma di monitoraggio da quella richiesta alla Scarlet? Se la Corte in Sabam ha affermato che l'ingiunzione di predisporre il sistema di filtraggio richiesto "*implicherebbe un'analisi sistematica di tutti i contenuti*" e che ciò è contrario ai diritti alla privacy ed alla vita privata, ad avviso di chi scrive le stesse considerazioni dovrebbero essere compiute per quanto riguarda l'articolo 17.

Parte della dottrina concorda con questa osservazione. Engeler, ad esempio, afferma che nella sentenza Sabam, la Corte di Giustizia dell'Unione europea aveva già affermato che richiedere a un fornitore di servizi di installare un sistema di filtraggio non sarebbe stato conforme al requisito di un giusto equilibrio tra il diritto alla proprietà intellettuale, da un lato, e la libertà di impresa, il diritto alla protezione dei dati personali e la libertà di ricevere o comunicare informazioni, dall'altro. [621] Altri autori segnalano poi che "*è l'ampiezza dell'oggetto del monitoraggio che rappresenta il discrimine tra monitoraggio generale e specifico. Anche filtrare le violazioni*

[621] M. ENGELER, *Copyright Directive: Does the best effort principle comply with GDPR*?, in *Telemedicus. Recht der Informationsgesellschaft*, 23 marzo 2019, disponibile sul sito: «https://www.telemedicus.info/*copyright*-directive-does-the-best-effort-principle-comply-with-gdpr/» (Ultimo accesso: 10 maggio 2022).

di una sola parte di contenuto protetto da copyright da una piattaforma richiede di esaminare tutti i contenuti su tale piattaforma al fine di scoprire tali infrazioni"[622].

In questo contesto, alcuni autori[623] segnalano tuttavia che mentre il filtraggio sarebbe un modo per ottenere gli effetti richiesti dall'articolo 17, paragrafo 4, lettere b) e c) altre misure preventive probabilmente potrebbero essere sufficienti.

Le soluzioni potrebbero essere quelle della sospensione dell'account del singolo autore della violazione od anche una forma di moderazione da parte della comunità, in cui agli utenti viene chiesto di segnalare casi di violazione di materiale protetto e il fornitore rimuove tale materiale in base alle "informazioni pertinenti e necessarie" ricevute da titolari di diritti. Inoltre, gli OCSSP potrebbero distribuire avvisi *popup* o *banner* che avvertono gli utenti della possibile violazione di tale materiale. Misure similari potrebbero essere più idonee al rispetto dei diritti alla privacy degli utenti ed al rispetto della loro vita privata, mentre un obbligo di sorveglianza sarebbe totalmente incompatibile con questi. Senza contare che il legislatore, come segnalato, dispone egli stesso che la Direttiva non pone alcun obbligo di sorveglianza, entrando quindi in contraddizione non solo con la Carta di Nizza, ma persino con se stesso.

Come sottolineano Geiger e Jütte, nel caso dell'articolo 17 sembra difficile immaginare come gli OCSSP possano adempiere ai propri obblighi in modo diverso rispetto all'installazione di sistemi di filtraggio e monitoraggio. "*Sebbene il modo in cui le informazioni vengono fornite all'OCSSP possa variare a seconda del contesto, l'obbligo di garantire l'indisponibilità di alcune opere sarà assolto nel modo più semplice ed efficace filtrando i contenuti sulla base di ampi database di metadati. Di conseguenza, il tipo di monitoraggio che sarà richiesto, o al quale gli OCSSP saranno incentivati per sottrarsi alla responsabilità, molto probabilmente equivarrà a un monitoraggio generale*"[624].

Gli autori aggiungono poi che il "*problema con l'articolo 17 è la sua incompatibilità con i Trattati dell'UE e i principi fondamentali del diritto dell'UE. In primo luogo, le contraddizioni […] trasformano il recepimento dell'articolo 17 in un esercizio estremamente complicato per i legislatori nazionali. È a livello nazionale che dovranno essere prese importanti decisioni normative, che incidono sui diritti fondamentali degli utenti, dei titolari dei diritti e degli operatori di piattaforma. Tuttavia, dopo la sentenza Schrems II è chiaro che tali determinazioni normative ai sensi del diritto dell'UE devono essere effettuate dal legislatore dell'UE e non possono essere lasciate ai parlamenti nazionali. In secondo luogo, il difficile compito affidato ai legislatori nazionali dall'attuale formulazione dell'articolo 17 molto probabilmente non porterà a un livello di armonizzazione che avrebbe giustificato l'esercizio dell'articolo 114 TFUE come base giuridica per l'armonizzazione del mercato interno. Progetti di disegno di legge di attuazione della Direttiva in diversi Stati membri stanno già dimostrando che l'articolo 17 sarà attuato in vari modi divergenti, il che aumenterà la confusione già creata da una disposizione con una formulazione poco chiara e obiettivi contrastanti a scapito della creazione di un vero mercato unico digitale*"[625].

---

[622] L. CAMARELLA, *La responsabilità dell'Internet Service Provider alla luce della nuova Direttiva sul diritto d'autore nel mercato unico digitale*, cit., 188 e ss.

[623] M. SENFTLEBEN, C. ANGELOPOULOS, *The Odyssey of the Prohibition on General Monitoring Obligations on the Way to the Digital Services Act: Between Article 15 of the ECommerce Directive and Article 17 of the Directive on Copyright in the Digital Single Market*, cit., 6 e ss.

[624] Libera traduzione di C. GEIGER C., B.J. JÜTTE *Platform liability under article 17 of the copyright in the Digital Single Market directive, automated filtering and fundamental rights: an impossible match*, 2020, cit., 46. Nel testo originale si rinviene: "*Although the way information is provided to OCSSPS might differ depending on the context, the obligation to ensure the unavailability of certain works will be most easily and effectively discharged by filtering content based on larger databases of metadata. As a result, the type of monitoring which will be required, or to which OCSSPs will be incentivized in order to escape liability will most likely amount to general monitoring* […]"

[625] Libera traduzione di C. GEIGER C., B.J. JÜTTE *Platform liability under article 17 of the copyright in the Digital Single Market directive, automated filtering and fundamental rights: an impossible match*, 2020, cit., 66. "*The problem with Article*

8. Compatibilità con il GDPR

Come abbiamo avuto modo di spiegare, le disposizioni dell'art. 17 paragrafo quarto equivalgono, nei fatti, ad imporre ai prestatori di servizi di condivisione di contenuti online, dei meccanismi di filtraggio automatici in grado di rilevare le possibili violazioni del diritto d'autore sul web, così garantendo meccanismi automatici di *enforcement* del diritto d'autore. Come affermato, un simile obbligo corrisponde ad imporre ai *provider* un obbligo di monitoraggio e di sorveglianza degli utenti sul web, in contraddizione con l'art. 17 paragrafo ottavo, articolo 15 della Direttiva e-commerce, nonché con i diritti garantiti dalla Carta di Nizza.

A queste osservazioni deve aggiungersi allora un ulteriore elemento nella nostra analisi, ossia la compatibilità della disciplina con i principi e le regole previste dal Regolamento UE 679/2016. Si è incoraggiati nel condurre questa analisi dallo stesso fraseggio del legislatore europeo che in più occasioni chiede il rispetto della disciplina europea sul trattamento dei dati personali. In merito ricordiamo che l'art. 17 paragrafo nono statuisce che la Direttiva 2019/790 *"non comporta l'identificazione dei singoli utenti né il trattamento dei dati personali, salvo conformemente alla Direttiva 2002/58/CE e al regolamento (UE) 2016/679*". Parimenti, anche i considerando 70 ed 85 ripropongono le stesse considerazioni nell'affermare che "*qualsiasi trattamento dei dati personali a norma della presente Direttiva dovrebbe rispettare i diritti fondamentali, compresi il diritto al rispetto della vita privata e della vita familiare e il diritto alla protezione dei dati di carattere personale di cui agli articoli 7 e 8 della Carta e deve essere conforme alla Direttiva 2002/58/CE e al regolamento (UE) 2016/679*".

Eppure, il legislatore non sembra tenere in considerazione che l'utilizzo di simili tecnologie di filtraggio impone proprio il trattamento dei dati personali che il fraseggio della Direttiva invece tendenzialmente escluderebbe. Una parte della dottrina, infatti, ricorda come la tecnologia richiesta soddisferebbe le disposizioni della Direttiva sul diritto d'autore solo quando non solo è in grado di riconoscere il contenuto (l'immagine, l'audio o il file di testo effettivo), ma anche il contesto del caricamento[626]. Tale "contesto" del caricamento dei contenuti in violazione dei diritti d'autore richiederebbe informazioni sulle circostanze dello stesso che rivelano dati degli utenti classificabili come "personali". Non che il trattamento di dati personali non sia possibile in questi contesti, anzi, spesso si rivela essenziale al funzionamento delle piattaforme stesse e del loro modello di business. Chiaramente però è necessario investigare su quale base giuridica tale trattamento potrebbe avvenire ed essere

---

17 is its incompatibility with the Treaties of the EU and the fundamental basic principles of EU law. First, the contradictions and vague concepts which we have exposed above turn the transposition of Article 17 into an extremely complicated exercise for national legislators. It is at the national level where important normative decisions will have to be made, which impact on the fundamental rights of users, rightholders and platform operators. However, after the Schrems II ruling it is clear that such normative determinations under EU law must be made by the EU legislator and cannot be left to national parliaments. Second, the difficult task left to national legislators under the current formulation of Article 17will very likely not lead to a level of harmonization that would have justified the exercise of Article 114 TFEU as legal basis for internal market harmonization. Draft implementation bills of the Directive in several Member States are already showing that Article 17 will be implemented in various diverging ways, which will augment the confusion already created by a provision with unclear wording and conflicting aims to the detriment of the creation of a true Digital Single Market." Gli autori citano a proposito: P. KELLER, *Divergence instead of guidance: the Article 17 implementation discussion in 2020 – Part 1*, in *Kluwer Copyright Blog*, 2020 liberamente accessibile presso: «http://*copyright*blog.kluweriplaw.com/2021/01/21/divergence-instead-of-guidance-the-article-17-implementation-discussion-in-2020-part-1/» (Ultimo accesso: 10 maggio 2022).

[626] M.ENGELER, *Copyright Directive: Does the best effort principle comply with GDPR*?, in *Telemedicus. Recht der Informationsgesellschaft*, 2019, disponibile sul sito: «https://www.telemedicus.info/*copyright*-directive-does-the-best-effort-principle-comply-with-gdpr/» (Ultimo accesso: 10 maggio 2022).

giustificato, nonché se l'eventuale lecito trattamento rispetti i principi e le regole in materia di privacy previste dal GDPR.

Il primo punto da investigare è l'applicabilità della disciplina del GDPR ai prestatori di servizi di condivisione di contenuti online previsti dall'articolo 17 della Direttiva 2019/790.

L'articolo 2 del GDPR stabilisce l'ambito di applicazione materiale del Regolamento, definendo che coinvolge il "*trattamento interamente o parzialmente automatizzato di dati personali e il trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi*". Alcune attività sono estranee a questa disciplina ed elencate sempre dall'art. 2, tuttavia nessuna di queste pare potersi applicare agli OCSSP[627].

Per quanto invece riguarda l'ambito di applicazione territoriale non vi sono dubbi che il GDPR possa applicarsi ai *provider* previsti dall'art. 2 punto 6 della Direttiva 2019/790. Se il monitoraggio avviene nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento nell'Unione o anche al di fuori della stessa, si applicherebbe il Regolamento, alla peggio per la previsione della lettera b) dell'art. 3 GDPR che prescrive l'applicabilità del Regolamento in ogni caso quando l'attività di un *provider* comporti il monitoraggio del comportamento degli interessati al trattamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione.

Si deve affermare poi che la caratteristica soggettiva di "titolare del trattamento" deve essere attribuita alle piattaforme di condivisione di contenuti online sulla base della considerazione per cui un titolare è "*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri*". Dato il ruolo attribuito dall'articolo 17 agli OCSSP, essi devono essere identificati come titolari del trattamento. In questa considerazione si è anche sostenuti da parte della dottrina che ritiene che "*l'obbligo di implementare meccanismi di prevenzione del caricamento ai sensi dell'art. 17 par. 4 della Direttiva sul diritto d'autore richiede ai fornitori di servizi di dimostrare i loro migliori sforzi. L'onere effettivo della decisione sulle tecnologie da implementare è quindi a carico dei fornitori di servizi che in cambio li qualifica come titolari del trattamento secondo il GDPR. A seconda dell'effettiva implementazione tecnica, ci sarà ovviamente spazio per una "contitolarità" o per i rapporti titolare-responsabile del trattamento con i fornitori di servizi di filtraggio*"[628].

Sicuri quindi della possibile applicazione materiale, territoriale e soggettiva del Regolamento agli OCSSP, rimane da investigare se effettivamente l'attività da essi posta in essere si configuri o meno come un "trattamento dei dati personali". Infatti, anche la stessa Commissione non pare del parere che le tecnologie di filtraggio impongano attività da

---

[627] *"Il presente regolamento non si applica ai trattamenti di dati personali:*
a)effettuati per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione;
b)effettuati dagli Stati membri nell'esercizio di attività che rientrano nell'ambito di applicazione del titolo V, capo 2, TUE;
c)effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico;
d)effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse".

[628] Traduzione libera di M. ENGELER, *Copyright Directive: Does the best effort principle comply with GDPR*?, cit., il quale, nel testo originale, scrive: "*The obligation to implement upload prevention mechanisms compliant to Art. 17 para. 4 Copyright Directive requires service providers to demonstrate their best efforts. The actual burden of the decision which technologies to implement is therefore put on the service providers which in return qualifies them as controllers according to the GDPR. Depending on the actual technical implementation there will of course be room for joint controllership or controller-processor-relationships with providers of filtering services*".

compiersi sui dati degli utenti. Le linee guida in questo senso affermano proprio che "*in linea di principio l'uso di tecnologie come il riconoscimento dei contenuti non dovrebbe di per sé rendere necessaria l'identificazione degli utenti che caricano i loro contenuti; se però questo è il caso, devono essere rispettate le pertinenti norme in materia di protezione dei dati, compresi i principi di minimizzazione dei dati e limitazione delle finalità*"[629].

Engeler nota come effettivamente si potrebbe sostenere che i meccanismi di filtraggio dovrebbero principalmente rilevare e confrontare un dato contenuto caricato e protetto da *copyright* con un database di autorizzazioni per determinare se il caricamento di un determinato contenuto può procedere o deve essere bloccato. Tale filtraggio, afferma, potrebbe, a prima vista, essere possibile senza elaborare le informazioni sull'utente che tenta il caricamento. Ciò, tuttavia, sarebbe vero solo fintanto che è possibile determinare se un contenuto è coperto da una particolare licenza senza informazioni che vanno oltre la conoscenza del contenuto stesso[630]. L'ipotesi potrebbe essere infatti quella per cui, sulla base del primo paragrafo dell'art. 17, un titolare dei diritti d'autore abbia concesso in licenza il caricamento delle proprie opere, motivo per cui il sistema non avrebbe altro da fare che confrontare il contenuto da caricare con quello autorizzato e "lasciarlo passare". Questo non è il caso però delle altre disposizioni dell'art. 17, in quanto "*il contesto del caricamento è estremamente rilevante per determinare se un caricamento specifico, pur non essendo coperto da un contratto di licenza, è coperto dall'art. 17 par. 7 della Direttiva*"[631].

In questo senso quindi, Engeler nota che il rilevamento automatico di parodie, citazioni o critiche è, se possibile, fortemente dipendente dalla conoscenza delle circostanze del caricamento. Lo stesso contenuto, nota, può essere caricato legalmente come parte di una critica cinematografica in uno scenario, mentre potrebbe non essere così in un altro caso. Il rilevamento della parodia dipende infatti dalle meta-informazioni sul caricamento. Engeler nota che un video protetto da *copyright* (ad esempio una clip pubblicitaria) potrebbe essere vista come una parodia in un momento (ad esempio dopo che detti prodotti si sono rivelati altamente dannosi) ma non in un altro. L'identità, il luogo, la data e l'ora di un caricamento sarebbero quindi rilevanti per l'elaborazione da parte dei meccanismi di filtraggio.

Christoph Schmon afferma inoltre che i "*dati trasmessi durante il processo di registrazione sono dati personali, rendendosi quindi inevitabile l'applicazione del GDPR all'eventuale trattamento effettuato dai filtri. Anche i contenuti postati in forma anonima sarebbero comunque corredati da metadati, come ad esempio l'indirizzo IP […], che può essere utilizzato per identificare l'utente. L'anonimizzazione è tecnicamente difficile da ottenere e, in ogni caso, non potrà aversi se il contenuto è collegato ad un profilo su Facebook o a un account su Youtube*"[632].

Tali informazioni sono quindi da considerarsi "dati personali" ai sensi dell'art. 4 n. 1 GDPR, essendo informazioni riguardanti una persona fisica identificata o identificabile, e la loro analisi un "trattamento", ai sensi dell'art. 4 n. 2 GDPR comprendendo quest'ultimo *"qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e*

---

[629] Communication From The Commission To The European Parliament And The Council: Guidance on Article 17 of Directive 2019/790 on Copyright in the Digital Single Market COM/2021/288 final, cit.

[630] M. ENGELER, *Copyright Directive: Does the best effort principle comply with GDPR*?, cit.

[631] Traduzione libera di M. ENGELER, *Copyright Directive: Does the best effort principle comply with GDPR*?, cit., il cui testo originale dispone: "*This is not the case with the Copyright Directive as the context of the upload is highly relevant to determine whether a specific upload – while not being covered by a license agreement – is covered by Art. 17 para. 7 Copyright Directive".*

[632] C. SCHMON, *Filtri automatici e privacy: la tempesta perfetta*, 3 marzo 2020, in *Electonic Frontier Foundation*, nella traduzione di R. DUCATO con la collaborazione di P. GUARDA, 21 marzo 2020, liberamente accessibile presso: «https://www.eff.org/it/deeplinks/2020/02/upload-filters-are-odds-gdpr» (Ultimo accesso: 10 maggio 2022).

applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione".

Il diritto europeo chiede poi che sussista una base legale per il trattamento dei dati personali in questione. Queste, come affermato nel capitolo terzo, di cui si richiamano per rimando le osservazioni, sono rinvenibili all'art. 6 del GDPR. Questo articolo dispone che le possibili basi legali per un lecito trattamento sono, riassumendo: (a) il consenso al trattamento dei propri dati personali per una o più specifiche finalità; (b) l'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;(c) obbligo legale al quale è soggetto il titolare del trattamento; (d) salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica; (e) l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento; (f) il legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali.

Si potrebbe argomentare di basare il necessario trattamento dei dati sul consenso (art. 6 punto 1a GDPR) o di farne parte dei termini di servizio (art. 6 punto 1b GDPR). Entrambe le opzioni sembrano inadatte però. Engeler nota che difficilmente il consenso sarebbe considerato liberamente prestato ai sensi dell'art. 7 par. 4 GDPR in quanto l'obbligo legale di conformarsi alla Direttiva sul diritto d'autore deve essere soddisfatto da tutti i servizi, il che in cambio porta a una mancanza di alternative. Rendere i filtri di caricamento parte dell'accordo contrattuale, d'altro canto, sembra altrettanto problematico in quanto una possibile clausola di filtraggio di caricamenti dovrebbe superare la prova della legge sulla protezione dei consumatori e potrebbe essere considerata nulla nella misura in cui va oltre ciò che è legalmente richiesto. Per quanto richiesto dalla legge, tale clausola sarebbe d'altronde semplicemente superflua. L'unica base legale che, secondo Engeler, meriterebbe di essere investigata è quella dell'articolo 6 lettera c) del GDPR, ossia quella riguardante l'obbligo legale al quale è soggetto il titolare del trattamento[633].

Parte della dottrina allora nota che i prestatori di servizi di condivisione di contenuti online avranno chiari incentivi ad attuare meccanismi di filtraggio piuttosto estesi in quanto il mancato rispetto dell'art. 17 paragrafo quarto, lettere b) e c), comporta la responsabilità per tutti i contenuti caricati dagli utenti. Data la complessità tecnica dei meccanismi che si ritengono addirittura in grado di soddisfare le elevate esigenze dell'art. 17 ed il pericolo di responsabilità connesso, "*sembra probabile che i fornitori soprattutto più piccoli, nonostante l'art. 17 par. 5 Direttiva sul diritto d'autore – scelgano di implementare servizi di terze parti offerti da piattaforme che hanno esperienza con tecnologie come l'algoritmo Content ID di Google (tuttavia, anche queste tecnologie all'avanguardia sono ancora insufficienti). Allo stesso modo in cui la piattaforma pubblicitaria centralizzata di Google AdSense ha visto un'adozione diffusa, questo potrebbe essere anche il caso delle sue tecnologie di filtraggio*"[634]. Le questioni legali, in particolare nell'area della protezione dei dati, sarebbero simili: come le reti pubblicitarie centralizzate richiedono al fornitore della rete di elaborare i

633 M. ENGELER *Copyright Directive: Does the best effort principle comply with GDPR*?, cit.

634 In questo senso si esprime M. ENGELER, *ibidem,* il quale afferma, letteralmente che "*it seems likely that especially smaller providers will – notwithstanding Art. 17 para. 5 Copyright Directive – choose to implement third party services offered by platforms that have experience with such technologies like Googles Content ID algorithm (however insufficient even these state-of-the-art technologies still are). In the same way Googles centralized advertisement platform AdSense has seen widespread adoption, this could be the case with its filtering technologies, too.*"

dati personali dei visitatori del sito Web, del pari pure i servizi di filtraggio richiederebbero il trattamento dei dati personali degli utenti che caricano materiale protetto da *copyright*.

Ciò porterebbe a che effettivamente pochi grandi fornitori di servizi sarebbero in grado di elaborare informazioni su circostanze, data, ora e contenuto dei caricamenti effettuati della maggior parte degli utenti[635]. La considerazione non è peregrina, tanto che Maria Chiara Pievatolo[636] ha efficacemente affermato che "*Non paradossalmente né sorprendentemente Alphabet, che controlla Google, ha già prodotto e reso disponibile sul mercato un sistema di filtri di caricamento per chi non desidera acquistare quello offerto da Audible Magic, la quale a sua volta ha fatto lobbying a favore dell'ex articolo 13 ora 17. In generale, Facebook, Apple, Microsoft e Google saranno avvantaggiati dal regime europeo, perché i suoi costi e oneri soffocheranno i loro potenziali concorrenti nella culla: l'Internet dei media sociali proprietari centralizzati e manipolatori – che a parole preoccupa il legislatore europeo – ne uscirà rafforzato. Del resto, l'interesse degli editori e dei produttori multimediali che hanno sostenuto la direttiva non è propriamente la demolizione degli oligopoli: è la partecipazione ai loro profitti, anche a costo di farsi disegnare un regime ormai più simile al sistema protomoderno del privilegio librario che al copyright dello Statute of Anne. Anche allora – contro la libertà di espressione di tutti gli altri – l'interesse politico alla censura si sposava con l'interesse economico al monopolio, ma con una differenza: nel XVI secolo a nessuno sarebbe venuto in mente di imporre una censura privata preventiva al solo scopo di compensare gli scriptoria incapaci di stare al passo con la stampa*".

Con riferimento allora all'art. 6 lettera c) del GDPR, un simile ragionamento porterebbe alla conclusione che la Direttiva 2019/790 si tradurrebbe in un obbligo legale di implementare tecnologie che richiedono infrastrutture di filtraggio centralizzate. Questo in quanto soluzioni altrettanto efficaci ma meno estese, come meccanismi di filtraggio implementati "localmente" difficilmente sarebbero in grado di dimostrare il possesso dei requisiti imposti dalla Direttiva, men che meno, ad esempio, la capacità tecnica di rilevare sufficientemente le eccezioni dell'art. 17 paragrafo settimo.

I massimi sforzi imposti per impedire i caricamenti ai sensi dell'art. 17 par. quarto lettere b) e c) deve quindi essere visto come un obbligo legale che si pone tendenzialmente in contrasto con gli artt. 7 e 8 della Carta di Nizza. I titolari del trattamento "*sono invitati a scegliere tra due rischi ugualmente inaccettabili: il trattamento dei dati senza fondamento giuridico perché l'art. 17 par. 4b e 4c Direttiva sul diritto d'autore non soddisfa i requisiti dell'art. 6 GDPR o affrontare la responsabilità dell'art. 17 par. 4*[637]".

Ove si rinvenisse una base legale per il trattamento dei dati personali, altre due questioni sorgerebbero nel porre in essere un simile trattamento dei dati personali. La prima questione riguarda quanto disposto dall'art. 22 GDPR sulle decisioni automatizzate e sulla profilazione, sui cui rilievi ci si è già spesi nel precedente capitolo e cui si rimanda interamente la trattazione[638]. In questa sede basti richiamare quanto ricorda Christoph Schmon ove

---

635 Così afferma infatti M. ENGELER, *ibidem*.

636 M.C. PIEVATOLO, *L'età del privilegio: il diritto d'autore nel mercato unico digitale europeo*, in *Archivio Marini*, 2019, «www.rivistailmulino.it/news/newsitem/index/Item/News:NEWS_ITEM:4675» (Ultimo accesso: 10 maggio 2022).

637 In questo senso si esprime M. ENGELER *Copyright Directive: Does the best effort principle comply with GDPR*?, cit., il quale afferma, letteralmente che "*The mandated best efforts to prevent uploads according to Art. 17 para. 4b and 4c Copyright Directive must therefore be seen as a legal obligation that is in violation of Art. 7 and Art. 8 CFR and controllers are asked to choose between two equally unacceptable risks: Processing data without a legal basis because Art. 17 para. 4b and 4c Copyright Directive does not meet the requirements of Art. 6 GDPR or face the liability Art. 17 para. 4 Copyright Directive imposes on them*"

638 Per maggiori informazioni sulle decisioni algoritmiche ed il rapporto che queste istaurano con la normativa a tutela dei dati personali si veda G. ALPA, G. RESTA, *Le persone e la Famiglia 1, Le persone fisiche e i diritti della personalità*, in Trattato di Diritto Civile (a cura di R. SACCO), Milano, 2019, 515-520.

afferma che i processi decisionali automatizzati richiesti dall'articolo 17 della Direttiva "*implicano una decisione sul "se" uno specifico utente sia autorizzato a condividere un determinato contenuto. Che il post caricato corrisponda ai patterns e alle informazioni fornite dai titolari dei diritti è solo un passaggio intermedio dell'intero processo. I filtri potrebbero inoltre non utilizzare necessariamente dati personali per determinare se rimuovere un contenuto, ma la decisione riguarda in ogni caso cosa un determinato individuo possa o non possa caricare sulla piattaforma. In altri termini: un sistema che monitora e rimuove contenuti, i quali possono contenere le opinioni e le convinzioni degli utenti stessi, può davvero consistere in decisioni che non riguardano gli utenti stessi?"* [639].

Una seconda questione riguarda il rispetto di alcuni principi generali in merito al trattamento dei dati personali che anche i prestatori di servizi di condivisione dei contenuti online sono tenuti a rispettare. L'articolo 5 GDPR prescrive infatti sei principi che i *provider* devono tenere a mente e rispettare.

In virtù del primo paragrafo dell'art. 5, i dati personali devono essere trattati in modo "*lecito, corretto e trasparente*" nei confronti dell'interessato, ma anche essere esatti e, se necessario, aggiornati nonché sicuramente anche trattati in maniera da garantire un'adeguata sicurezza, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali. Dei vari principi espressi dal primo paragrafo, ad avviso di chi scrive, quelli su cui i *provider* dovrebbero fare maggiore attenzione sono i principi di (a) minimizzazione; (b) limitazione delle finalità; e (c) limitazione della conservazione.

Il primo fra questi dispone che i dati personali devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati. Nel caso concreto questo significa che i prestatori di servizi di condivisione dei contenuti online dovrebbero limitare il loro trattamento solamente a quei dati strettamente necessari al funzionamento tecnico dei sistemi di filtraggio, senza trasmodare nella raccolta degli stessi per finalità ultronee rispetto a quelle dichiarate. Il Gruppo di Lavoro Articolo 29 aveva, in altre occasioni, anche affermato che, date le opportunità commerciali create da costi di memorizzazione più economici e dalla capacità di trattare grandi quantità di informazioni, le organizzazioni potrebbero essere incoraggiate a "*raccogliere più dati personali di quelli di cui hanno effettivamente bisogno, poiché tali dati potrebbero rivelarsi utili in futuro*[640]". Per evitare di incorrere in questi rischi il Gruppo sostiene che "*Il titolare del trattamento dovrebbe essere in grado di spiegare in maniera chiara e giustificare la necessità della raccolta e della conservazione dei dati personali oppure prendere in considerazione l'utilizzo di dati aggregati, anonimizzati o […] pseudonimizzati […].*[641]" In secondo luogo, poi si chiede che i dati personali siano raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità. L'ultimo requisito che si deve ritenere applicabile impone che i dati siano conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati.

Come ricorda Christoph Schmon quindi, "*gli effetti negativi sugli utenti sottoposti a processi decisionali automatizzati e le incertezze giuridiche legate all'applicazione dei filtri automatici dovrebbero*

---

639 C. SCHMON, *Filtri automatici e privacy: la tempesta perfetta*, cit.

640 Gruppo Di Lavoro Articolo 29 Per La Protezione Dei Dati; Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del Regolamento 2016/790; 17/IT WP 251 rev.01, adottate il 3 ottobre 2017; versione emendata e adottata in data 6 febbraio 2018, accessibili presso: «https://ec.europa.eu/newsroom/article29/items/612053» (Ultimo accesso: 10 maggio 2022).

641 Gruppo Di Lavoro Articolo 29 Per La Protezione Dei Dati; Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del Regolamento 2016/790; 17/IT WP 251 rev.01,cit.

indurre i legislatori nazionali ad un approccio volto alla minimizzazione dei rischi (anche) privacy per i soggetti coinvolti. Le implementazioni a livello nazionale dovrebbero tenere conto, in particolare, dei diritti alla privacy e alla protezione dei dati personali, della libertà di espressione e degli altri diritti fondamentali, di modo che appropriate misure di garanzia e salvaguardia siano poste in essere prima che un upload sia valutato, bloccato o rimosso"[642].

Solo ove si rispettino, pur nelle difficoltà segnalate, tutti i requisiti del trattamento corretto dei dati personali, come imposti dal GDPR ed esplicitati nel presente capitolo e nel precedente, allora si potrà ritenere legittimo un trattamento dei dati personali degli utenti. Per concludere la presente trattazione, volta a mostrare il delicato bilanciamento che chiede di porre in essere l'art. 17 della Direttiva 2019/790, è necessario fare riferimento a come questi ragionamenti sono stati trasposti nella pratica. L'attenzione deve quindi cadere sul ricorso proposto dalla Repubblica di Polonia, deciso con recente pronuncia della Corte di Giustizia del 26 aprile 2022.

9. Il ricorso della Polonia e le Conclusioni dell'Avvocato Generale nella Causa C-401/2019

Il 24 maggio del 2019 la Repubblica di Polonia, affermando l'illiceità della disciplina prevista dall'art. 17 della Direttiva 2019/790, ha deciso di proporre un ricorso alla Corte di Giustizia ai sensi dell'art. 263 del TFUE per sentir dichiarare dalla stessa l'illegittimità della Direttiva, nella parte concernente proprio l'articolo 17.

Nello specifico, la Repubblica di Polonia chiedeva l'annullamento dell'articolo 17, paragrafo 4, lettera b) e c), ed in subordine, qualora la Corte di Giustizia avesse dovuto ritenere che le disposizioni impugnate non potessero essere separate da altre disposizioni contemplate complessivamente nell'articolo 17 senza alterare la sostanza della disciplina contenuta in tale articolo, chiedeva l'annullamento *in toto* dell'articolo 17 della Direttiva (UE) 2019/790[643].

Argomentando avverso le disposizioni impugnate, la Polonia deduceva a motivo della richiesta di declaratoria di illegittimità la violazione del diritto alla libertà di espressione e di informazione, garantito, come visto, dall'articolo 11 della Carta di Nizza.

La Repubblica di Polonia, nel suo ricorso, sosteneva dunque che l'assoggettamento dei prestatori di servizi di condivisione di contenuti online all'obbligo di compiere i "massimi sforzi" per assicurare che non siano disponibili opere e altri materiali specifici per i quali abbiano ricevuto le informazioni pertinenti e necessarie dai titolari dei diritti (articolo 17, paragrafo 4, lettera b), nonché l'imposizione di compiere i massimi sforzi per impedire il caricamento in futuro delle opere che sono state oggetto di una "segnalazione sufficientemente motivata" da parte dei titolari dei diritti, avrebbe implicato, in sostanza, un meccanismo di filtraggio e di controllo preventivo delle attività degli utenti. Secondo la Polonia, un siffatto meccanismo avrebbe pregiudicato l'essenza del diritto alla libertà di espressione e di informazione e non avrebbe soddisfatto i requisiti di proporzionalità e di necessità nella limitazione di tale diritto.

---

642 C. SCHMON, *Filtri automatici e privacy: la tempesta perfetta*, cit.

643 Ricorso proposto il 24 maggio 2019 — Repubblica di Polonia/Parlamento europeo e Consiglio dell'Unione europea (Causa C-401/19), liberamente consultabile presso: «https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:62019CN0401&from=EN» (Ultimo accesso: 10 maggio 2022).

Per una completa comprensione delle ragioni che hanno mosso la Repubblica di Polonia e per una miglior disamina della pronuncia della Corte di Giustizia sul ricorso stesso si ritiene necessario partire dalle Conclusioni presentate dall'Avvocato Generale Henrik Saugmandsgaard Øe[644], in gran parte confermate dalla successiva pronuncia della Grande Sezione. In questo, si segnala sin da ora che il richiamo esclusivo alla compressione della libertà di espressione, ad avviso di chi scrive, non è stato sufficiente, dovendosi, come precedentemente reso evidente, sollevare la questione di illegittimità anche alla luce, quantomeno, della libertà di impresa e della privacy, capaci, forse, di sovvertire il bilanciamento in senso opposto a quello che vedremo risultare dalle parole dell'Avvocato Generale e dalla Corte di Giustizia.

Secondo una corretta e consueta scansione delle questioni di rito e delle questioni di merito, l'Avvocato Generale parte nelle sue conclusioni dalla ricevibilità del ricorso, utile per comprendere la portata delle richieste della Polonia. In questo contesto, l'Avvocato ricorda che, in conformità ad una costante giurisprudenza della Corte, l'annullamento parziale di un atto dell'Unione è possibile solo se gli elementi di cui è chiesto l'annullamento sono separabili dal resto dell'atto. Tale requisito, nel caso concreto non è soddisfatto quando un siffatto annullamento parziale avrebbe l'effetto di modificarne la sostanza. Sulla domanda proposta in subordine, l'Avvocato Generale invece si esprime affermando, per contro, che è ricevibile. Infatti, per quanto importante sia tale articolo, il suo annullamento non modificherebbe la sostanza di tale Direttiva. I numerosi articoli della stessa hanno oggetti diversi e sono ripartiti in titoli e capi differenti. L'articolo 17 di detta Direttiva è, pertanto, separabile dagli altri suoi articoli, i quali potrebbero senz'altro sussistere in caso di annullamento del primo.

La medesima conclusione viene sostenuta negli stessi termini anche dalla Corte di Giustizia, dichiarando infatti irricevibile il ricorso proposto in via principale, accogliendo in rito, quindi dichiarando ricevibile, quello proposto in subordine[645].

Passando invece al merito, l'Avvocato Generale deve risolvere la questione controversa consistente nel fatto che l'obbligo di sorveglianza preventiva imposto, come visto, ai *provider*, costituirebbe, secondo la Polonia, una limitazione nell'esercizio del diritto alla libertà di espressione, garantito all'articolo 11 della Carta. Tale limitazione non sarebbe compatibile con siffatto strumento poiché arrecherebbe pregiudizio al "contenuto essenziale" di tale diritto fondamentale o, quantomeno, non rispetterebbe il principio di proporzionalità. Quanto viene chiesto costituisce dunque la ricerca, ancora una volta, di un bilanciamento fra l'*enforcement* del diritto d'autore sul web e la tutela della libertà di espressione. Purtroppo, come detto, non venne sollevata alcuna censura dalla Polonia con riguardo agli articoli 7 od 8 della Carta di Nizza.

Innanzitutto, le considerazioni sugli obblighi di sorveglianza imposti dalla Direttiva sono confortanti, nel senso che l'Avvocato riconosce espressamente che quanto richiesto dalle lettere b) e c) del quarto paragrafo dell'art. 17 è una obbligazione imponente di predisporre tecnologie di riconoscimento automatico, cosa che il legislatore si astiene, come visto, dall'affermare, ma che implicitamente sottende. L'avvocato infatti, onestamente, ammette che "*mi sembra che le disposizioni impugnate effettivamente obblighino i prestatori di servizi di condivisione, in numerose situazioni, ad utilizzare tali strumenti di riconoscimento di contenuto. A mio*

[644] Avvocato Generale Henrik Saugmandsgaard Øe, conclusioni presentate il 15 luglio 2021 nella Causa C-401/19, Repubblica di Polonia contro Parlamento europeo, Consiglio dell'Unione europea, ricorso presentato ex art. 263 TFUE, cit.

[645] CGUE 26 aprile 2022, C-401/2019, Repubblica di Polonia contro Parlamento europeo, Consiglio dell'Unione europea, cit., par. 16 e ss.

avviso, il legislatore dell'Unione ha semplicemente cambiato metodo fra la proposta di Direttiva e la sua adozione quale Direttiva 2019/790. Piuttosto che prevedere direttamente un obbligo di predisporre tali strumenti, esso li ha imposti indirettamente, tramite le condizioni di esenzione da responsabilità previste a tali disposizioni". Su questo punto, come visto, non si può che concordare con quanto affermato. Tanto che anche l'Avvocato Generale si esprime affermando "*non vedo con quali mezzi, se non con l'utilizzo di uno strumento di riconoscimento automatico che consente loro di filtrare i contenuti caricati sui loro servizi, tali prestatori potrebbero ragionevolmente «assicurare che non siano disponibili» opere e materiali protetti identificati dai titolari dei diritti e «impedirne il caricamento in futuro» sui loro servizi, in conformità agli obiettivi di cui alle disposizioni impugnate – e il riferimento del Parlamento e del Consiglio ad eventuali «soluzioni innovative» apporta in proposito un aiuto solo relativo. Del resto, le parti convenute e gli intervenienti hanno ammesso a malincuore, in udienza, in risposta ai quesiti della Corte, che tali strumenti saranno, molto spesso, de facto, indispensabili al riguardo*"[646].

In precedenza, si è avuto modo di sostenere che l'articolo 17 entrasse in conflitto frontalmente con la libertà di espressione, come protetta dalla Carta di Nizza. In quella sede si è avuto altresì modo di constatare come difficilmente il diritto degli utenti potrebbe essere compresso, dovendo in ogni caso essere rispettato un contenuto essenziale dello stesso, probabilmente violato dai sistemi di sorveglianza. Secondo la Polonia, infatti, le misure di filtraggio che i prestatori di servizi di condivisione sono costretti a predisporre costituirebbero, per loro natura, "misure preventive" di controllo delle informazioni degli utenti. Tali misure darebbero luogo a "restrizioni ex ante", trasmodanti in una censura generale automatizzata di natura preventiva. Dette disposizioni costituirebbero in questo senso un'ingerenza del legislatore dell'Unione nella libertà di espressione e di informazione di detti utenti sufficientemente grave, secondo la Polonia, da giustificarne una declaratoria di illegittimità.

Secondo l'Avvocato Generale, effettivamente il filtraggio è, per sua natura, una misura preventiva di controllo delle informazioni, e le misure di blocco che possono conseguirne costituiscono restrizioni *ex ante*, come definito dallo Stato polacco. Da ciò consegue, secondo l'Avvocato Generale, che in tali situazioni, "*gli utenti non sono dunque «liberi» di mettere in rete i contenuti desiderati sui servizi di condivisione. Le misure di filtraggio e di blocco attuate dai loro prestatori restringeranno i contenuti che essi possono caricare. Ne consegue un'«ingerenza» nell'esercizio della libertà di comunicazione di detti utenti. Il filtraggio e il blocco di contenuti prima della loro diffusione comportano, inoltre, un'«ingerenza» nella libertà del pubblico di ricevere informazioni*".

Come notato nelle pagine precedenti, anche in sede di conclusioni dell'Avvocato Generale si nota, pragmaticamente, che, dato che è palese che i prestatori di servizi di condivisione non possono materialmente ottenere un'autorizzazione per tutti i materiali protetti da diritto d'autore esistenti, e che gli utenti possono comunque mettere in rete quantità di contenuti che riproducono i materiali in questione, "*il ricorso al meccanismo di esenzione previsto all'articolo 17, paragrafo 4, della Direttiva 2019/790 sarà, per tali prestatori, non una «possibilità», bensì una necessità, pena sopportare un rischio di responsabilità smisurato. Pertanto, in un elevato numero di casi, le condizioni di esenzione previste alle disposizioni impugnate costituiranno, in pratica, veri e propri obblighi per detti prestatori*".

Il punto che desta maggiore interesse è chiaramente quello concernente il bilanciamento fra diritto di proprietà intellettuale e la libertà di pensiero, condotto, alla luce

[646] Paragrafi da 57 a 69; Avvocato Generale Henrik Saugmandsgaard Øe, conclusioni presentate il 15 luglio 2021 nella Causa C-401/19, Repubblica di Polonia contro Parlamento europeo, Consiglio dell'Unione europea, ricorso presentato ex art. 263 TFUE, cit.

delle norme europee, secondo il principio di proporzionalità. Sulla base dell'art. 52 della Carta di Nizza, le limitazioni all'esercizio di tale libertà sono ammissibili a condizione che esse (a) siano previste dalla legge, (b) rispettino il contenuto essenziale di tale libertà e, (c) rispettino il principio di proporzionalità.

Non sembra in questa sede il caso di soffermarsi sul primo punto in quanto è evidente che la limitazione alla libertà di espressione sia prevista dalla legge, segnatamente dall'art. 17 della Direttiva 2019/790, dunque la limitazione in questione ha manifestamente una base giuridica. I sottopunti b) e c) invece meritano di ottenere separata considerazione.

Sul profilo del "contenuto essenziale", il punto di partenza espresso dall'Avvocato Generale è dato dal fatto che il legislatore europeo è legittimato a limitare l'esercizio di determinati diritti fondamentali nell'interesse comune, al fine di proteggere altri diritti e interessi. Il legislatore in questo dispone di un certo potere discrezionale per bilanciare e trovare un giusto equilibrio fra i diversi diritti e interessi coinvolti, con tuttavia un limite assoluto dato, appunto, dal contenuto essenziale di un diritto fondamentale che deve restare scevro da qualsivoglia interferenza. Nelle parole dell'Avvocato Generale questo è espresso sostenendo che "*nessun obiettivo, per quanto legittimo esso sia, giustifica che vengano arrecate determinate violazioni – eccezionalmente gravi – ai diritti fondamentali. In altre parole, il fine non giustifica qualsiasi mezzo*".

La Repubblica di Polonia, allora, nelle norme di cui si chiede l'annullamento ritiene che non sia stato rispettato tale contenuto essenziale. Infatti, ad avviso della ricorrente, la sorveglianza preventiva che deve essere effettuata dai prestatori di servizi di condivisione sui contenuti messi in rete dai loro utenti rimetterebbe in discussione tale diritto, poiché essa implica l'ingerenza in tali contenuti, e il loro eventuale blocco, ancor prima della loro diffusione.

In base alle considerazioni esposte in precedenza nel presente capitolo, si ritiene di concordare, tendenzialmente, con la Polonia sul punto, sebbene l'Avvocato Generale si esprima in senso opposto. In particolare, appare non convincente l'argomentazione dello stesso sulla distinzione compiuta fra obblighi di sorveglianza "generale" o "specifica", avendo in precedenza già espresso che, ad avviso di chi scrive, e ad avviso della Polonia, quanto richiesto dall'art. 17 è una sorveglianza generale. L'Avvocato Generale non tiene forse nemmeno in debito conto quanto egli stesso afferma quando sostiene che "*in linea di principio, tali misure preventive vengono condannate in una società democratica, per il fatto che, limitando talune informazioni ancora prima della loro diffusione, esse impediscono ogni dibattito pubblico sul contenuto, privando in tal modo la libertà di espressione della sua funzione stessa di vettore del pluralismo*".

L'Avvocato Generale infatti afferma che se le autorità europee o nazionali dovessero imporre "*direttamente o indirettamente, ai prestatori intermedi che controllano tali infrastrutture di espressione l'obbligo di sorvegliare preventivamente, in via generale, i contenuti degli utenti dei loro servizi alla ricerca di qualsiasi tipo di informazioni illecite […] tale libertà di comunicazione verrebbe rimessa in discussione in quanto tale. Il «contenuto essenziale» del diritto alla libertà di espressione, come previsto all'articolo 11 della Carta, sarebbe in tal caso, a mio avviso, leso*".

Tuttavia, contrariamente a quanto da questo elaborato sostenuto, l'Avvocato Generale si spende in difesa di alcune forme di sorveglianza tanto che richiama come proprio la Corte di Giustizia, nella sua giurisprudenza relativa alle ingiunzioni che possono essere pronunciate nei confronti degli intermediari online, ha ammesso che sia possibile ingiungere ad un intermediario di prevenire talune infrazioni, esercitando una forma di sorveglianza mirata del suo servizio. Come nel Considerando 47 della Direttiva e-commerce, già visto in precedenza,

allora anche l'Avvocato Generale distingue fra obblighi di sorveglianza "generali" da quelli applicabili in casi "specifici".

L'Avvocato Generale argomenta la sua opinione affermando che "*nella specie, per conseguire gli obiettivi di cui alle disposizioni impugnate, i prestatori di servizi di condivisione devono effettivamente sorvegliare la totalità dei contenuti che i loro utenti mettono in rete. Tuttavia, si tratta di ricercare, fra tali contenuti, le «opere e [gli] altri materiali specifici» per i quali i titolari dei diritti avranno previamente comunicato loro le «informazioni pertinenti e necessarie» [articolo 17, paragrafo 4, lettera b), della Direttiva 2019/790] oppure una «segnalazione sufficientemente motivata» [lettera c) di detto paragrafo 4]. […] Cionondimeno, nella presente fase dell'analisi, tali elementi sono sufficienti, a mio avviso, a dimostrare che tali disposizioni ben prevedono, indirettamente, un obbligo di sorveglianza «specifico» e ad escludere una violazione del «contenuto essenziale» del diritto alla libertà di espressione*".

Giustamente invece la ricorrente replica a queste argomentazioni che l'obbligo di sorveglianza imposto ai prestatori di servizi di condivisione in applicazione delle disposizioni impugnate è invece generale. Infatti, per assicurare che non siano disponibili opere e altri materiali protetti identificati dai titolari dei diritti e impedirne il caricamento in futuro sui loro servizi, tali prestatori devono, in pratica, filtrare la totalità dei contenuti caricati da tutti gli utenti. Sebbene si concordi con la prospettazione del ricorrente, si segnala che un compiuto riferimento anche agli altri diritti irrimediabilmente compressi da una simile sorveglianza avrebbero potuto far propendere l'Avvocato Generale a conclusioni diverse, in particolare in relazione al diritto alla privacy ed alla tutela della vita privata.

Come vedremo, nella sentenza della Corte di Giustizia questo richiamo specifico alla dimensione della sorveglianza non è, paradossalmente, oggetto di trattazione, limitandosi la Corte ad un apodittico richiamo alle parole del legislatore che ne escludono categoricamente la possibilità, senza tuttavia addentrarsi ad una dimostrazione del perché nei fatti tale sorveglianza non si dovrebbe verificare. La Corte non ripropone nemmeno la distinzione compiuta fra sorveglianza generale e specifica proposta invece dall'Avvocato Generale, ad ulteriore dimostrazione di come la sentenza che in seguito verrà commentata pecchi gravemente di vaghezza e presenti una motivazione totalmente inidonea ad affrontare le censure concretamente sollevate dal Paese membro ricorrente.

Dato che l'Avvocato Generale sostiene che il contenuto essenziale della libertà di espressione è stato rispettato dal legislatore europeo, procede ad analizzare il terzo punto sopra citato, ossia la proporzionalità della misura. In questo ritiene necessario verificare se tale limitazione sia (1) appropriata, (2) necessaria, nonché (3) proporzionata *stricto sensu*. Sul primo punto nessuno contesta che la misura sia appropriata nel senso di idonea a raggiungere il fine. Sicuramente la sorveglianza imposta dai meccanismi di filtraggio è idonea a raggiungere il risultato prefissato dal legislatore, ossia l'*enforcement* del diritto d'autore. Rimane tuttavia, criticamente, il fatto che vi possa essere una eccessiva tutela.

Sul carattere della necessarietà invece l'Avvocato Generale afferma che si risolve nel verificare l'esistenza di misure alternative altrettanto efficaci della misura scelta per conseguire l'obiettivo perseguito essendo al contempo meno restrittive. Su questo punto egli afferma che "*un regime di responsabilità che si limiti ad imporre gli obblighi previsti alla lettera a) e alla lettera c), in principio, del paragrafo 4 dell'articolo 17 della Direttiva 2019/790 chiaramente non sarebbe altrettanto efficace per conseguire l'obiettivo perseguito dal legislatore dell'Unione di un regime che preveda, inoltre, gli obblighi risultanti dalla lettera b) e dalla lettera c), in fine, di tale paragrafo – anche se i primi obblighi sono effettivamente meno restrittivi per il diritto alla libertà di espressione rispetto ai secondi*". Aggiunge poi che "*è innegabile, dall'altro, che, come sottolineato dalle parti convenute, un sistema di notifica e rimozione, come quello risultante dall'articolo 14 della Direttiva 2000/31 e ripreso, in sostanza,*

all'articolo 17, paragrafo 4, lettera c), in principio, della Direttiva 2019/790 non consente ai titolari interessati di opporsi all'utilizzo illecito delle loro opere sui servizi di condivisione in maniera altrettanto efficace di un sistema, come quello risultante dalle disposizioni impugnate, che impone, inoltre, ai prestatori di tali servizi obblighi di sorveglianza". Sul punto è possibile anche concordare con l'Avvocato Generale, essendo effettivamente evidente che il regime delineato è sicuramente efficace per l'obiettivo dell'*enforcement* del diritto d'autore; tuttavia, dovrebbe essere obiettivo della norma anche rispettare gli usi legittimi, le eccezioni e limitazioni, le libertà di espressione e di impresa ed il diritto alla privacy, finalità di almeno pari rilievo rispetto a quelle di *enforcement* del diritto d'autore. Se allora si considerasse la finalità della norma in un senso più complesso rispetto alla mera esigenza di tutela del diritto d'autore, si potrebbe giungere a conclusioni diverse.

Il punto su cui tuttavia ci si sente di dissentire rispetto alla prospettazione dell'Avvocato Generale è proprio quello concernente la proporzionalità *stricto sensu* della misura, avendo ampiamente dimostrato nei paragrafi precedenti come questa non possa essere rinvenuta imponendo una eccessiva restrizione alle libertà ed ai diritti garantiti dalla Carta di Nizza. Correttamente, infatti, la Polonia notava che il pregiudizio causato alla libertà di espressione dalle disposizioni impugnate sarebbe smisurato rispetto ai vantaggi che esse sono idonee a procurare in termini di protezione dei diritti di proprietà intellettuale. La pecca rinvenibile nelle argomentazioni della ricorrente, tuttavia, consiste proprio nell'aver considerato solo la libertà di espressione, avendo invece potuto sollevare censure più stringenti e penetranti su questo punto.

L'argomentazione adottata dall'Avvocato Generale lascia invece a desiderare sulla sua puntualità e significanza, facendo riferimento primario alla "discrezionalità" del legislatore. Egli afferma infatti che "*in un contesto ampiamente dibattuto, il legislatore dell'Unione ha fatto una scelta politica a favore delle industrie creative. Esso ha ritenuto che l'equilibrio anteriore fra i diritti e gli interessi coinvolti non fosse più soddisfacente e che, al fine di continuare ad assicurare ai titolari dei diritti un livello elevato di protezione, occorresse adottare un nuovo regime di responsabilità per taluni prestatori di servizi del «Web 2.0», imponendo loro determinati obblighi di sorveglianza dei contenuti messi in rete dagli utenti dei loro servizi. Alla luce dell'ampio potere discrezionale di cui disponeva il legislatore, ritengo che una siffatta scelta non fosse, nel suo principio stesso, sproporzionata*". Secondo l'Avvocato Generale infatti il carattere proporzionato delle disposizioni impugnate risiederebbe (a) nell'importanza del danno economico causato ai titolari dei diritti dalla messa in rete illecita di loro opere; (b) nel fatto che, per queste stesse ragioni, il sistema di *notice and take down* solo difficilmente consente a tali titolari di controllare l'utilizzo delle loro opere su detti servizi; (c) nelle difficoltà che essi incontrano per perseguire gli utenti responsabili e, (d) nel fatto che gli obblighi di sorveglianza riguardano prestatori intermedi particolari. Chiamare in causa l'importanza del danno economico o la tediosità e difficoltà di altri sistemi non pare, ad avviso di chi scrive, poter avere un peso significativo ove contrapposto alle esigenze degli utenti di veder rispettate delle prerogative fondamentali della loro stessa individualità e dignità, quali quelle tutelate dagli articoli 7, 8 ed 11 della Carta di Nizza.

Correttamente l'Avvocato Generale segnala poi che "*il nesso che il legislatore dell'Unione ha istituito, in dette disposizioni, fra responsabilità dei prestatori di servizi di condivisione e efficacia di tale filtraggio comporta un rischio importante per la libertà di espressione, ossia quello di un «blocco eccessivo» di contenuti leciti. Un siffatto rischio di «blocco eccessivo» esiste, in generale, qualora le pubbliche autorità considerino i prestatori intermedi responsabili delle informazioni illecite fornite dagli utenti dei loro servizi. Al fine di sottrarsi a qualsivoglia rischio di responsabilità, tali intermediari possono avere la tendenza a dar prova di zelo e a bloccare in maniera esagerata tali informazioni al minimo dubbio sulla loro liceità*". Come infatti abbiamo già avuto modo di segnalare, questo rischio è concreto e reale, i prestatori di servizi di condivisione, al fine di evitare ogni rischio di responsabilità nei confronti dei titolari

dei diritti, sono tendenzialmente e naturalmente portati a bloccare, calibrando restrittivamente il filtro automatizzato, tutti contenuti che riproducono le opere e gli altri materiali protetti per i quali gli OCSSP abbiano hanno ricevuto le "informazioni pertinenti e necessarie" o una "segnalazione sufficientemente motivata" dai titolari dei diritti. E quando si afferma "tutti" i contenuti, in questi sono inclusi quelli che non violano il diritto perché ad esempio oggetto di un uso legittimo o di una eccezione o limitazione. Ricordiamo che il diritto d'autore è fatto, al pari di molte aree del diritto, se non tutte, di sfumature e concetti ambigui. Distinguere ad esempio un'opera originale, e dunque protetta, da una non originale, e dunque non protetta, è spesso oggetto di delicata analisi da parte delle Corti, analisi che difficilmente potrebbe essere tradotta in algoritmo. Ma ancora, non risulta allo stato dell'arte esservi sicurezza che un algoritmo sia in grado di cogliere quelle sfumature contestuali che integrano una eccezione o limitazione, come una parodia. Allora appare naturale che, come riconosce anche l'Avvocato Generale, senza poi attribuirne peso, in tutte le situazioni equivoche, ai prestatori di servizi di condivisione potrebbe sembrare più semplice impedire la messa a disposizione dei contenuti, così cautelandosi avverso possibili azioni in responsabilità.

In questo senso argomentava anche la Repubblica polacca, la quale riteneva che alla luce delle limitazioni inerenti al funzionamento degli strumenti di riconoscimento di contenuto, e segnatamente della loro incapacità di individuare l'applicazione delle eccezioni e delle limitazioni al diritto d'autore, "*l'articolo 17, paragrafo 7, della Direttiva 2019/790 costituirebbe un pio desiderio piuttosto che una garanzia effettiva. Di fatto, i contenuti rientranti in tali eccezioni e limitazioni saranno bloccati automaticamente da detti strumenti. Tale disposizione non sarebbe dunque idonea ad assicurare agli utenti dei servizi di condivisione una protezione efficace contro il blocco abusivo o arbitrario dei loro contenuti*".

Nonostante questa considerazione, che a chi scrive pare decisiva per la risoluzione della questione circa la proporzionalità *stricto sensu*, l'Avvocato Generale tenta argomentativamente di salvare la misura. Infatti, egli afferma che "*il diritto degli utenti dei servizi di condivisione di fare utilizzi legittimi di materiali protetti, previsto all'articolo 17, paragrafo 7, della Direttiva 2019/790, dovrebbe essere preso in considerazione ex ante dai prestatori di tali servizi, nel processo stesso di filtraggio. Infatti, le disposizioni impugnate e tale paragrafo 7 dovrebbero essere letti congiuntamente, e gli obblighi da essi previsti si applicherebbero «simultaneamente». I «massimi sforzi» che tali prestatori devono compiere, in conformità a tali disposizioni, per prevenire la messa in rete delle opere e dei materiali protetti identificati dai titolari dei diritti non possono dunque tradursi, in pratica, in un blocco preventivo e sistematico di tali utilizzi legittimi. Il meccanismo di reclamo e ricorso di cui al paragrafo 9 di tale articolo 17 costituirebbe una garanzia supplementare, e ultima, per le situazioni in cui, nonostante l'obbligo figurante a questo stesso paragrafo 7, detti prestatori blocchino ugualmente, per errore, siffatti contenuti legittimi*".

La visione dell'Avvocato Generale pare sotto molti aspetti utopistica. Secondo la sua interpretazione, infatti, le misure di filtraggio che i prestatori di servizi di condivisione sono tenuti ad attuare devono essere conformi a due obblighi cumulativi: "*esse devono tentare di prevenire la messa in rete di contenuti che riproducono in maniera illecita le opere e gli altri materiali protetti identificati dai titolari dei diritti, non impedendo al contempo la disponibilità dei contenuti che riproducono tali materiali in maniera lecita*". In un contesto perfetto certamente questo dovrebbe essere l'obiettivo da raggiungere, ma, come dimostrato, i *provider* saranno tentati di procedere in senso opposto per il timore di incorrere in responsabilità. Secondo l'avvocato poi "*in tutte le situazioni equivoche – brevi estratti di opere riprese in contenuti più lunghi, opere «trasformative», ecc. – nelle quali, in particolare, sia ragionevolmente ipotizzabile l'applicazione di eccezioni e limitazioni al diritto d'autore, i contenuti interessati non possono essere oggetto di una misura di blocco preventivo*".

Secondo l'Avvocato Generale, "*l'obbligo di risultato, previsto all'articolo 17, paragrafo 7, primo comma, della Direttiva 2019/790, di non impedire la messa in rete di contenuti legittimi è, al riguardo, più vincolante degli obblighi di «massimi sforzi» risultanti dalle disposizioni impugnate, i quali costituiscono obblighi di mezzo. Ciò significa che il legislatore dell'Unione ha inteso assicurare, a mio avviso correttamente, che, in una simile ipotesi, i prestatori di servizi di condivisione privilegino la libertà di espressione. In altri termini, il legislatore ha ritenuto che i «falsi positivi», consistenti nel bloccare contenuti legali, siano più gravi dei «falsi negativi», che si risolvono nel far passare taluni contenuti illeciti*".

Secondo l'Avvocato quindi in tali situazioni equivoche, si deve presumere che i contenuti interessati siano leciti e, di conseguenza, la loro messa in rete non può essere ostacolata. Nella possibilità materiale di applicazione di una simile interpretazione del disposto dell'art. 17, l'Avvocato Generale si macchia ancora una volta di una concezione vagamente utopica, affermando che le soluzioni tecniche da implementare "*consisteranno nell'integrare, negli strumenti di riconoscimento di contenuto, parametri che consentono di aiutare a distinguere il manifesto dall'equivoco. Ciò può variare a seconda dei tipi di materiali protetti e di eccezioni in questione. Si tratterà, ad esempio, di tenere conto dei tassi di corrispondenza rilevati da tali strumenti, nonché di fissare soglie al di sopra delle quali il blocco automatico di un contenuto è giustificato, e al di sotto delle quali è ragionevolmente ipotizzabile l'applicazione di un'eccezione, come la citazione. Una siffatta soluzione potrebbe essere abbinata ad un meccanismo che consenta agli utenti di indicare (flagging), al momento o immediatamente dopo la messa in rete, se, a loro avviso, essi beneficiano di un'eccezione o di una limitazione, il che implicherebbe, per il prestatore interessato, di procedere ad una revisione manuale del contenuto in questione al fine di verificare se l'applicazione di tale eccezione o limitazione sia manifestamente esclusa o, al contrario, ragionevolmente ipotizzabile*".

La speranza che un simile sistema possa effettivamente essere implementato e reso tecnologicamente fattibile ed affidabile permane, tuttavia serve anche sottolineare la necessaria consapevolezza che ad oggi una materia come quella delle eccezioni e limitazioni al diritto d'autore è talmente complessa che persino la giurisprudenza è altalenante nelle sue interpretazioni, potendosi dubitare allora che un algoritmo sia in grado di dissipare la complessità del reale tramutandola in una somma di 0 e di 1. Quello che realisticamente vedremo accadere sarà il contrario, ossia l'implementazione di un sistema di filtraggio che blocchi in maniera sistematica i contenuti che facciano un'utilizzazione legittima di materiale protetto. E questo, come riconosce anche l'Avvocato Generale, arrecherebbe un pregiudizio eccessivo alla libertà di espressione e di informazione. "*Ciò vale, a mio avviso, proprio in quanto l'effetto collaterale di un siffatto filtraggio è troppo importante per essere compatibile con tale libertà – e ciò indipendentemente dal fatto che gli utenti lesi beneficino o meno di un diritto di ricorso contro il blocco di loro informazioni[…]*". L'Avvocato Generale, volendo credere in un ipotetico mondo in cui le macchine sono la risposta, si rende conto dei pericoli di simili meccanismi, ma vuole persistere in una fiducia, forse leggermente cieca. Il risultato quasi certamente, per come lo stato dell'arte finora si è evoluto, sarà il blocco preventivo della totalità dei contenuti anche potenzialmente legittimi. Questo, come nota persino l'Avvocato Generale, "*avrebbe per effetto quello di fare sistematicamente gravare il peso dell'inerzia sugli utenti, poiché la diffusione dei contenuti legittimi non potrebbe avere luogo senza che essi formulino un reclamo, con successo. Se tali utenti dovessero far valere sistematicamente i loro diritti nell'ambito del meccanismo di ricorso, è fortemente probabile che una parte significativa di essi rinuncerebbe a farlo, in assenza, segnatamente, di conoscenze sufficienti per valutare se l'utilizzo che gli stessi fanno di tali materiali sia legittimo e se, pertanto, esistano motivi per formulare un siffatto reclamo. Il «blocco eccessivo» preventivo di tutti questi utilizzi legittimi, e l'inversione sistematica a carico degli utenti dell'onere di dimostrare tale legittimità, rischierebbero pertanto di comportare, a breve o a lungo termine, un «chilling effect» sulla libertà di espressione e di creazione, che si tradurrebbe in un calo dell'attività di questi stessi utenti*".

L'Avvocato Generale consiglia dunque alla Corte di Giustizia di salvare le disposizioni dell'art. 17, per le ragioni così delineate, non ritenendolo idoneo a infirmare irrimediabilmente la libertà di espressione e di informazione. Invece, se questo elaborato può aver avuto un merito, questo è stato di aver messo in luce come serva molta attenzione nel bilanciamento fra l'*enforcement* del diritto d'autore ed altre prerogative contrapposte. Come più volte rimarcato, purtroppo la Polonia ha censurato l'articolo 17 solamente sotto l'aspetto dell'articolo 11 della Carta di Nizza, quando invece, come dimostrato, sono anche altre le prerogative degli utenti che vengono compresse dalla disciplina della nuova Direttiva 2019/790.

In considerazione di quanto consigliato dall'Avvocato Generale, la Corte di Giustizia, pronunciandosi sul ricorso con sentenza del 26 aprile 2022, respinge le censure della Repubblica Polacca e conferma la legittimità dell'articolo 17. Tuttavia, la decisione si espone a numerose critiche non solo sul piano logico, per non aver debitamente considerato il risvolto pratico dell'articolo in commento, ma anche per l'eccesiva tautologia nei vacui richiami alle parole del legislatore senza ammettere alcuna censura all'operabilità pratica di alcuni principi che, come visto, ad oggi, costituiscono mere utopie, tecnologicamente impossibili da realizzare.

10. La decisione della Corte di Giustizia, Sentenza del 26 aprile 2022: l'articolo 17 è salvo

Si è infine scelto di chiosare il presente capitolo, e con esso l'elaborato intero, con l'ennesima pronuncia che, disattendendo le aspettative degli utenti ad un corretto bilanciamento fra *enforcement* del diritto d'autore e tutela della libertà di informazione e della privacy, offre il guanto della vittoria, ancora una volta, ai *copyright holders*, mascherando nella pronuncia mere scelte di politica del diritto in quanto, per le ragioni che si avrà modo di esporre, non si può certo ritenere che nella decisione in esame sia presente una motivazione giuridica di pregnanza tale da risultare anche solo minimamente convincente.

Limitandoci a richiamare la decisione della Corte di Giustizia per quanto strettamente necessario a risolvere il punto controverso, è possibile rinvenire come la Corte abbia compiuto la scelta di non procedere ad annullare l'articolo 17[647]. Tuttavia, l'operazione di salvataggio compiuta dalla Corte si basa su fondamenta barcollanti, su motivazioni apodittiche, su sterili richiami alle parole del legislatore comunitario senza voler fare i conti con la realtà economica e tecnologica che l'articolo 17 mira a disciplinare, così compiendo un'operazione forse più politica che giuridicamente ortodossa.

La Corte di Giustizia, infatti, ricorda come il punto di frizione su cui si incentrava la controversia riguardava il fatto che, ai sensi di una corretta interpretazione dell'articolo 17, i fornitori di servizi di condivisione di contenuti online sarebbero stati costretti a controllare

[647] Per alcune prime ricostruzioni dottrinali della vicenda ed un primo commento si vedano: J. P. QUINTAIS, *Article 17 survives, but freedom of expression safeguards are key: C-401/19 – Poland v Parliament and Council,* in *Kluwer Copyright Blog*, 26 aprile 2022, liberamente accessibile presso: «http://copyrightblog.kluweriplaw.com/2022/04/26/article-17-survives-but-freedom-of-expression-safeguards-are-key-c-401-19-poland-v-parliament-and-council/». (Ultimo accesso: 10 maggio 2022); F. REDA, P. KELLER, *CJEU upholds Article 17, but not in the form (most) Member States imagined,* in *Kluwer Copyright Blog*, 28 aprile 2022, liberamente accessibile presso: «http://copyrightblog.kluweriplaw.com/2022/04/28/cjeu-upholds-article-17-but-not-in-the-form-most-member-states-imagined/» (Ultimo accesso: 10 maggio 2022); E. ROSATI, *Article 17 of the DSM Directive is valid: an early take on today's Grand Chamber ruling,* in *The IPKat*, 26 aprile 2022, liberamente accessibile presso: «https://ipkitten.blogspot.com/2022/04/article-17-of-dsm-directive-is-valid.html» (Ultimo accesso: 10 maggio 2022).

tutti i contenuti caricati dai loro utenti preliminarmente alla loro diffusione al pubblico. A tal fine, detti fornitori, in assenza di altre soluzioni praticabili, sarebbero stati indotti a utilizzare strumenti di filtraggio automatico.

Su questo punto, che è di cruciale importanza per quanto sin qui esposto, la Corte non può far altro che concordare. Infatti essa stessa, analizzando il punto di diritto, afferma che "*un siffatto controllo preventivo costituirebbe un'ingerenza particolarmente grave nel diritto alla libertà di espressione e d'informazione degli utenti di servizi di condivisione di contenuti online, dal momento che, da un lato, comporterebbe il rischio che contenuti leciti siano bloccati e, dall'altro, l'illiceità e, quindi, il blocco dei contenuti sarebbero stabiliti in modo automatico da algoritmi, e ciò ancor prima di qualsiasi diffusione dei contenuti in questione*"[648]. Se questa dunque è la premessa, come ostinatamente questo elaborato ha voluto dimostrare, la conseguenza che ci si aspetterebbe sarebbe quella della incompatibilità della disposizione impugnata con il diritto europeo. Eppure, nonostante questo essenziale riconoscimento, la Corte trova il modo di salvare la disciplina in esame. Ancora una volta, forse, se si avesse avuto la prontezza di sollevare censure riguardanti anche la libertà di impresa, la tutela della vita privata e della privacy, allora l'esito avrebbe potuto essere opposto.

Se questo non bastasse, si potrebbe altresì aggiungere che la Corte riconosce, come rilevato dall'Avvocato Generale ai paragrafi da 57 a 69 delle sue conclusioni, che per poter effettuare un controllo preventivo come quello richiesto dall'articolo 17, "*i fornitori di servizi di condivisione di contenuti online sono tenuti, a seconda del numero di file caricati e del tipo di materiale protetto di cui trattasi e nei limiti stabiliti dall'articolo 17, paragrafo 5, della direttiva 2019/790, a utilizzare strumenti automatici di riconoscimento e filtraggio*" [649]. A questo aggiunge poi che, evidentemente, "*né le istituzioni convenute né gli intervenienti sono stati in grado, nel corso dell'udienza dinanzi alla Corte, di designare possibili alternative a tali strumenti*"[650]. Questo sarebbe, ad avviso di chi scrive, da valorizzare nel senso che l'articolo 17 in realtà impone tassativamente l'adozione di sistemi di *Automatic Content Recognition*, infrangendo la libertà di impresa dei provider e arrecando, come già pienamente affermato, un grave nocumento alla privacy degli utenti. A maggior ragione dovrebbe confortare il fatto che la stessa Corte di Giustizia, in motivazione, afferma che "*un siffatto controllo e un siffatto filtraggio preventivi sono atti ad apportare una restrizione ad un importante mezzo di diffusione di contenuti online e a costituire, pertanto, una limitazione del diritto garantito all'articolo 11 della Carta*"[651].

Ancora una volta la decisione deve ridursi sul porre in essere un bilanciamento fra opposte esigenze alla luce e sotto la guida del principio di proporzionalità di cui all'art 52 della Carta di Nizza. Nel fare questo, molte delle conclusioni espresse dall'Avvocato Generale vengono riprese dalla Corte, anche se con una minor pregnanza argomentativa.

La Corte di Giustizia afferma in proposito che "*secondo un principio ermeneutico generale, un atto dell'Unione dev'essere interpretato, nei limiti del possibile, in modo da non inficiare la sua validità e in conformità con il diritto primario nel suo complesso e, in particolare, con le disposizioni della Carta. Pertanto, quando un testo di diritto derivato dell'Unione ammette più di un'interpretazione, si deve dare la preferenza a quella che rende la disposizione conforme al diritto primario rispetto a quella che porti a constatarne l'incompatibilità con quest'ultimo*"[652]. Una sorta di principio per cui quello che può essere salvato, anche con costruzioni ardite, retoriche e probabilmente infondate deve essere salvato?

[648] CGUE 26 aprile 2022, C-401/2019, Repubblica di Polonia contro Parlamento europeo, Consiglio dell'Unione europea, cit., par. 41
[649] CGUE 26 aprile 2022, C-401/2019, Ibidem, par. 54
[650] CGUE 26 aprile 2022, C-401/2019, Ibidem, par. 54
[651] CGUE 26 aprile 2022, C-401/2019, Ibidem, par. 55
[652] CGUE 26 aprile 2022, C-401/2019, Ibidem, par. 70

Singolare risulterebbe se potesse essere valevole una simile interpretazione, sottointesa evidentemente dalla Corte di Giustizia, dato che è esattamente ciò che è stato compiuto nel caso di specie. Il principio, di ben altro tenore rispetto al modo in cui viene usato nella controversia in questione, varrebbe se vi fosse almeno una interpretazione della norma che non si ponga in contrasto con norme di rango superiore. Cosa che nel caso di specie, ad avviso di chi scrive, non si verifica.

Quello che risulta davvero inaccettabile alla lettura della sentenza della Corte di Giustizia è che, al posto di risolvere concretamente la questione, con un puntuale riferimento alla concretezza dei sistemi di filtraggio automatico ed alle reali ripercussioni che questi possono avere non solo sulla libertà di espressione, ma anche sugli altri diritti di cui si è voluto occupare il presente capitolo, decide che un mero richiamo normativo poteva essere sufficiente ad escludere la lesione dei diritti fondamentali, e questo per la semplice ragione che la legge ne assicura, formalmente, sulla carta ed in teoria (ma non nei fatti) il rispetto.

Questo è particolarmente evidente nel momento in cui la Corte, chiamata a valutare sul rispetto del contenuto essenziale della libertà di espressione, afferma che l'articolo 17 non lederebbe tale nucleo ineludibile di tutela nel momento in cui afferma che "*si deve rilevare che l'articolo 17, paragrafo 7, primo comma, della direttiva 2019/790 precisa in modo esplicito che la «cooperazione tra i prestatori di servizi di condivisione di contenuti online e i titolari dei diritti non deve impedire la disponibilità delle opere o di altri materiali caricati dagli utenti, che non violino il diritto d'autore o i diritti connessi, anche nei casi in cui tali opere o altri materiali siano oggetto di un'eccezione o limitazione» di tali diritti. Secondo la sua formulazione univoca, tale articolo 17, paragrafo 7, primo comma, contrariamente all'articolo 17, paragrafo 4, lettera b), e lettera c), in fine, della direttiva 2019/790, non si limita ad esigere che i fornitori di servizi di condivisione di contenuti online compiano, a tal fine, i «massimi sforzi», ma prescrive un risultato preciso da conseguire*"[653]. A questa prima affermazione la Corte poi aggiunge che "*l'articolo 17, paragrafo 9, terzo comma, della direttiva 2019/790 sottolinea che tale direttiva «non incide in alcun modo sugli utilizzi legittimi, quali quelli oggetto delle eccezioni o limitazioni previste dal diritto dell'Unione»*[654]". A parere della Corte, il mero richiamo alla disposizione normativa per cui il legislatore comunitario imporrebbe il rispetto delle eccezioni e limitazioni e degli usi legittimi potrebbe essere in grado di escludere nella disciplina dell'articolo 17 una concreta lesione della libertà di espressione. Tuttavia, tale visione non può che essere gravemente censurata in quanto non tiene conto di ciò che è invece stato affermato nei precedenti paragrafi di questo capitolo, nonché ribadito dall'Avvocato Generale, ossia che le tecnologie, allo stato dell'arte, non consentono di rispettare efficacemente tali imposizioni. Abbiamo già avuto modo di sottolineare ampiamente in precedenza una simile affermazione, ma vale richiamare il punto così come emerge dalle stesse parole della Commissione Europea. Anche le linee guida della Commissione, come richiamate, affermano che "*allo stato attuale delle conoscenze tecniche, nessuna tecnologia è in grado di raggiungere gli standard richiesti dalla legge nel valutare se il caricamento di contenuti che un utente desidera effettuare costituisca un uso legittimo o lesivo del diritto d'autore o dei diritti connessi. La tecnologia di riconoscimento dei contenuti può tuttavia individuare un contenuto specifico protetto dal diritto d'autore in relazione al quale i titolari dei diritti hanno fornito ai prestatori di servizi le informazioni pertinenti e necessarie*"[655].

---

[653] CGUE 26 aprile 2022, C-401/2019, Ibidem, par. 77

[654] CGUE 26 aprile 2022, C-401/2019, Ibidem, par. 79

[655] Communication From The Commission To The European Parliament And The Council: *Guidance on Article 17 of Directive 2019/790 on Copyright in the Digital Single Market* COM/2021/288 final, liberamente accessibili presso: «https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52021DC0288&from=EN» (Ultimo accesso: 10 maggio 2022).

La Corte di Giustizia invece non pare tenere conto di una consapevolezza tecnologica che invece avrebbe dovuto essere il fulcro della sua decisione sulla validità o meno dell'articolo 17. Ribadisce allora, apoditticamente e acriticamente che, "*risulta quindi chiaramente dall'articolo 17, paragrafi 7 e 9, della direttiva 2019/790 nonché dai considerando 66 e 70 di quest'ultima che, al fine di tutelare il diritto alla libertà di espressione e d'informazione degli utenti di servizi di condivisione di contenuti online, sancito all'articolo 11 della Carta, e il giusto equilibrio tra i diversi diritti e interessi in gioco, il legislatore dell'Unione ha previsto che l'attuazione degli obblighi imposti ai fornitori di tali servizi all'articolo 17, paragrafo 4, lettera b), e lettera c), in fine, di tale direttiva non può segnatamente avere come conseguenza che questi ultimi adottino misure che pregiudichino il contenuto essenziale di tale diritto fondamentale degli utenti che condividono, sulle piattaforme di detti fornitori, contenuti che non violano il diritto d'autore e i diritti connessi*"[656].

La Corte di giustizia tenta di richiamare sei argomenti a sostegno della perdurante validità della disposizione di cui all'articolo 17. Nessuno di questi argomenti, tuttavia, entra nel vivo della questione, limitandosi ad un mero richiamo delle disposizioni normative che, in astratto, servirebbero a tutelare gli utenti, ma, per quanto dimostrato in precedenza, non hanno alcuna possibilità di imporsi sulle tecnologie ad oggi richieste ed utilizzabili. In primo luogo, abbiamo già avuto modo di commentare il mero richiamo ai paragrafi 7 e 9, con quindi riferimento alle tecnologie che presuntivamente dovrebbero essere in grado di distinguere fra usi leciti ed illeciti. In aggiunta vengono richiamati (2) come "diritti degli utenti" le disposizioni che richiedono di riconoscere come usi leciti quelli con finalità di citazione, critica, rassegna, caricatura, parodia o pastiche; (3) si richiama la applicabilità dei filtri solo in presenza di "informazioni pertinenti e necessarie"; (4) si evoca l'articolo 17 paragrafo 8 sull'assenza di un obbligo generale di sorveglianza; (5) si ricordano le garanzie procedurali previste nei meccanismi di reclamo di cui al paragrafo 9; (6) si ritiene integrato il meccanismo di garanzie dei diritti degli utenti dal richiamo dell'articolo 17 paragrafo 10 all'obbligo per la Commissione di organizzare dialoghi tra le parti interessate per discutere le migliori prassi per la cooperazione tra i fornitori di servizi di condivisione di contenuti online e i titolari dei diritti. Come si potrà facilmente notare, le motivazioni della Corte di Giustizia, persino enumerate nel loro procedere, non compiono alcuno sforzo nel definire la compatibilità dell'articolo 17 con il panorama europeo dei diritti fondamentali, limitandosi a sterili richiami a disposizioni legislative che, come visto, saranno nella pratica di scarsa o difficile attuazione[657].

Per i punti maggiormente controversi, la Corte sembra non aver compreso fino in fondo la portata della critica mossa dalla Repubblica di Polonia in quanto, a corroborare la sua tesi, ma finendo poi per sconfessarsi nei fatti, afferma che "*si deve ricordare che la Corte ha già avuto occasione di constatare che un sistema di filtraggio che rischi di non distinguere adeguatamente tra un contenuto illecito e un contenuto lecito, sicché il suo impiego potrebbe avere come risultato di bloccare comunicazioni aventi un contenuto lecito, sarebbe incompatibile con il diritto alla libertà di espressione e d'informazione, garantito all'articolo 11 della Carta, e non rispetterebbe il giusto equilibrio tra quest'ultimo e il diritto di proprietà intellettuale. La Corte ha sottolineato, a tal riguardo, che la questione della liceità di una trasmissione dipende anche dall'applicazione di eccezioni di legge al diritto d'autore che variano da uno Stato membro all'altro. Inoltre, in determinati Stati membri talune opere possono rientrare nel pubblico dominio o possono essere state messe in linea a titolo gratuito da parte dei relativi autori*"[658]. È infatti

[656] CGUE 26 aprile 2022, C-401/2019, Repubblica di Polonia contro Parlamento europeo, Consiglio dell'Unione europea, cit., par. 80

[657] Per una più puntuale ricostruzione dei punti segnalati si veda: J. P. QUINTAIS, *Article 17 survives, but freedom of expression safeguards are key: C-401/19 – Poland v Parliament and Council,* cit.

[658] CGUE 26 aprile 2022, C-401/2019, Ibidem, par. 86

proprio questo che risulta essere uno fra i problemi di cui all'articolo 17, o forse il problema principale. La Corte in questo passaggio motivazionale sta affermando, sostanzialmente, che obbligare i provider ad adottare un sistema informatico, quale gli ACR, che però non sia in grado di distinguere fra contenuti leciti od illeciti e che avrebbe il rischio di bloccare comunicazioni lecite, sarebbe illegittimo. Per quanto dimostrato nelle pagine che hanno preceduto l'esposizione di questa pronuncia apparirà dunque chiaro che, nei fatti, l'articolo 17 impone esattamente questo. La conseguenza dovrebbe essere l'illegittimità della disciplina e l'annullamento della stessa come richiesto dalla Polonia, ma la Corte di Giustizia decide di salvare l'articolo 17. L'assenza di realismo della Corte e la scissione fra il piano delle declamazioni di diritto e le possibilità invece concretamente offerte dalla tecnologia rendono la motivazione della Corte sostanzialmente illogica, alla luce delle considerazioni compiute.

Dulcis in fundo, è necessario richiamare le affermazioni circa gli obblighi di sorveglianza e di monitoraggio che si imporrebbero in capo ai provider. Gran parte dell'esposizione del presente elaborato è incentrata proprio su queste forme di sorveglianza, più o meno legali, più o meno occulte. Anche le conclusioni dell'Avvocato Generale si profondevano copiosamente nel tentare di salvare la disposizione distinguendo fra un obbligo generale o specifico di sorveglianza o comunque edulcorando la realtà in modo da fornire una giustificazione più o meno pregnante ad un obbligo che, per quanto dimostrato, è pacificamente imposto. Le aspettative verso una risoluzione del punto controverso da parte della Corte di Giustizia erano alte, essendo appunto stata sollevata una specifica censura da parte della Polonia proprio sul punto del monitoraggio e della sorveglianza implicita nell'articolo 17. Tali aspettative sono state purtroppo disattese da una pronuncia che pare quasi abbia deciso di non volersi pronunciare davvero. È infatti dalla Corte solamente affermato che "*l'articolo 17, paragrafo 8, della direttiva 2019/790, prevedendo, al pari dell'articolo 15, paragrafo 1, della direttiva 2000/31, che l'applicazione di tale articolo 17 non comporta alcun obbligo generale di sorveglianza, stabilisce una garanzia aggiuntiva per il rispetto del diritto alla libertà di espressione e d'informazione degli utenti di servizi di condivisione di contenuti online. Infatti, tale precisazione implica che i fornitori di tali servizi non possono essere tenuti a prevenire il caricamento e la messa a disposizione del pubblico di contenuti la constatazione della cui illeceità richiederebbe, da parte loro, una valutazione autonoma del contenuto alla luce delle informazioni fornite dai titolari di diritti nonché di eventuali eccezioni e limitazioni al diritto d'autore*"[659]. La motivazione, se tale si vuole intendere, si limita a questo. Non risponde quindi alle censure sollevate dallo Stato Membro ricorrente, che invece affermavano, giustamente, che l'obbligo di sorveglianza imposto ai prestatori di servizi di condivisione è generale. Infatti, la Polonia sosteneva che per assicurare che non fossero disponibili opere e altri materiali protetti identificati dai titolari dei diritti e impedirne il caricamento in futuro sui loro servizi, tali prestatori dovessero, in pratica, filtrare la totalità dei contenuti caricati da tutti gli utenti.

La Corte, dunque, conclude l'esame della legittimità dell'articolo 17 con vaghi richiami all'articolo 17 paragrafo nono, in cui sono previsti i meccanismi di reclamo. Alla fine dei conti, la Corte respinge il ricorso della Polonia e salva la totalità dell'articolo 17 affermando che esso "*è stato accompagnato dal legislatore dell'Unione da garanzie adeguate per assicurare, conformemente all'articolo 52, paragrafo 1, della Carta, il rispetto del diritto alla libertà di espressione e d'informazione degli utenti di tali servizi, garantito all'articolo 11 della Carta, nonché il giusto equilibrio tra tale diritto, da un lato, e il diritto di proprietà intellettuale, protetto all'articolo 17, paragrafo 2, della Carta, dall'altro*"[660].

[659] CGUE 26 aprile 2022, C-401/2019, Ibidem, par. 90
[660] CGUE 26 aprile 2022, C-401/2019, Ibidem par. 98

Merita ancora di essere segnalato un punto controverso. Secondo la Corte, come è stato recentemente osservato, la questione di cosa costituisca una violazione manifesta agli occhi di un algoritmo di filtraggio deve essere risolta dal legislatore, non dalle piattaforme o dai fornitori privati di tecnologie di *Automatic Content Recognition*[661]. Nella sentenza, infatti, viene affermato che gli "*Stati membri sono tenuti, in occasione della trasposizione dell'articolo 17 della direttiva 2019/790 nel loro ordinamento interno, a fondarsi su un'interpretazione di tale disposizione atta a garantire un giusto equilibrio tra i diversi diritti fondamentali tutelati dalla Carta. Inoltre, in sede di attuazione delle misure di recepimento di tale disposizione, le autorità e i giudici degli Stati membri devono non solo interpretare il loro diritto nazionale in modo conforme a detta disposizione, ma anche provvedere a non fondarsi su un'interpretazione di essa che entri in conflitto con i summenzionati diritti fondamentali*". Tale ultima indicazione della Corte deve essere letta in relazione a quanto già da essa affermato al paragrafo 86 della sentenza in commento, ossia che un sistema di filtraggio che rischi di non distinguere adeguatamente tra un contenuto illecito e un contenuto lecito sarebbe incompatibile con il diritto alla libertà di espressione e d'informazione. La Corte lascia dunque agli Stati membri il compito di rinvenire i mezzi più opportuni per adempiere ad un obbligo che pare impossibile. In questo senso, è stato notato che la maggior parte dei Paesi membri dovrà rivedere le proprie legislazioni nazionali a meno di non voler esporre a censure di illegittimità le disposizioni di recepimento. Nel frattempo, i tribunali di tali Stati membri saranno tenuti ad interpretare il diritto nazionale in modo conforme a quanto stabilito dalla sentenza. La questione, quindi, è ancora aperta[662].

Bruno Saetta si è recentemente chiesto dove si ponesse il punto di equilibrio tra diritti fondamentali del cittadino e meri diritti economici delle aziende. L'impressione è che i secondi siano spesso valutati come sovraordinati rispetto ai primi[663]. Rimane comunque il dubbio che forse un più pregnante richiamo anche ai diritti alla privacy ed al trattamento dei dati personali avrebbero potuto orientare diversamente la decisione della Corte e sollecitare ancora una volta quel dibattito che si incentra nel costante tentativo di bilanciare *l'enforcement* del diritto d'autore con la tutela della privacy.

---

661 F. REDA, P. KELLER, *CJEU upholds Article 17, but not in the form (most) Member States imagined,* cit.

662 Per una più compiuta analisi si veda F. REDA, P. KELLER, *CJEU upholds Article 17, but not in the form (most) Member States imagined,* cit.

663 B. SAETTA, Il copyright, il filtraggio dei contenuti, il ricorso della Polonia respinto e il futuro della Rete, in ValigiaBlu, articolo del 30 aprile 2022, liberamente consultabile presso il sito: «https://www.valigiablu.it/copyright-polonia-futuro-rete/» (Ultimo accesso: 10 maggio 2022). In particolare, l'autore ricorda anche che "*l'impressione è che il delicato punto di equilibrio venga solo spostato dal piano giuridico a quello meramente tecnico. Infatti, nel momento in cui si sdoganano i sistemi di filtraggio dei contenuti online come mezzo per valutare la liceità di un contenuto, anche se le norme chiariscono che i contenuti leciti non possono essere rimossi, il problema diventa che i sistemi di filtraggio non sono in grado di comprendere il contesto (es. parodia), e quindi in realtà non sono in grado di stabilire se un contenuto è lecito oppure no. Tutto ciò che possono stabilire è che un contenuto è uguale o simile ad un altro. Ciò non è sufficiente. Quindi che si fa? Si dice che i sistemi di filtraggio sono non conformi alle norme e li si eliminano? La Corte stessa sostiene che non esistono (o non sono stati menzionati) altri sistemi per ottemperare agli obblighi previsti per i fornitori, e la stessa quantità di contenuti immessi nei server rende impossibile gestire diversamente tali obblighi (ovvero i sistemi di filtraggio sono essenziali per raggiungere il "best effort" previsto dal paragrafo 4). Quindi il problema viene lasciato alla gestione tecnica degli algoritmi, e alla realizzazione di prassi per una implementazione degli algoritmi*".

CONCLUSIONI:
L'*ENFORCEMENT* DEL DIRITTO D'AUTORE: LUCI ED OMBRE

Ὁ μῦθος δηλοῖ ὅτι, "la favola mostra che", così era solito Esopo chiudere le sue narrazioni introducendone la morale, traendone un insegnamento. Ma quali considerazioni possiamo sollevare alla luce dei capitoli precedenti?

Sin dalle prime battute della presente trattazione è stato segnalato che la nascita del diritto d'autore è connessa all'invenzione della macchina da stampa a caratteri mobili che ha favorito l'emersione della *Stationers' Company* e delle corporazioni di stampatori, primo nucleo di strategie di *enforcement* del diritto d'autore che da quel momento storico in poi si sono riproposte, in contesti diversi ed in modi parzialmente simili per tutti i secoli successivi, dal "*commando addestrato*" di Preston ed Abbott, passando dal furgoncino della BBC capace di combattere la "*guerra dell'oscillazione*" per giungere fino alle azioni legali della RIAA contro gli utenti ed ai sistemi di *Automatic Content Recognition*.

Si è avuto modo di notare un costante ricorso all'autotutela da parte dei titolari dei diritti d'autore, prima per i poteri di cui gli *Stationer* erano investiti dalla loro Charter, poi per mezzo del "*subpoena* del DMCA", dei "*John Doe proceedings*" e dell'art. 156-bis della Legge 633/1941. Si è così notato come gli ordinamenti moderni sembrino quasi incoraggiare una vasta attività di monitoraggio e di sorveglianza degli utenti sulla rete, sostenendo le attività di investigazione privata da parte dei titolari del *copyright*.

Il ricorso alla tecnologia ha poi rappresentato un wagneriano *leitmotiv* nel corso di questo elaborato. Dall'inizio del XX secolo, i titolari dei diritti d'autore hanno costantemente ricercato, nell'avanzamento tecnologico, degli strumenti per rafforzare i loro interessi ed il loro potere. Questo ha comportato, in ogni momento storico, una pericolosa attività di monitoraggio degli utenti, idonea ad invadere la loro sfera di riservatezza e di privacy, troppo spesso dimenticata dal legislatore o marginalizzata a vuote declamazioni di principio prive di forza cogente. Questo è stato riaffermato non solo nel contesto del *file-sharing* su reti *peer-to-peer*, ma anche e soprattutto nell'analisi dei sistemi di *Digital Rights Management*.

L'enforcement del diritto d'autore allora, per quanto si è scelto di considerare nella presente analisi, ha sempre sviluppato una forte tensione con il diritto alla privacy ed al trattamento dei dati personali, con uno spettro, quello della sorveglianza, che ha accompagnato la stesura dell'elaborato per ogni sua pagina. Eppure, questo spettro non accenna ad arrendersi, ad indietreggiare, a soccombere per il peso importuno che fa gravare sugli utenti. Si è più volte affermato che non era l'intento di questo elaborato mostrare altro rispetto alla delicatezza dei bilanciamenti, volendo meramente segnalare i punti in cui massimamente si avverte la frizione fra i diritti fondamentali. Tuttavia, in più occasioni si sono incontrate possibili risoluzioni di questo scontro, spesso già rinvenibili negli ordinamenti giuridici considerati. È stato il caso dei vari richiami al Regolamento UE 679/2016, ai "*Privacy Tort*", alle "*Privacy Enhancing Technologies*".

Gli scontri si riflettono tutti nella nuova Direttiva 2019/790 e nel suo articolo 17, approfonditamente analizzato nell'ultimo capitolo. In questo contesto il legislatore europeo sembra ancora una volta cedere alle istanze dei titolari dei diritti d'autore, tentando di attuare delle strategie che, in verità, si pongono in contrasto con i diritti fondamentali alla libertà di impresa, alla libertà di espressione ed al diritto alla privacy.

L'ultimo scontro cui stiamo assistendo si sta svolgendo sulle piattaforme online come *YouTube* od altri social media, quegli attori fondamentali del mondo digitale in cui le opere dell'ingegno perdono il loro *corpus mechanicum* e lo trasformano in una sequenza numerica, coloro che vengono dalla Direttiva definiti "*i prestatori di servizi di condivisione di contenuti online*". In un contesto fortemente connotato da interessi contrapposti, il legislatore europeo sceglie, implicitamente e senza mai dichiararlo, di sacrificare i diritti degli utenti facendosi paladino degli interessi economici intesi ad affrontare il c.d. "*value gap*".

La disciplina del 2019 stupisce particolarmente l'interprete considerando che solo tre anni prima era stato emanato il Regolamento 679/2016 che intendeva fare del rispetto dei diritti degli utenti, in particolare della privacy, una priorità. In una disciplina contorta ed in contraddizione con se stessa, si manifestano tutti i timori di una sorveglianza sul web, desunta dalle norme senza che il legislatore mai la ammetta. Alcuni aspetti critici sono stati ribaditi anche dal ricorso, esaminato in conclusione dell'ultimo capitolo, proposto dalla Repubblica di Polonia, con l'unico peccato di non aver sollevato tutte le possibili censure di illegittimità dell'articolato normativo, ma solo quelle relative alla libertà di espressione.

Si intende tessere allora non già una conclusione, un "addio", ma solo un "arrivederci": non si può mettere una parola fine al bilanciamento fra le esigenze di *enforcement* del diritto d'autore e la tutela della privacy perché con ogni probabilità queste istanze continueranno a vedersi contrapposte; in ogni teatro in cui una di queste si voglia affermare, anche l'altra seguirà in una sempiterna esigenza di equilibro che non sarà statico ma sempre dinamico e mutevole come la storia e le pronunce giurisprudenziali esaminate hanno dimostrato. Ci si vuole tuttavia lasciare con una speranza, ossia quella per cui il legislatore e le Corti, nazionali e sovranazionali, si profondano con maggior solerzia nel cercare un giusto equilibrio delle varie istanze in gioco nel mondo digitale. Si vuole così ricordare che, per combattere le forme più forti di compressione dei diritti degli utenti, deve ergersi a baluardo il potere normativo dello Stato quale naturale antagonista delle derive di autotutela tecnologica.

Come ricorda Ann Cavoukian, infatti, "*la privacy determina le fondamenta della nostra libertà: senza privacy, non rimarremo una società libera e civilizzata*"[664]. Ove si volesse cercare di trovare un merito al presente contributo che vada oltre la ricognizione e l'analisi giuridica di questioni attuali e di oscure norme da interpretare, questo verrebbe rinvenuto nell'aver messo in luce le differenti esigenze che si fronteggiano nel mondo digitale, le difficoltà, le contraddizioni, le incongruenze del panorama giuridico, ma in fin dei conti economico, in cui siamo tutti chiamati ad operare o a vivere, senza l'utopica pretesa di risolvere qualcosa che può essere conosciuto in questa sede solo nella sua superfice.

Se allora le parole spese verranno interpretate come una richiesta di tutela degli utenti, di rispetto della loro libertà e della loro privacy dinnanzi alle più subdole e patenti violazioni dei loro diritti, saranno certamente null'altro che una goccia in un mare di parole, eppur vero rimane che *gutta cavat lapidem non vi, sed saepe cadendo*[665].

---

[664] Così si esprime in un'intervista Ann Cavoukian, in J. HAYWARD, *Loss of privacy leads to society devoid of freedom*, in *Toronto Sun*, 11 marzo 2019, liberamente consultabile presso: «https://torontosun.com/opinion/columnists/opinion-loss-of-privacy-leads-to-an-uncivilized-society-devoid-of-freedom» (Ultimo accesso: 10 maggio 2022).

[665] Proverbio latino presente già in Lucrezio ed Ovidio, proposto nella versione di Alano di Matera, letteralmente "la goccia scava la pietra non già con la forza, ma continuamente cadendo".

BIBLIOGRAFIA

ADAMS A. A., *DRM: Valid protection or abusive control?,* in *International Review of Law, Computers & Technology*, 20, 3, 233-237, 2006, liberamente accessibile presso: «https://doi.org/10.5281/zenodo.810869».

ALBERTINI L., *La modifica al diritto d'autore europeo per tener conto del contesto digitale: note sugli artt. 11 (diritto degli editori) e 13 (responsabilità dei provider) della bozza di Direttiva UE nel febbraio 2019, uscita dalla fase c.d. trilogue*, in *MediaLaws*, Law and Media Working Paper Series no. 2/2019, 2019, liberamente accessibile presso: «https://www.medialaws.eu/wp-content/uploads/2019/04/Lorenzo.pdf».

ALPA G., RESTA G., *Le Persone e la Famiglia 1, Le persone fisiche e i diritti della personalità*, in Trattato di Diritto Civile (a cura di R. SACCO), Milano, 2019.

ANGELOPOULOS C., *On Online Platforms and the Commission's New Proposal for a Directive on Copyright in the Digital Single Market*, in *SSRN*, 2017, liberamente accessibile presso DOI: «10.2139/SSRN.2947800».

ANGELOPOULOS C., QUINTAIS J.P., *Fixing Copyright Reform: How to Address Online Infringement and Bridge the Value Gap*, in *Kluwer Copyright Blog*, 2018, liberamente accessibile presso: «http://*copyright*blog.kluweriplaw.com/2018/08/30/fixing-*copyright*-reform-address-online-infringement-bridge-value-gap/».

ANGELOPOULOS C., QUINTAIS J. P., *Fixing Copyright Reform: A Better Solution to Online Infringement,* 10(2) *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 2019, 147-172, liberamente accessibile presso: «https://www.jipitec.eu/issues/jipitec-10-2-2019/4913».

ARBER E., *A Transcript of the Registers of the Company of Stationers of London, 1554-1640 A.D.,* Stationer's Company, London, 1875.

AUTIERI P., *Il Caso Napster alla luce del diritto comunitario*, in UBERTAZZI L. C. (ed.), *TV, Internet e "new trends" di diritti d'autore e connessi,* Milano, 2003.

AXBERG R., *File-Sharing Tools and Copyright Law: A Study of In re Aimster Copyright Litigation and MGM Studios, Inc. v. Grokster, Ltd.*, Volume 35 Issue 1 Fall 2003, *Loyola University Chicago Law Journal*, 2003, liberamente accessibile presso: «https://lawecommons.luc.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1280&context=luclj».

BACKERMAN R., *How the RIAA Litigation Process Work,* in *recordindustryvspeople.blogspot.it*, 11 gennaio 2008, liberamente accessibile presso: «http://recordingindustryvspeople.blogspot.com/2007/01/how-riaa-litigation-process-works.html».

BARNETT LIDSKY L., *Silencing John Doe: Defamation & Discourse in Cyberspace*, 49 *Duke Law Journal* 855-946, 2000, liberamente accessibile presso: «https://scholarship.law.duke.edu/dlj/vol49/iss4/1/».

BARTOCCI U., *Aspetti giuridici dell'attività letteraria in Roma antica. Il complesso percorso verso il riconoscimento dei diritti degli autori,* Torino, 2009.

BELLI M., *La responsabilità dei «prestatori di servizi di condivisione di contenuti online» ai sensi della dir. 2019/790/UE*, in *Nuove Leggi Civ. Comm.,* 2020, 2, 551.

BENNETT H.S., *English Books & Readers 1558 to 1603,* Cambridge University Press, Cambridge, 1989.

BINCOLETTO G., *La privacy by design: Un'analisi comparata nell'era digitale*, in *Trento LawTech,* Student Paper n. 35, liberamente accessibile presso: «https://iris.unitn.it/retrieve/handle/11572/177733/511170/LawTech_Student_Papers_Bincoletto_Giorgia.pdf».

BOEVE M. R., *Will Internet Service Providers Be Forced to Turn in Their Copyright Infringing Customers? The power of the Digital Millennium Copyright Act's Subpoena Provision after In Re Charter Communication*, in *Hamline Law Review* 177, 2006, accessibile presso «https://heinonline.org/HOL/LandingPage?handle=hein.journals/hamlrv29&div=3&id=&page=».

BOWREY K., RIMMER M., *Rip, Mix, Burn: The Politics of Peer to Peer and Copyright Law*, 7 *First Monday* 8, 2002, liberamente consultabile presso: «http://www.firstmonday.dk/issues/issue7_8/bowrey/index.html».

BRIDY A., *The Price of Closing the 'Value Gap': How the Music Industry Hacked EU Copyright Reform*, in *Vanderbilt Journal of Entertainment & Technology Law*, volume 22, 2020, 323-358, liberamente accessibile presso: «https://ssrn.com/abstract=3412249» o «http://dx.doi.org/10.2139/ssrn.3412249».

CAMARELLA L., *La responsabilità dell'Internet Service Provider alla luce della nuova Direttiva sul diritto d'autore nel mercato unico digitale*, in *Trento Law and Technology Research Group,* Student Paper n. 58, liberamente accessibile presso:

«https://iris.unitn.it/retrieve/handle/11572/255244/311950/Trento%20LawTech%20-%20Laura%20Camarella_58.pdf».

CASO R., PASCUZZI G. (a cura di), *I diritti sulle opere digitali: copyright statunitense e diritto d'autore italiano*, Padova, 2002.

CASO R., *Digital rights management: il commercio delle informazioni digitali tra contratto e diritto d'autore*, Padova, 2004, liberamente accessibile presso: «http://eprints.biblio.unitn.it/4375/».

CASO R. (a cura di), *Digital Rights Management: problemi teorici e prospettive applicative. Atti del Convegno tenuto presso la Facoltà di Giurisprudenza di Trento il 21 ed il 22 marzo 2007*, Quaderni del dipartimento di Scienze Giuridiche; 70 (70), Università di Trento, Trento, 2008, liberamente accessibile presso: «http://eprints.biblio.unitn.it/1336/».

CASO R., *Il conflitto tra copyright e privacy nelle reti Peer to Peer: il caso Peppermint – Profili di diritto comparato,* 2007, liberamente accessibile presso: «http://eprints.biblio.unitn.it/1334/».

CASO R., *Il conflitto tra diritto d'autore e protezione dei dati personali: appunti dal fronte euro-italiano*, in *Diritto dell'Internet*, vol. 4, n. 5 IPSOA - Wolters - Kluwer, 466-472, 2008, disponibile sul sito: «http://eprints.biblio.unitn.it/1637/».

CASO R., *Alle Origini del Copyright e del Diritto d'Autore: Spunti in Chiave di Diritto e Tecnologia*, (The Origins of Copyright and Droit D'Auteur: Some Insights in the Law and Technology Perspective), in *Trento Law and Technology Research Group,* Research Paper Series No. 2, 2010, liberamente accessibile presso *SSRN*: «https://ssrn.com/abstract=2254259» o «http://dx.doi.org/10.2139/ssrn.2254259»

CASO R., *Misure tecnologiche di protezione: cinquanta (e più) sfumature di grigio della Corte di Giustizia europea*, in *Trento Law & Technology Research Group,* Research Paper No. 19, 2 aprile 2014, liberamente accessibile presso: «https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2424490».

CASO R., *Il diritto d'autore dell'era digitale,* in PASCUZZI G., (a cura di), *il diritto dell'era digitale*, Bologna, 2016, 145.

CASO R., *La società della mercificazione e della sorveglianza: dalla persona ai dati*, Milano, 2021, liberamente accessibile presso: «https://www.ledizioni.it/prodotto/la-societa-della-mercificazione-e-della-sorveglianza-dalla-persona-ai-dati/».

CASSANO G., BUFFA F., *Responsabilità del content provider e dell'host provider,* in *Il Corriere giuridic*o, fasc. 1, 2003, 77-81, liberamente consultabile presso: «https://www.altalex.com/documents/news/2005/07/19/responsabilita-del-content-provider-e-dell-host-provider».

COHEN J. E., *Lochner in Cyberspace: the New Economic Orthodoxy of Rights Management,* 97 *Mich. L. Rev.* 462 (1998), liberamente accessibile presso: «https://scholarship.law.georgetown.edu/facpub/811/».

COHEN J. E., *DRM and Privacy,* 18 *Berkeley Tech. L.J.* 575-617 (2003), in *Georgetown Law Faculty Publications and Other Work*, liberamente accessibile presso: «https://scholarship.law.georgetown.edu/facpub/60».

COHEN J. E., *The Place of the User in Copyright Law*, 74 *Fordham L.Rev.* 347-374, (2005), liberamente accessibile presso: «https://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=1059&context=facpub».

D'ARRIGO R., *Recenti sviluppi in tema di responsabilità degli Internet Service Providers*, Milano, 2012.

DAFFARRA L. *Copyright, come identificare gli autori delle violazioni nel file-sharing secondo la Corte di Giustizia UE*, in *Agenda Digitale.EU*, liberamente accessibile presso: «https://www.agendadigitale.eu/mercati-digitali/*copyright*-la-Corte-di-giustizia-fa-chiarezza-sullidentificazione-degli-autori-delle-violazioni-nel-file-sharing/».

DE ANGELIS D., LEVA F., *The Italian transposition of the CDSM Directive: A missed opportunity?*, in *Communia*, 28 aprile 2021, disponible sul sito: «https://www.communia-association.org/2021/04/28/the-italian-transposition-of-cdsm-a-missed-chance/».

DE CATA M., *Il caso Peppermint. Ulteriori riflessioni anche alla luce del caso Promusicae*, in *Rivista di diritto industriale*, vol. 57, fasc. 4/5, 2008.

DE CATA M.*, La responsabilità civile dell'Internet Service Provider*, Milano, 2010.

DEKEL T., RUBINSTEIN M., LIU C., FREEMAN W. T., *Google Research, On the Effectiveness of Visible Watermarks,* in *Computer Vision Foundation e IEEE Xplore*, 2017, disponibile in open access presso: *«https://openaccess.thecvf.com/content_cvpr_2017/papers/Dekel_On_the_Effectiveness_CVPR_2017_paper.pdf*».

DEL NINNO A., *Il caso Promusicae-Telefonica: la Corte di Giustizia UE si pronuncia sul rapporto tra tutela della privacy e protezione del copyright nell'ordinamento comunitario*, in *Diritto & Giustizia,* 2 Febbraio 2008, liberamente accessibile presso: «https://www.alessandrodelninno.it/articoli-singolo.php?id=22&L=en&L=en&L=en».

DORE G., *Plagio e diritto d'autore. Un'analisi comparata e interdisciplinare*, Milano, 2021, accessibile presso: «https://zenodo.org/record/5961499#.YnifBy2uZ-W»

DUTCHER T. A., *A Discussion of the Mechanics of the DMCA Safe Harbor and Subpoena Power, as applied in RIAA v. Verizon Internet Services*, in *Santa Chiara Computer & High Tech Law Journal* 493, 2005, liberamente accessibile presso «https://digitalcommons.law.scu.edu/chtlj/vol21/iss2/6/».

ENGELER M., *Copyright Directive: Does the best effort principle comply with GDPR*?, in *Telemedicus. Recht der Informationsgesellschaft*, 23 marzo 2019, liberamente accessibile presso: «https://www.telemedicus.info/*copyright*-directive-does-the-best-effort-principle-comply-with-gdpr/».

FISHER W., *Theories of Intellectual Property*, in MUNZER S. (ed.), *New Essays in the Legal and Political Theory of Property*, Cambridge University Press, 2001, liberamente accessibile presso: «https://cyber.harvard.edu/people/tfisher/iptheory.pdf».

FISHER W., YANG C., *Peer-to-Peer Copying, an Introduction*, in *Berkman Center for Internet & Society* (Nov. 18, 2001), liberamente accessibile presso: «http://cyber.law.harvard.edu/ilaw/P2P.html».

FLORIO A., *I sistemi di Digital Rights Management (DRM)* in *dirittodellinformatica.it*, 2009, disponibile sul sito: «https://www.dirittodellinformatica.it/diritto-autore/*copyright*-focus/i-sistemi-di-digital-rights-management-drm.html».

FREELAND A., *Negotiating Under the New EU Copyright Directive 2019/790 and GDPR,* in *Journal of International Economic Law*, 2020, liberamente accessibile presso: «https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3573605».

FROSIO G., *The Death of No Monitoring Obligations: A Story of Untameable Monsters*, 8(3) *Journal of Intellectual Property, Information Technology and E-Commerce Law (JIPITEC)* 212, 2017 liberamente accessibile presso SSRN: «https://ssrn.com/abstract=2980786».

GALGANO F., *Storia del diritto privato romano, Torino, 2017.*

GEIGER C., *Intellectual Property shall be protected!? – Article 17 (2) of the Charter od Fundamental Rights of the European Union: a Mysterious provision with an Unclear Scope*, in *European Intellectual Property Review* 113, 2009, liberamente accessibile presso: «https://www.researchgate.net/profile/Christophe-Geiger/publication/43234343_Intellectual_Property_shall_be_protected_Article_17_2_of_the_Charter_of_Fundamental_Rights_of_the_European_Union_a_Mysterious_Provision_with_an_Unclear_Scope/links/56b30e8f08ae795dd5c7dbb0/Intellectual-Property-shall-be-protected-Article-17-2-of-the-Charter-of-Fundamental-Rights-of-the-European-Union-a-Mysterious-Provision-with-an-Unclear-Scope.pdf».

GEIGER C., JÜTTE B.J., *Platform liability under article 17 of the copyright in the Digital Single Market directive, automated filtering and fundamental rights: an impossible match*, in *PIJIP/TLS Research Paper Series* no. 64, 2020, liberamente accessibile presso: «https://digitalcommons.wcl.american.edu/research/64/».

GEIGER C., JÜTTE B.J., *The EU Commission's Guidance on Article 17 of the Copyright in the Digital Single Market Directive – A Guide to Virtue in Content Moderation by Digital Platforms?,* in *Intellectual Property: Copyright Law eJournal*, 2021, liberamente accessibile presso: «https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3876608».

GIANNI F., ORIGONI G., GRIPPO E., *Linking e diritto d'autore - La sentenza Svensson e altri contro Retriever Sverige AB della Corte di Giustizia dell'Unione Europea sul linking ad opere dell'ingegno messe a disposizione su Internet*, in *www.gop.it (Proprietà intellettuale, IT e Media)*, 2014, liberamente accessibile presso «https://www.gop.it/doc_pubblicazioni/367_jswrs4qohr_cn.pdf».

GIANNOPOULOU A., *Proposed Directive on Copyright in the Digital Single market: a missed opportunity?*, in *Zenodo*, 2018, liberamente accessibile presso: «https://doi.org/10.5281/zenodo.1415493».

GIARDINI G. *Le regole dell'informazione. Principi giuridici, strumenti, casi,* Milano, 2009.

GINSBURG J., *A United States Perspective on Digital Single Market Directive Art. 17, EU COPYRIGHT LAW: A COMMENTARY*, STAMATOUDI I., TORREMANS P., eds., *Columbia Public Law Research Paper* No. 14-654, liberamente accessibile presso: «https://ssrn.com/abstract=3579076».

GIOVANELLA F., *Enforcement del diritto d'autore nell'ambito di Internet vs. protezione dei dati personali: bilanciamento tra diritti fondamentali e contesto culturale*, in *Trento Law and Technology Research Group*, Research Paper n.20, 2014, liberamente accessibile presso: «http://eprints.biblio.unitn.it/4273/».

GIOVANELLA F., *Copyright and Information Privacy. Conflicting Rights in Balance*, Cheltenham, 2017.

GUARDA P., *Meraviglioso come a volte ciò che sembra non è: la qualificazione giuridica del contratto,* in PASQUINO T. (a cura di), *Antologia di Casi Giurisprudenziali, Materiali per lo studio del diritto privato*, seconda edizione, Torino, 2015, 165.

HALDERMAN J. A., FELTEN E. W, *Lessons from the Sony DRM Episode*, *Ctr. for Info. Tech., Princeton Univ., Dep't of Computer Sci.*, Working Paper, 2006, liberamente accessibile presso: «http://itpolicy.princeton.edu/pub/sonydrm-ext.pdf».

HANUZ B., *Direct Copyright Liability As Regulation Of Hosting Platforms For The CopyrightInfringing Content Uploaded By Their Users: Quo Vadis?,* 11(3) *Journal of Intellectual Property, Information Technology and E-Commerce Law* (2020), 315-339, liberamente accessibile presso: «https://www.jipitec.eu/issues/jipitec-11-3-2020/5186».

HOLLAAR L. A., *Sony Revisited: A new look at contributory copyright infringement*, in *University of Utah*, 2004, liberamente accessibile presso: «http://digital-law-online.info/papers/lah/sony-revisited-june6.pdf».

HUSOVEC M., QUINTAIS J., *How to License Article 17? Exploring the Implementation Options for the New EU Rules on Content-Sharing Platforms* (January 2021) in *GRUR International* (Issue 4/2021), liberamente accessibile presso «https://ssrn.com/abstract=3463011» o «http://dx.doi.org/10.2139/ssrn.3463011».

IZZO U., *Alle radici della diversità tra copyright e diritto d'autore*, in PASCUZZI G., CASO R., *I diritti sulle opere digitali*, Padova, 2002, 43.

IZZO U., *Alle origini del copyright e del diritto d'autore. Tecnologia, interessi e cambiamento giuridico,* Roma, 2010.

JACQUES S., GARSTKA K., HVIID M., STREET J., *An Empirical Study of the Use of Automated Anti-Piracy Systems and Their Consequences for Cultural Diversity*, in 15(2) *SCRIPTed* (2018), 277-312, liberamente accessibile presso: «https://script-ed.org/article/an-empirical-study-of-the-use-of-automated-anti-piracy-systems-and-their-consequences-for-cultural-diversity/».

JOHNS A., *Pop music pirate hunters*, in *Daedalus*, vol. 131, no. 2, 2002, liberamente accessibile presso: «https://www.amacad.org/publication/pop-music-pirate-hunters».

JOHNS A., *Pirateria: storia della proprietà intellettuale da Gutenberg a Google*, Torino, 2011.

KATYAL S., *Privacy vs. Piracy*, *Yale Journal of Law & Technology* 222, 272-273 (2004), liberamente accessibile presso SSRN: «https://ssrn.com/abstract=722441».

KELLER P., *Divergence instead of guidance: the Article 17 implementation discussion in 2020 – Part 1*, in *Kluwer Copyright Blog*, 2020, liberamente accessibile presso: «http://*copyright*blog.kluweriplaw.com/2021/01/21/divergence-instead-of-guidance-the-article-17-implementation-discussion-in-2020-part-1/».

KELLER P., *CJEU hearing in the Polish challenge to Article 17: Not even the supporters of the provision agree on how it should work*, in *Kluwer Copyright Blog*, 2020, liberamente accessibile presso: «http://copyrightblog.kluweriplaw.com/2020/11/11/cjeu-hearing-inthe-polish-challenge-to-article-17-not-even-the-supporters-of-the-provision-agree-onhow-it-should-work/».

KUCZERAWY A., *From 'Notice and take down' to 'Notice and Stay Down': Risks and Safeguards for Freedom of Expression*, in FROSIO G. (ed), *The Oxford Handbook of Intermediary Liability Online*, 2019, liberamente accessibile presso: «https://ssrn.com/abstract=3305153».

LA BELLE M. M., *The 'Rootkit Debacle': The Latest Chapter in the Story of the Recording Industry and the War on Music Piracy* (2006), in *Denver University Law Review*, Vol. 84, No. 1, p. 79, 2006, CUA Columbus School of Law Legal Studies Research Paper No. 2010-28, liberamente accessibile presso: «https://ssrn.com/abstract=1564903».

LA ROSA A., *La nuova Direttiva "Copyright" (n. 2019/790): focus su art. 17*, in *4cLegal*, 11 gennaio 2021, liberamente accessibile presso: «https://www.4clegal.com/opinioni/nuova-Direttiva-*copyright*-n-7902019-focus-art-17».

LARROYED A., *When Translations Shape Legal Systems: How Misguided Translations Impact Users and Lead to Inaccurate Transposition – The Case of 'Best Efforts' Under Article 17 DCDSM*, in *SRNN*, 2020, liberamente accessibile presso: «https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3740066».

LARSON R. G., GODFREAD P. A., *Bringing John Doe to Court: Procedural Issues in Unmasking Anonymous Internet Defendants,* in *William Mitchell Law Review* 328, Vol. 38: Iss. 1, Article 6., 2011, liberamente accessibile presso: «https://open.mitchellhamline.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1435&context=wmlr».

LEE A. J., *MGM Studios, Inc. v. Grokster, Ltd. & In re Aimster Litigation: A Study of Secondary Copyright Liability in the Peer-to-Peer Context*, in *Berkeley Technology Law Journal*, vol. 20:485, liberamente accessibile presso: «https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjhkN_p4cfzAhUnhP0HHaXxCboQFnoECAMQAQ&url=https%3A%2F%2Flawcat.b

erkeley.edu%2Frecord%2F1119856%2Ffiles%2Ffulltext.pdf&usg=AOvVaw30jatFo-VDjNIaPQQtCJCU».

LEFEBVRE F., CHUPEAU B., MASSOUDI A., DIEHL E., *Image and video fingerprinting: forensic applications*, in *Proc. SPIE* 7254, in *Media Forensics and Security*, 725405, 2009, liberamente accessibile presso «https://www.spiedigitallibrary.org/conference-proceedings-of-spie/7254/1/Image-and-video-fingerprinting-forensic-applications/10.1117/12.806580.short?SSO=1».

LEISTNER M., *European Copyright Licensing and Infringement Liability Under Art. 17 DSM-Directive Compared to Secondary Liability of Content Platforms in the U.S. – Can We Make the New European System a Global Opportunity Instead of a Local Challenge?*, in *Zeitschrift für Geistiges Eigentum/Intellectual Property Journal (ZGE/IPJ)*, Issue 2, 123-214, 2020, liberamente accessibile presso: «https://ssrn.com/abstract=3572040».

LIGUORI J., *La responsabilità degli Internet Service Provider*, Tesi di dottorato, in Diritto, economia e finanza internazionali, Università degli Studi di Parma, 2012, liberamente accessibile presso: «https://www.repository.unipr.it/bitstream/1889/1787/3/Tesi%20Jacopo%20Liguori%20La%20Responsabilità%20degli%20Internet%20Service%20Provider.pdf».

LOO A. W. S., *Peer-to-peer computing: Building Supercomputers with web Technologies*, Berlino, 2007.

LUCCHI N., *DRM, Contratto Protezione Dei Consumatori*, in CASO R. (a cura di), *Digital Rights Management: problemi teorici e prospettive applicative. Atti del Convegno tenuto presso la Facoltà di Giurisprudenza di Trento il 21 ed il 22 marzo 2007*, Quaderni del dipartimento di Scienze Giuridiche; 70 (70), Università di Trento, Trento, 2008, liberamente accessibile presso: «http://eprints.biblio.unitn.it/1336/».

LUCCHINI GUASTALLA E., *Il Nuovo Regolamento Europeo Sul Trattamento Dei Dati Personali*: *I Principi Ispiratori*, in *Contratto e Impr.*, 2018, 1, 106.

MILES E., *In re Aimster & MGM, Inc. v. Grokster, Ltd.: Peer-to-Peer and the Sony Doctrine,* in *Berkeley Technology Law Journal*, 19(1), 21–57, 2004, liberamente accessibile presso: «http://www.jstor.org/stable/24117528».

MOHANTY S. P., SENGUPTA A., et. al., *Everything You Want to Know About Watermarking: From Paper Marks to Hardware Protection*, in *IEEE Consumer Electronics Magazine* 6(3), 2017, liberamente accessibile presso: «https://www.researchgate.net/publication/309179925_Everything_you_Wanted_to_Know_About_Watermarking_From_Paper_Marks_to_Hardware_Protection».

MONTAGNANI M. L., *A New Interface between Copyright Law and Technology: How User-Generated Content Will Shape the Future of Online Distribution*, in *Bocconi Legal Studies Research Paper* No. 1275326, 2009, liberamente accessibile presso: «https://ssrn.com/abstract=1275326».

MONTAGNANI M. L., TRAPOVA A., *New Obligations for Internet Intermediaries in the Digital Single Market — Safe Harbors in Turmoil?*, in *Journal of Internet Law*, Jan 2019, Vol. 22 Issue 7, p3-11. 9p., 2019, liberamente accessibile presso: «https://ssrn.com/abstract=3361073».

MONTAGNANI M. L., *A New Liability Regime for Illegal Content in the Digital Single Market Strategy*, in *SSRN,* 2019, liberamente accessibile presso: «https://ssrn.com/abstract=3398160».

MONTAGNANI M. L., *Virtues and Perils Of Algorithmic Enforcement and Content Regulation in The EU – A Toolkit For A Balanced Algorithmic Copyright Enforcement*, in *Case Western Reserve Journal of Law, Technology & the Internet*, Vol. 11, No. 1, 2020, *Bocconi Legal Studies Research Paper* No. 3767008, liberamente accessibile presso: «https://ssrn.com/abstract=3767008».

MORGESE G., *La Normativa Internazionale ed Europea sul Diritto d'autore*, in *La Comunità Internazionale* Fasc. 4/2014 Pp. 569-594 Editoriale Scientifica Srl, liberamente accessibile presso: «https://www.uniba.it/docenti/morgese-giuseppe/pubblicazioni/Articolodirittoautore.pdf».

MOSCATI L., *Alessandro Manzoni avvocato: la causa contro le Monnier e le origini del diritto d'autore in Italia,* Bologna, 2017, accessibile liberamente presso: «https://www.academia.edu/35712441/Alessandro_Manzoni_avvocato_la_causa_contro_le_Monnier_e_le_origini_del_diritto_dautore_in_Italia».

NORDEMANN J.B., WAIBLINGER J., *Art. 17 DSMCD: a class of its own? How to implement Art. 17 into the existing national copyright acts, including a comment on the recent German Discussion Draft – Part 1*, in *Kluwer Copyright Blog*, 2020, liberamente accessibile presso: «http://copyrightblog.kluweriplaw.com/2020/07/16/art.-17-dsmcd-a-class-of-its-ownhow-to-implement-art.-17-into-the-existing-national-copyright-acts-including-acomment-on-the-recent-german-discussion-draft-part1/?doing_wp_cron=1597142146.3135290145874023437500».

NORDEMANN J.B., WAIBLINGER J., *Art. 17 DSMCD: a class of its own? How to implement Art. 17 into the existing national copyright acts, including a comment on the recent German Discussion Draft – Part 2*, in *Kluwer Copyright Blog*, 2020, liberamente accessibile presso: «http://copyrightblog.kluweriplaw.com/2020/07/17/art.-17-dsmcd-a-class-of-its-ownhow-to-implement-art.-17-into-the-existing-national-copyright-acts-including-acomment-on-the-recent-german-discussion-draft-part2/?doing_wp_cron=1597144877.2035028934478759765625».

O'ROURKE M. A., *Property Rights and Competition on the Internet: In Search of an Appropriate Analogy*, 16 *Berkeley Tech. L.J.* 561, 570-71 (2001), liberamente accessibile presso: «https://www.jstor.org/stable/24115693».

PALMIERI A., *DRM e Disciplina Europea della Protezione dei Dati Personali* in R. CASO (a cura di), *Digital Rights Management: problemi teorici e prospettive applicative. Atti del Convegno tenuto presso la Facoltà di Giurisprudenza di Trento il 21 ed il 22 marzo 2007*, Quaderni del dipartimento di Scienze Giuridiche; 70 (70), Università di Trento, Trento, 2008, liberamente accessibile presso: «http://eprints.biblio.unitn.it/1336/».

PASCUZZI G., *La videoregistrazione domestica di opere protette davanti alla «Supreme Court»*, nota alla sentenza Sony Corp. of America v. Universal City Studios, in *Foro it.*, 1984, IV, 351, disponibile anche al sito: «https://www.giovannipascuzzi.eu/1984/10/23/la-videoregistrazione-domestica-di-opere-protette-davanti-alla-supreme-court/».

PASCUZZI G., *Opere musicali su Internet: il formato MP3*, in *Foro it.*, 2001, IV, 101-111.

PASCUZZI G., (a cura di*), Il diritto dell'era digitale. Tecnologie informatiche e regole privatistiche*, II ed., Bologna, 2006.

PASCUZZI G., GIOVANELLA F., *Dal diritto alla riservatezza alla computer privacy,* in PASCUZZI G., (a cura di) *Il diritto dell'era digitale,* Bologna, 2016, 43 e ss.

PASCUZZI G., *Il problem solving nelle professioni legali*, Bologna, 2017.

PASQUINO T.*, Servizi telematici e criteri di responsabilità*, Milano, 2003.

PIEVATOLO M. C., *L'età del privilegio*, in *Rivista il Mulino*, 2 aprile 2019, disponibile sul sito: «https://www.rivistailmulino.it/a/l-et-del-privilegio».

POLLICINO O., BASSINI M., *Free Speech, Defamation and the Limits to Freedom of Expression in the EU: A Comparative Analysis,* in SAVIN A., TRZASKOWSKI J., (eds), *Research Handbook on EU Internet Law*, 2014, Bocconi Legal Studies Research Paper No. 2706112, liberamente accessibile presso: «https://ssrn.com/abstract=2706112».

POLLICINO O., *Right to Internet Access: Quid Iuris?*, in VON ARNAULD A., VON DER DECKEN K., SUSI M. (eds), *The Cambridge Handbook on New Human Rights. Recognition, Novelty, Rhetoric*, Cambridge, 2019, liberamente accessibile presso: «https://ssrn.com/abstract=3397340».

POLLICINO O., SOMAINI L., *Online Disinformation and Freedom of Expression in the Electoral Context: The European and Italian Responses* (2020), in BAUME S., BOILLET V., MARTENET V. (eds), *Misinformation in referenda*, 2020, liberamente accessibile presso: «https://ssrn.com/abstract=3552680».

POSNER R. A., *Il piccolo libro del plagio,* Roma, 2007.

PROSSER W. L., *Privacy,* in *California Law Review* 383, 1960, liberamente accessibile presso: «https://lawcat.berkeley.edu/record/1109651».

QUILTER L., *Note, The Continuing Expansion of Cyberspace Trespass to Chattels*, 17 *Berkeley Tech. L.J.* 421, 423-24 (2002), liberamente accessibile presso: «https://www.jstor.org/stable/24120114».

QUINTAIS J.P., FROSIO G., GOMPEL S., HUGENHOLTZ P. B., HUSOVEC M., JÜTTE B. J., SENFTLEBEN M., *Safeguarding User Freedoms in Implementing Article 17 of the Copyright in the Digital Single Market Directive: Recommendations from European Academics*, 10 (2020) *JIPITEC* 277, liberamente accessibile presso: «https://www.jipitec.eu/issues/jipitec-10-3-2019/5042».

QUINTAIS J.P., *The New Copyright in the Digital Single Market Directive: A Critical Look* in *European Intellectual Property Review,* in *SSRN,* 2020, liberamente accessibile presso: «https://ssrn.com/abstract=3424770» o «http://dx.doi.org/10.2139/ssrn.3424770».

QUINTAIS J.P., JOOST POORT J., *The Decline of Online Piracy: How Markets – Not Enforcement – Drive Down Copyright Infringement*, in *American University International Law Review*, Vol. 34, No. 4, pp. 807-876, 2019, liberamente accessibile presso: «https://ssrn.com/abstract=3437239».

QUINTAIS J. P., MEZEI P., HARKAI I., MAGALHÃES J. C., KATZENBACH C., SCHWEMER S. F., RIIS T., *Final Report on mapping of EU legal framework and intermediaries' practices on copyright content moderation and removal*, in *Zenodo*, 2022, liberamente accessibile presso: «https://doi.org/10.5281/zenodo.6461568».

QUINTAIS J. P., *Article 17 survives, but freedom of expression safeguards are key: C-401/19 – Poland v Parliament and Council,* in *Kluwer Copyright Blog*, 26 aprile 2022, liberamente accessibile presso: «http://copyrightblog.kluweriplaw.com/2022/04/26/article-17-survives-but-freedom-of-expression-safeguards-are-key-c-401-19-poland-v-parliament-and-council/».

REDA J., SELINGER J., SERVATIUS M., *Article 17 of the Directive on Copyright in the Digital Single Market: a Fundamental Rights Assessment,* in *Gesellschaft für Freiheitsrechte*, 2020, liberamente accessibile presso: «https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3732223».

REDA F., KELLER P., *CJEU upholds Article 17, but not in the form (most) Member States imagined,* in *Kluwer Copyright Blog*, 28 aprile 2022, liberamente accessibile presso: «http://copyrightblog.kluweriplaw.com/2022/04/28/cjeu-upholds-article-17-but-not-in-the-form-most-member-states-imagined/».

RICCIO G. M., *La responsabilità civile degli Internet providers*, Torino, 2002, 207-208, liberamente accessibile presso: «https://www.researchgate.net/publication/286454131_La_responsabilita_civile_degli_Internet_providers».

RICCIO G. M., GIANNONE CODIGLIONE G., *Copyright Collecting Societies, Monopolistic Positions and Competition in the EU Single Market*, in *Masaryk University Journal of Law and Technology* (MUJLT), Vol. 7, Fall, 2013, liberamente accessibile presso SSRN: «https://ssrn.com/abstract=2398891».

RICE C. M., *Meet John Doe: It is Time for Federal Civil Procedure to Recognize John Doe Parties,* in 57 *U. Pitt. L. Rev.* 883 (1995), liberamente accessibile presso: «https://scholarship.law.ua.edu/cgi/viewcontent.cgi?article=1035&context=fac_articles».

ROBINSON E. A., *Digital Rights Management, Fair Use, and Privacy: Problems for Copyright Enforcement through Technology* (2009), in *Other Topics* 12, liberamente accessibile presso: «https://soar.usa.edu/other/12».

ROMERO MORENO F., '*Upload filters' and human rights: implementing Article 17 of the Directive on Copyright in the Digital Single Market*, 34(2) *International Review of Law, Computers & Technology* (2020), 153-182, liberamente accessibile presso: «https://www.tandfonline.com/doi/full/10.1080/13600869.2020.1733760».

ROSATI E., *DSM Directive Series #5: Does the DSM Directive mean the same thing in all language versions? The case of 'best efforts' in Article 17(4)(a)*, in *The IPKat,* 2019, liberamente acessibile presso: «https://ipkitten.blogspot.com/2019/05/dsm-directive-series-5-does-dsm.html».

ROSATI E., *Article 17 of the DSM Directive is valid: an early take on today's Grand Chamber ruling,* in *The IPKat*, 26 aprile 2022, liberamente accessibile presso: «https://ipkitten.blogspot.com/2022/04/article-17-of-dsm-directive-is-valid.html».

ROSENBLATT B., DYKSTRA G., *Integrating Content Management with Digital Rights Management: Imperatives and Opportunities for Digital Content Lifecycles*, in *Giantsteps Media Technology Strategies and Dykstra Research*, 2003, liberamente accessibile presso: «https://robertoigarza.files.wordpress.com/2010/03/art-integrating-content-management-with-digital-rights-management-vvaa-2003.pdf».

RUSSINOVICH M., *Sony, Rootkits and Digital Rights Management Gone Too Far*, in *Mark's Blog Microsoft MSDN*, 31 ottobre 2005, liberamente accessibile presso: «https://web.archive.org/web/20150317040653/http://blogs.technet.com/b/markrussinovich/archive/2005/10/31/sony-rootkits-and-digital-rights-management-gone-too-far.aspx».

RUSSINOVICH M., *More on Sony: Dangerous Decloaking Patch, EULAs and Phoning Home*, in *TechNet*, 4 novembre 2005, liberamente consultabile presso:«https://techcommunity.microsoft.com/t5/windows-blog-archive/more-on-sony-dangerous-decloaking-patch-eulas-and-phoning-home/ba-p/723452».

SAETTA B., *Il copyright, il filtraggio dei contenuti, il ricorso della Polonia respinto e il futuro della Rete*, in *ValigiaBlu*, 30 aprile 2022, liberamente consultabile presso il sito: «https://www.valigiablu.it/copyright-polonia-futuro-rete/».

SAKULA A. *Doctor Nehemiah Grew (1641-1712) and the Epsom salts,* in *Clio Med. 1984*; 19(1-2):1-21. PMID: 6085985, 1984, liberamente accessibile presso «https://pubmed.ncbi.nlm.nih.gov/6085985/».

SAMUELSON P., *Pushing Back on Stricter Copyright ISP Liability Rules,* in *Michigan Technology Law Review*, 2020, liberamente accessibile presso: «https://ssrn.com/abstract=3630700».

SANTUCCI G., *Diritti dell'autore in Roma antica?,* in *Index*, 2011, 143.

SANTUCCI G., *Diritto romano e diritti europei, Continuità e discontinuità nelle figure giuridiche,* Bologna, 2018.

SCHMON C., *Filtri automatici e privacy: la tempesta perfetta*, in *Electonic Frontier Foundation*, 3 marzo 2020, nella traduzione di DUCATO R. con la collaborazione di GUARDA P., 21 marzo 2020, liberamente accessibile presso: «https://www.eff.org/it/deeplinks/2020/02/upload-filters-are-odds-gdpr».

SCHWEMER S. F., SCHOVSBO J., *What is Left of User Rights? – Algorithmic Copyright Enforcement and Free Speech in the Light of the Article 17 Regime* (December 20, 2019), in TORREMANS P. (ed), *Intellectual Property Law and Human Rights,* 4th edition (Wolters Kluwer, 2020), pp. 569-589, liberamente accessibile presso: «https://ssrn.com/abstract=3507542» o «http://dx.doi.org/10.2139/ssrn.3507542».

SCIALDONE M., *I profili internazionali del Diritto d'Autore*, in *Altalex.com*, 2008, liberamente accessibile presso: «https://www.altalex.com/documents/news/2010/03/24/i-profili-internazionali-del-diritto-d-autore».

SENFTLEBEN M., ANGELOPOULOS C., *The Odyssey of the Prohibition on General Monitoring Obligations on the Way to the Digital Services Act: Between Article 15 of the E- Commerce Directive and Article 17 of the Directive on Copyright in the Digital Single Market*, in *SSRN*, 2020, liberamente accessibile presso: «https://ssrn.com/abstract=3717022».

SENICAR V., JERMAN-BLAZIC B., KLOBUCAR T., *Privacy-Enhancing Technologies—approaches and development, Laboratory for Open Systems and Networks, Jozef Stefan Institute*, Jamova 39, 1000 Ljubljana, Slovenia, liberamente accessibile presso: «https://www.researchgate.net/publication/223673501_Privacy-Enhancing_Technologies-approaches_and_development».

SGANGA C., *A Decade of Fair Balance Doctrine, and How to Fix It: Copyright Versus Fundamental Rights Before the CJEU from Promusicae to Funke Medien, Pelham and Spiegel Online,* in *European Intellectual Property Review* (n.11/2019), 2019, liberamente accessibile presso SSRN: «https://ssrn.com/abstract=3414642».

SGANGA C., *A New Era for EU Copyright Exceptions and Limitations? Judicial Flexibility and Legislative Discretion in the Aftermath of the CDSM Directive and the Trio of the Grand Chamber of the CJEU,* in *ERA Forum*, vol.21, pp.311-339, 2020, liberamente accessibile presso: «https://ssrn.com/abstract=3804228».

SOLOVE D.J., SCHWARTZ P.M., *Privacy information and technology,* Boston, 2009.

SOLOVE D.J., SCHWARTZ P. M., *Information privacy law*, Boston, 2014.

SPEDICATO G., *I Digital Rights Management System tra produzione e diffusione di opere dell'ingegno. Quale nuovo assetto per il diritto d'autore*?, in *Ciberspazio e diritto*, vol. 5, n. 3, 2004, pp. 273-302.

SPEDICATO G., *Le misure tecnologiche di protezione del diritto d'autore nella normativa italiana e comunitaria*, in *Ciberspazio e diritto*, 2006, fasc. 4 pag. 535 – 580.

SPOERRI T., *On Upload-Filters and other Competitive Advantages for Big Tech Companies under Article 17 of the Directive on Copyright in the Digital Single Market,* 10(2) *Journal of Intellectual Property, Information Technology and E-Commerce Law* (2019), liberamente accessibile presso: «https://www.jipitec.eu/issues/jipitec-10-2-2019/4914/JIPITEC_10_2_2019_173_Spoerri».

STALLMAN R., *The Right to Read*, 1997, liberamente consultabile presso: «http://www.gnu.org/philosophy/right-to-read.html».

STEINMETZ R., WEHRLE K., *Peer-to-peer Systems and Applications*, Berlino, 2005.

TERRY R., *Plagiarism: A Literary Concept in England to 1775*, in *English*, vol. 56, spring 2007, 1, 2.

TRIPALDI G., *Digital Rights Management: come affrontare la salvaguardia del Copyright nell'era digitale*, Milano, 2002.

UBERTAZZI L. C., *Commentario breve alle leggi su proprietà intellettuale e concorrenza,* Volume 5 di Breviaria iuris, Padova, 2019.

URBAN J.M., KARAGANIS J., SCHOFIELD B.L., *Notice and takedown in everyday practice, Version 2*: Updated March 2017, in *SSRN*, liberamente accessibile presso: «https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2755628».

VERBIEST T., SPINDLER G., RICCIO G. M., *Study on the Liability of Internet Intermediaries*, in *SSRN*, 2007, liberamente accessibile presso: «https://ssrn.com/abstract=2575069» o «http://dx.doi.org/10.2139/ssrn.2575069».

WARREN S. D., BRANDEIS L. D., *The Right to Privacy,* in *Harvard Law Review*, Vol. 4, No. 5. (Dec. 15, 1890), pp. 193-220 liberamente accessibile presso: «https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf».

INDICE DELLE DECISIONI

GIURISPRUDENZA STATUNITENSE

Lake v. Wal-Mart Stores 528 N.W.2d 231 – Minn. 1998, liberamente accessibile presso: «https://casetext.com/case/lake-v-wal-mart-stores-inc-1».

Columbia Ins. Co. v. Seescandy.com, 185 F.R.D. 573 (N.D. Cal. 1999), liberamente consultabile presso: «https://cyber.harvard.edu/property00/domain/Sees.html».

In re Subpoena Duces Tecum to Am. Online, Inc., 52 Va. Cir 26, 2000, liberamente consultabile presso: «https://h2o.law.harvard.edu/cases/4393».

A&M Records, Inc v. Napster, 114 F. Supp. 2d 896, 900 (N.D. Cal 2000), liberamente accessibile presso: «https://law.justia.com/cases/federal/district-courts/FSupp2/114/896/2343353/».

A&M Records, Inc v. Napster, Inc., 239 F.3d 1004 (2001), liberamente accessibile presso: «https://casetext.com/case/a-m-records-inc-v-napster-inc-3».

Kyllo v. United States, 533 U.S. 27 (2001), liberamente accessibile presso: «https://supreme.justia.com/cases/federal/us/533/27/».

MGM Studios, Inc v. Grokster, Ltd, 259 F. Supp. 2d 1029 (C.D. Cal. 2003) liberamente consultabile presso: «https://law.justia.com/cases/federal/district-courts/FSupp2/259/1029/2362925/».

In re Verizon Internet Services, Inc. 240 F. Supp. 2d 24 (D.D.C. 2003), liberamente accessibile presso: «https://casetext.com/case/in-re-verizon-Internet-services-inc-5».

RIAA v. Verizon Internet Services, 351 F.3d 1229 (DC Cir. 2003), liberamente accessibile presso: «https://law.justia.com/cases/federal/appellate-courts/F3/351/1229/525976/».

In Re Verizon Internet Services, 257 F.Supp 2d 244 (D.D.C. 2003) (In Re Verizon 2), liberamente accessibile presso:«https://casetext.com/case/in-re-verizon-Internet-services-inc-4».

Eldred v. Ashcroft, 537 U.S. 186 (2003), liberamente accessibile presso: «https://supreme.justia.com/cases/federal/us/537/186/».

MGM Studios, Inc v. Grokster, Ltd 380 F.3d 1154 (9th Circuit, 2004), liberamente accessibile presso: «https://casetext.com/case/metro-goldwyn-mayer-v-grokster-ltd».

7 v. Corbis Corp. v. Amazon.com, Inc., 351 F. Supp. 2d 1090, (W.D. Wash. 2004), liberamente accessibile presso: «https://casetext.com/case/corbis-corporation-v-amazoncom-2».

Sony Music Entertainment, Inc. v. Does 1-40 326 F. Supp. 2d 556 (S.D.N.Y. 2004), liberamente accessibile presso: «https://www.casemine.com/judgement/us/5914b700add7b0493477c750».

Texas v. Sony BMG Music Entm't, Dist. Ct., Travis Co, Texas, (2005), liberamente accessibile presso: «http://www.sonysuit.com/classactions/texas/complaint.pdf».

MGM Studios, Inc v. Grokster, Ltd 545 U.S. 913 (2005), liberamente accessibile presso: «https://supreme.justia.com/cases/federal/us/545/913/».

In Re Charter Communications, Inc., Subpoena Enforcement Matter, 393 F.3d 771, 773, (8th Cir., 2005), liberamente accessibile presso: «https://casetext.com/case/in-re-charter-communications-inc-2».

In Re Subpoena to University of North Carolina at Chapel Hill, 367 F. Supp. 2d 945 (M.D.N.C., 2005), liberamente accessibile presso: «https://www.casemine.com/judgement/us/5914b65eadd7b04934778bb2».

Perfect 10, Inc. v. CCBill LLC, 448. F.3d 1102 (9th Cir. 2007), liberamente accessibile presso:«https://casetext.com/case/perfect-10-inc-v-ccbill-llc».

Arista Records, LLC v. Does 1-12, 2008 U.S Dist. LEXIS 825448, liberamente accessibile presso: «https://www.casemine.com/judgement/us/591469a7add7b049342dc137».

Arista Records, LLC v. Does 1-16, 2009 U.S. Dist. LEXIS 12159, liberamente accessibile presso: «https://www.anylaw.com/case/arista-records-llc-v-does-1-16/n-d-new-york/02-172009/o5ngRGYBTlTomsSBeJhp».

UMG Recordings, Inc. v. Veoh Networks, Inc., 665 F. Supp. 2d 1099, (C.D. Cal. 2009), liberamente accessibile presso: «https://casetext.com/case/umg-recordings-56».

U.S. v. Jones, 132 S. Ct. 945 (2012), liberamente accessibile presso: «https://www.law.cornell.edu/supremecourt/text/10-1259».

Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19, (2d Cir. 2012), liberamente accessibile presso: «https://cyber.harvard.edu/people/tfisher/cx/2012_Viacom.pdf».

Riley v. California, 136 S. Ct. 506 (2015), liberamente accessibile presso: «https://www.law.cornell.edu/supremecourt/text/13-132».

GIURISPRUDENZA EUROPEA

CGEU 12 giugno 2003, C-112/00, *Eugen Schmidberger, Internationale Transporte und Planzüge contro Republik Österreich*, liberamente accessibile presso: «https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A62000CJ0112».

CGUE 7 dicembre 2006, C-306/05, *Sociedad General de Autores y Editores de España (SGAE)*, liberamente accessibile presso: «https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A62005CJ0306&qid=1645712058879».

CGUE 29 gennaio 2008, C-275/06*, Productores de Música de España (Promusicae) v. Telefónica de España SAU*, Grande Sezione, liberamente consulatbile presso: «https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:62006CJ0275&from=IT».

CGUE 24 novembre 2011, C-70/10, *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, liberamente accessibile presso: «https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:62010CJ0070&from=EN».

CGUE 16 febbraio 2012, C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV*, liberamente consulatbile presso: «https://curia.europa.eu/juris/document/document.jsf?docid=119512&doclang=IT».

CGUE 19 aprile 2012, C-461/10, *Bonnier Audio AB v. Perfect Communication Sweden AB*, liberamente accessibile presso: «https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:62010CJ0461&from=IT».

CGUE 26 febbraio 2013, C-617/10, *Åkerberg Fransson*, liberamente accessibile presso: «https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:62010CJ0617&from=IT» (Ultimo accesso: 10 maggio 2022).

CGUE 7 marzo 2013, C-607/11, *ITV Broadcasting*, liberamente accessibile presso: «https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX%3A62011CJ0607».

CGUE 13 febbraio 2014, C-466/12, *Svensson et al c. Retriever Sverige AB*, liberamente consultabile presso: «https://curia.europa.eu/juris/document/document.jsf?text=&docid=147847&pageIndex=0&doclang=it&mode=lst&dir=&occ=first&part=1&cid=327328»,

CGUE 16 luglio 2015, C-580/13, *Coty Germany GmbH v. Stadtsparkasse Magdeburg*, (Quarta Sezione), liberamente accessibile presso: «https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:62013CJ0580&from=IT».

CGUE 8 settembre 2016, C-160/15, *GS Media BV contro Sanoma Media Netherlands BV, Playboy Enterprises International Inc., Britt Geertruida Dekker*, liberamente accessibile presso: «https://curia.europa.eu/juris/document/document.jsf?docid=183124&doclang=IT». (Ultimo accesso: 27 aprile 2022)

CGUE 15 settembre 2016, C-484/14, *Tobias Mc Fadden contro, Sony Music Entertainment Germany GmbH,* liberamente consultabile presso: «https://curia.europa.eu/juris/document/document.jsf?text=&docid=183363&pageIndex=0&doclang=IT&mode=req&dir=&occ=first&part=1».

CGUE 14 giugno 2017, C-610/15*, Stichting Brein contro Ziggo BV e XS4ALL Internet BV* (Seconda Sezione), liberamente consultabile presso: «https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:62015CJ0610&from=IT».

CGUE 1° ottobre 2019, C-673/17, *Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband eV contro P. GmbH*, liberamente accessibile presso: «https://curia.europa.eu/juris/document/document.jsf?docid=218462&doclang=IT».

CGUE 9 luglio 2020, C-264/19, *Constantin Film Verleih V. Youtube Llc. E Google Inc.*, (Quinta Sezione), disponibile presso: «https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:62019CJ0264&from=it».

CGUE 17 giugno 2021, C-597/19, *Mircom International Content Management & Consulting (M.I.C.M.) Limited contro Telenet BVBA*, (Quinta Sezione), liberamente consulatbile presso: «https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:62019CJ0597&from=IT».

CGUE 22 giugno 2021, C-682/18 e C-683/18, *YouTube e Cyando,* liberamente accessibile presso:

«https://curia.europa.eu/juris/document/document.jsf?text=&docid=243241&pageIndex=0&doclang=IT&mode=lst&dir=&occ=first&part=1&cid=170202»

CGUE 26 aprile 2022, C-401/2019, *Repubblica di Polonia contro Parlamento europeo, Consiglio dell'Unione europea*, liberamente accessibile presso: «https://curia.europa.eu/juris/document/document.jsf?text=&docid=258261&pageIndex=0&doclang=IT&mode=req&dir=&occ=first&part=1&cid=10742191».

GIURISPRUDENZA ITALIANA

Cass. Civ., 22.12.1956, no. 4487 in *Foro.it*, 1957, I, 423. (Caso Caruso)

Cass. Civ., 20.4.1963, no. 990, in *Giust. Civ.*, 1963, I, 1280 ed in *Foro.it.*, 1963, I, 129 (Caso Petacci)

Cass. 27.5.1975, n. 2129 in *Foro.it.*, 1976, I, 2895 (Caso Soraya Esfandiari v. Rusconi Editore)

Cass. 22.6.1985, n. 3769, in *Foro it.,* 1985, I, 2211 (Caso Veronesi)

Tribunale di Roma, ordinanza 18.8.2006, *in Riv. Dir. Ind.*, n 4-5/2008, II, 328

Tribunale di Roma, ordinanza 9.2.2007, in *Resp. Civ. e prev.,* n. 7-8/2007, 1699

Tribunale di Roma, ordinanza 14.7.2007 in *Rivista Diritto Industriale*, n. 4-5/200, II, 330.

Tribunale di Roma, ordinanza 16.7.2007 in *Dir. Informatica* n 4-5/2007, 828;

Trib. Milano, sentenza 3.9.2012, n.9749, in *Danno e responsabilità*, 2013, 51-61 con nota di FOFFA R.

Consiglio di Stato, Sentenza 29.3.2021 n. 2631, in *Foro it.*, 2021, VI, 325

ALTRI DOCUMENTI, PARERI, COMUNICAZIONI

Resolution 45/95, *Guidelines for the Regulation of Computerized Personal Data Files* adottate dalla Assemblea Generale (ONU) il 14 dicembre 1990, liberamente accessibili presso: «https://www.refworld.org/pdfid/3ddcafaac.pdf».

Gruppo di Lavoro Articolo 29, (Article 29 – WP), Opinion 2/2002 *On the use of unique identifiers in telecommunication terminal equipment: the example of IPv6*, adottata il 30 maggio 2002, disponibile presso: «http://www.eu.ipv6tf.org/PublicDocuments/wp58_en.pdf».

Gruppo di Lavoro Articolo 29, (Article 29 – WP) 104 - *Data Protection Issues And Intellectual Property; Working document on data protection issues related to intellectual property rights*, 18 gennaio 2005, 3, liberamente accessibile presso: «https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1497279».

Gruppo di Lavoro Articolo 29, (Article 29 – WP), Opinion 4/2007 *On the concept of personal data,* adottata il 20 giugno 2007 disponibile presso: «https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1496512».

Provvedimento Garante per la protezione dei dati personali 28 febbraio 2008 n. 1495246, nei confronti di Peppermint Jam Records GmbH, Techland sp. z. o.o. e Logistep AG, liberamente accessibile presso: «https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1495246».

Comunicati stampa 17 luglio 2007 e 13 marzo 2008: *Internet - Caso Peppermint: il Garante privacy si costituisce in giudizio*, liberamente consultabili presso: «https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1406297».

Indagine conoscitiva della Commissione europea, *Tecnologie a protezione dei dati*, Doc-Web 1680228, 17/12/09 liberamente accessibile presso: «https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1680228».

Provvedimento 4 luglio 2013 del Garante, *Linee guida in materia di attività promozionale e contrasto allo spam*, consultabile sul sito Internet garanteprivacy.it, doc. web n. 2542348, liberamente accessibile presso: «https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/2542348».

Commissione Europea (2015) M/530 *Commission Implementing Decision C(2015) 102 final of 20.1.2015 on a standardisation request to the European standardisation organisations as regards European standards and European standardisation deliverables for privacy and personal data protection management pursuant to Article 10(1) of Regulation (EU) No 1025/2012 of the European Parliament and of the Council in support of Directive 95/46/EC of the European Parliament and of the Council and in support of Union's security industrial policy*, liberamente accessibile presso: «http://ec.europa.eu/growth/tools-databases/mandates/index.cfm?fuseaction=search.detail&id=548».

Comunicazione della Commissione al Parlamento europeo e al Comitato delle regioni, *Strategia per il mercato unico digitale in Europa* (COM 2015 192), 6 maggio 2015, disponibile al link: «https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A52015DC0192».

Enisa Europa, *Privacy by design in big data*, in ENISA, dicembre 2015, liberamente consultabile presso: «https://www.enisa.europa.eu/publications/big-data-protection»;

Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions: *Online Platforms and the Digital Single Market Opportunities and Challenges for Europe*, COM/2016/0288 final, liberamente accessibile presso: «https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52016DC0288&from=EN».

Proposta di Direttiva del Parlamento Europeo e del Consiglio sul diritto d'autore nel mercato unico digitale COM/2016/0593 final - 2016/0280 (COD), liberamente accessibile presso: «https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52016PC0593&from=IT».

Gruppo Di Lavoro Articolo 29 Per La Protezione Dei Dati; *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del Regolamento 2016/790*; 17/IT WP 251 rev.01, adottate il 3 ottobre 2017; versione emendata e adottata in data 6 febbraio 2018, accessibili presso: «https://ec.europa.eu/newsroom/article29/items/612053».

Comunicazione della Commissione del 1° marzo 2018, *Raccomandazione (Ue) 2018/334 della Commissione sulle misure per contrastare efficacemente i contenuti illegali online*, disponibile all'indirizzo: «https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32018H0334&from=IT».

European Data Protection Supervisor (EDPS) *Opinion 5/2018 - Preliminary Opinion on Privacy by Design,* 31 maggio 2018, liberamente accessibile presso: «https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf»

ALAI, *DRAFT OPINION on certain aspects of the implementation of Article 17 of Directive (EU) 2019/790 of 17 April 2019 on copyright and related rights in the digital single market*, liberamente accessibile presso: «https://www.alai.org/en/assets/files/resolutions/200330-opinion-article-17- directive-2019_790-en.pdf»;

Ricorso proposto il 24 maggio 2019 — Repubblica di Polonia/Parlamento europeo e Consiglio dell'Unione europea (Causa C-401/19), liberamente consultabile presso: «https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:62019CN0401&from=EN».

Mission Report, *Towards more effectiveness of copyright law on online content sharing platforms: overview of content recognition tools and possible ways forward*, Report sottoposto al CSPLA il 28 November 2019, Ministero della Cultura Francese, liberamente accessibile presso: «https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiH8P6bzeX1AhWWQvEDHa6fDX0QFnoECAoQAQ&url=https%3A%2F%2Fwww.culture.gouv.fr%2Fcontent%2Fdownload%2F265045%2Ffile%2FMission%2520Report%2520Content%2520Recognition%2520Tools%2520ENG%2520V.pdf%3FinLanguage%3Dfre-FR&usg=AOvVaw2P9rxPn_MDDsQtYmdnYMZR».

Ufficio dell'Unione europea per la proprietà intellettuale, *Automated content recognition: discussion paper. Phase 1, Existing technologies and their impact on IP*, in European Union Intellectual Property Office, 2020, liberamente accessisibile presso: «https://data.europa.eu/doi/10.2814/52085»

United States Copyright Office, *Section 512 of Title 17, A Report Of The Register Of Copyrights*, Maggio 2020, 164 e ss, liberamente accessibile presso: «https://www.copyright.gov/policy/section512/section-512-full-report.pdf»

Communication From The Commission To The European Parliament And The Council: *Guidance on Article 17 of Directive 2019/790 on Copyright in the Digital Single Market* COM/2021/288 final, liberamente accessibili presso: «https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52021DC0288&from=EN»

Conclusioni Avvocato Generale Henrik Saugmandsgaard Øe, 15 luglio 2021 nella Causa C-401/19, Repubblica di Polonia contro Parlamento europeo, Consiglio dell'Unione europea, ricorso presentato ex art. 263 TFUE, liberamente accessibili presso: «https://curia.europa.eu/juris/document/document.jsf?text=&docid=244201&pageIndex=0&doclang=it&mode=lst&dir=&occ=first&part=1&cid=130522»

The Student Paper Series of the Trento LawTech Research Group is published since 2010

https://lawtech.jus.unitn.it/main-menu/paper-series/student-paper-series-of-the-trento-lawtech-research-group/

Freely downloadable papers already published:

STUDENT PAPER N. 76

Il binomio «sport e salute» nella riforma del diritto dello sport: istituzioni, strutture, professionalità e responsabilità

NICOLA INTRONA (2022), Trento Law and Technology Research Group, Student Paper Series; 76. Trento: Università degli Studi di Trento.

STUDENT PAPER N. 75

La libertà di panorama: profili critici e spunti comparatistici

CAROLINA BATTISTELLA (2022), Trento Law and Technology Research Group, Student Paper Series; 75. Trento: Università degli Studi di Trento. DOI: 10.5281/zenodo.6393008

STUDENT PAPER N. 74

The role of copyright in innovation: a comparative analysis of the legal framework of text and data mining

EUGENIO DE BIASI (2022), The role of copyright in innovation: a comparative analysis of the legal framework of text and data mining, Trento Law and Technology Research Group, Student Paper Series; 74. Trento: Università degli Studi di Trento. DOI: 10.5281/ZENODO.5897183

STUDENT PAPER N. 73

Risarcimento del danno da violazione dei diritti di proprietà intellettuale e retroversione degli utili. Un'analisi comparata

FEDERICO BRUNO (2022), Risarcimento del danno da violazione dei diritti di proprietà intellettuale e retroversione degli utili. Un'analisi comparata, Trento Law and Technology Research Group, Student Paper Series; 73. Trento: Università degli Studi di Trento. DOI: 10.5281/zenodo.5878282

STUDENT PAPER N. 72

Eccezioni e limitazioni al diritto d'autore nell'Unione Europea: profili critici e spunti comparatistici applicati al settore GLAM alla luce dell'emergenza Covid-19

ELEONORA MARONI (2021), Eccezioni e limitazioni al diritto d'autore nell'Unione Europea: profili critici e spunti comparatistici applicati al settore GLAM alla luce dell'emergenza Covid-19, Trento Law and Technology Research Group, Student Paper Series; 72. Trento: Università degli Studi di Trento. DOI:10.5281/zenodo.587821

STUDENT PAPER N. 71

L'*animal welfare* **nelle filiere alimentari: etichettatura e certificazioni**

ZANON MIRIANA (2021), L'***animal welfare*** nelle filiere alimentari: etichettatura e certificazioni, Trento Law and Technology Research Group, Student Paper Series; 71. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-959-8

STUDENT PAPER N. 70

Aggiornamenti di diritto agroalimentare nella riflessione dottrinale angloamericana

ANADOTTI, ELENA; DI GIOVANNI, SILVIA; FREZZA, ANNA CAROLINA; HOSSU, LORENA PATRICIA; MARCONATO, ELENA; NOSCHESE, ANGELA; PENDENZA, ALICE; PEPE, FRANCESCO; PIEROBON, VALERIA; POLI, ELISA; PURITA, CLAUDIA; RAFFA, DJAMILA; ROTONDI, SERGIO ANDREA; SANTOLIN, GAIA – a cura di IZZO, UMBERTO; FERRARI, MATTEO (2021), Aggiornamenti di diritto agroalimentare nella riflessione dottrinale angloamericana, Trento

Law and Technology Research Group, Student Paper Series; 70. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-958-1

STUDENT PAPER N. 69

Diritto del turismo e Covid-19: cosa è cambiato nella seconda estate pandemica

ANGIARI, YOUSSEF; ARZARELLO, ANDREA; AZILI, FEDERICO; BONOMELLI, CHIARA; BUBBOLA, IRENE; CADAMURO, CLAUDIA; CARRETTA, ANNA; CONDOTTA, ALESSANDRO; DA PRATO, MARIKA; DAL TOSO, VIRGINIA; DE AGOSTINI, FILIPPO; DE FRANCESCHI, SERENA; DELL'EVA, MARTINA; DELMARCO, MARTINA; DELLA MURA, MARCO; DI MASCIO, FRANCESCA; FIUTEM, LORENZO; GENNARA, GIULIA; INNOCENTI, ALBERTO; LORIERI, ANNA; MAFFEI, BEATRICE; MARCOLINI, ALESSIA; MANZO, ARIANNA; MINERVINI, MONICA MARIA; MURESAN, ANAMARIA ELENA; NARDIN, NICOLÒ; PAISSAN, FILIPPO; PAISSAN, INGMAR; PANERO, MARTINA; PAVALEANU, CRISTIAN; RIZ, FRANCESCA; SCARSELLA, ALESSIA; SCODANIBBIO, GIULIA; SORRENTINO, MARIAROSA; TUCCI, GIULIANA; VIGNOLI, MARTINA; ZACCARIN, STEPHANIE; ZUCAL, SARA; IZZO, UMBERTO (a cura di) (2021), Diritto del turismo e Covid-19: cosa è cambiato nella seconda estate pandemica, Trento Law and Technology Research Group, Student Paper Series; 69. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-954-3

STUDENT PAPER N. 68

La protezione dei dati relativi alla salute nell'era dei Big Data. Un'analisi sulla sanità digitale in dialogo tra diritto e tecnologia

LIEVORE ANNA (2021), La protezione dei dati relativi alla salute nell'era dei Big Data. Un'analisi sulla sanità digitale in dialogo tra diritto e tecnologia, Trento Law and Technology Research Group, Student Paper Series; 68. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-903-1

STUDENT PAPER N. 67

«Cuius commoda, eius et incommoda»: l'art. 2049 del codice civile nella gig economy

PILZER LARA (2021), «Cuius commoda, eius et incommoda»: l'art. 2049 del codice civile nella gig economy, Trento Law and Technology Research Group, Student Paper Series; 67. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-946-8

STUDENT PAPER N. 66

La responsabilità sanitaria nel post Covid-19: scenari e proposte per affrontare il contenzioso

PRIMICERI GIORGIA (2021), La responsabilità sanitaria nel post Covid-19: scenari e proposte per affrontare il contenzioso, Trento Law and Technology Research Group, Student Paper Series; 66. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-945-1

STUDENT PAPER N. 65

Legal design e sanità digitale: un innovativo approccio per favorire la tutela dei dati personali

FRANCESCO TRAVERSO (2021), Legal design e sanità digitale: un innovativo approccio per favorire la tutela dei dati personali, Trento Law and Technology Research Group, Student Paper Series; 65. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-943-7

STUDENT PAPER N. 64

Sistemi decisionali automatizzati e tutela dei diritti: tra carenza di trasparenza ed esigenze di bilanciamento

IRENE TERENGHI (2021), Sistemi decisionali automatizzati e tutela dei diritti: tra carenza di trasparenza ed esigenze di bilanciamento, Trento Law and Technology Research Group. Student Paper Series; 64. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-942-0

STUDENT PAPER N. 63

Il disegno industriale e la moda tra disciplina dei disegni e modelli e normativa sul diritto d'autore

RUDIAN, MARGHERITA (2021), Il disegno industriale e la moda tra disciplina dei disegni e modelli e normativa sul diritto d'autore, Trento Law and Technology Research Group. Student Paper Series; 63. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-941-3

STUDENT PAPER N. 62

L'appropriazionismo artistico nell'arte visual: una comparazione tra Italia e Stati Uniti

DI NICOLA, LAURA (2021), L'appropriazionismo artistico nell'arte visual: una comparazione tra Italia e Stati Uniti, Trento Law and Technology Research Group. Student Paper Series; 62. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-940-6

STUDENT PAPER N. 61

Unfair trading practices in the business-to-business food supply chain between public and private regulation

BORGHETTO, MARIA VITTORIA (2020), Unfair trading practices in the business-to-business food supply chain between public and private regulation, Trento Law and Technology Research Group. Student Paper Series; 61. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-933-8

STUDENT PAPER N. 60

PFAS e inquinamento delle falde acquifere venete: la tutela civilistica fra danno ambientale e azioni risarcitorie collettive

RAISA, VERONICA (2020), PFAS e inquinamento delle falde acquifere venete: la tutela civilistica fra danno ambientale e azioni risarcitorie collettive, Trento Law and Technology Research Group. Student Paper Series; 60. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-927-7

STUDENT PAPER N. 59

Il turismo alla prova del covid-19: una ricerca interdisciplinare: da quali dati partire e quali risposte dare alla più grande crisi che il comparto turistico abbia mai affrontato

UMBERTO IZZO (a cura di), Autori: ANDREATTA, GIULIA; ANDREOLI, ELISA; ARDU, SIMONE; BORTOLOTTO, FABIO; BRUZZO, PIERLUIGI; CALZOLARI, GIULIA; CAMPOS SANTOS, DIEGO; CARLINO, PIETRO; CAVALLERA, LORENZO; CEPPAROTTI, GIACOMO; CIABRELLI, ANTONIA; DALLE PALLE, GIORGIA; DAPRÀ, VALENTINA; DE SANTIS, DIEGO; FAVARO, SILVIA; FAVERO, ELEONORA; FERRARI, LAURA; GATTI, VERONICA; GAZZI, CHRISTIAN; GISMONDO, MARIANNA; GIUDICEANDREA, ANNA; GUIDA, GIOVANNI; INCARNATO, ANDREA; MARANER, ROBERTA; MICHELI, MARTA; ELENA MORARASU, LAURA; CHIARA NARDELLI, MARIA; PALLOTTA, EMANUELE; PANICHI, NICCOLÒ; PELLIZZARI, LAURA; PLAKSII, ANDRII; RANIERO, SAMANTHA; REGNO SIMONCINI, EMANUELE; RUSSO, SARA; SCHIAVONE, SARA; SERAFINO, ANTONIO; SILENZI, LUCA; TIRONZELLI, ELENA; PEGGY TSAFACK, CYNTHIA; VIGLIOTTI, AYLA; ZINETTI, GIULIA, Il turismo alla prova del Covid-19: una ricerca interdisciplinare: da quali dati partire e quali risposte dare alla più grande crisi che il comparto turistico abbia mai affrontato, Trento Law and Technology Research Group, Student Paper Series; 59. Trento: Università degli Studi di Trento. 978-88-8443-903-1

STUDENT PAPER N. 58

La responsabilità dell'internet service provider alla luce della nuova direttiva sul diritto d'autore nel mercato unico digitale

CAMARELLA, LAURA (2020), La responsabilità dell'Internet Service Provider alla luce della nuova direttiva sul diritto d'autore nel mercato unico digitale, Student Paper Series; 58. Trento: Università degli Studi di Trento. 978-88-8443-893-5

STUDENT PAPER N. 57

Rischio idrogeologico e responsabilità civile

ROBERTI, CATERINA (2020), Rischio idrogeologico e responsabilità civile, Trento Law and Technology Research Group. Student Paper Series; 57. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-891-1

STUDENT PAPER N. 56

Assistente vocale e dati sanitari. Le sfide dell'intelligenza artificiale alla luce del Regolamento (UE) n. 2016/679

PETRUCCI, LIVIA (2020), Assistente vocale e dati sanitari. Le sfide dell'intelligenza artificiale alla luce del regolamento (UE) N. 2016/679, Trento Law and Technology Research Group. Student Paper Series; 56. Trento: Università degli Studi di Trento. ISBN: 978 88 8443 888 1

STUDENT PAPER N. 55

The Legal Dimension of Energy Security in EU Law

SCHMIEDHOFER, ANDREAS (2020), The legal dimensions of energy security in EU law, Trento Law and Technology Research Group. Student Paper Series; 55. Trento: Università degli Studi di Trento. ISBN: 978 88 8443 888 1

STUDENT PAPER N. 54

Macchine intelligenti che creano ed inventano. Profili e rilievi critici del nuovo rapporto tra intelligenza artificiale e diritti di proprietà intellettuale

TREVISANELLO, LAURA (2020), Macchine intelligenti che creano ed inventano. Profili e rilievi critici del nuovo rapporto tra intelligenza artificiale e diritti di proprietà intellettuale, Trento Law and Technology Research Group. Student Paper Series; 54. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-887-4

STUDENT PAPER N. 53

La protezione delle indicazioni geografiche: il sistema europeo e il sistema cinese a confronto

COGO, MARTA (2019), La protezione delle indicazioni geografiche: il sistema europeo e il sistema cinese a confront, Trento Law and Technology Research Group. Student Paper Series; 53. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-856-0

STUDENT PAPER N. 52

Responsabilità civile e prevenzione dell'abuso interpersonale, fra molestie sessuali e bullismo

PERETTI, FRANCESCA (2019), Responsabilità civile e prevenzione dell'abuso interpersonale, fra molestie sessuali e bullismo, Trento Law and Technology Research Group. Student Paper Series; 52. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-856-0

STUDENT PAPER N. 51

Blockchain, Smart Contract e diritto d'autore nel campo della musica

FAGLIA, FRANCESCO (2019), Blockchain, Smart Contract e diritto d'autore nel campo della musica, Trento Law and Technology Research Group. Student Paper Series; 51. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-855-3

STUDENT PAPER N. 50

Regole per l'innovazione: responsabilità civile e assicurazione di fronte all'auto a guida (progressivamente) autonoma

ZEMIGNANI, FILIPPO (2019), Regole per l'innovazione: responsabilità civile e assicurazione di fronte all'auto a guida (progressivamente) autonoma, Trento Law and

Technology Research Group. Student Paper Series; 50. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-850-8

STUDENT PAPER N. 49

Unravelling the nexus between food systems and climate change: a legal analysis. A Plea for smart agriculture, a "new" organic agriculture and a wiser use of biotechnologies in the name of human rights protection

TELCH, ALESSANDRA (2019), Unravelling the nexus between food systems and climate change: a legal analysis. A Plea for smart agriculture, a "new" organic agriculture and a wiser use of biotechnologies in the name of human rights protection, Trento Law and Technology Research Group. Student Paper Series; 49. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-842-3

STUDENT PAPER N. 48

Wireless community networks e responsabilità extracontrattuale

VIDORNI, CHIARA (2019), Wireless community networks e responsabilità extracontrattuale, Trento Law and Technology Research Group. Student Paper Series; 48. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-841-6

STUDENT PAPER N. 47

Proprietà intellettuale e scienza aperta: il caso studio del Montreal Neurological Institute

CASSIN, GIOVANNA (2019), Proprietà intellettuale e scienza aperta: il caso studio del Montreal Neurological Institute, Trento Law and Technology Research Group. Student Paper Series; 47. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-835-5

STUDENT PAPER N. 46

Il "ciclista previdente" che si scontrò due volte: con un'auto e col principio indennitario applicato all'assicurazione infortuni

CHRISTOPH SIMON THUN HOHENSTEIN WELSPERG (2019), Il "ciclista previdente" che si scontrò due volte: con un'auto e col principio indennitario applicato all'assicurazione infortuni, Trento Law and Technology Research Group. Student Paper Series; 46. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-834 8

STUDENT PAPER N. 45

«Errare humanum est». L'errore nel diritto tra intenzionalità, razionalità ed emozioni

BENSALAH, LEILA (2018), «Errare humanum est». L'errore nel diritto tra intenzionalità, razionalità ed emozioni, Trento Law and Technology Research Group. Student Paper Series; 45. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-829-4

STUDENT PAPER N. 44

La gestione del rischio fitosanitario nel diritto agroalimentare europeo ed italiano: il caso Xylella

DE NOBILI, MARINA (2018), La gestione del rischio fitosanitario nel diritto agroalimentare europeo ed italiano: il caso Xylella, Trento Law and Technology Research Group. Student Paper Series; 44. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-828-7

STUDENT PAPER N. 43

Mercato agroalimentare e disintermediazione: la dimensione giuridica della filiera corta

ORLANDI, RICCARDO (2018), Mercato agroalimentare e disintermediazione: la dimensione giuridica della filiera corta, Trento Law and Technology Research Group. Student Paper Series; 43. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-827-0

STUDENT PAPER N. 42

Causa, meritevolezza degli interessi ed equilibrio contrattuale

PULEJO, CARLO ALBERTO (2018), Causa, meritevolezza degli interessi ed equilibrio contrattuale, Trento Law and Technology Research Group. Student Paper Series; 42. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-810-2

STUDENT PAPER N. 41

Graffiti, street art e diritto d'autore: un'analisi comparata

GIORDANI, LORENZA (2018), Graffiti, street art e diritto d'autore: un'analisi comparata, Trento Law and Technology Research Group. Student Paper Series; 41. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-809-6

STUDENT PAPER N. 40

Volo da diporto o sportivo e responsabilità civile per l'esercizio di attività pericolose

MAESTRINI, MATTIA (2018), Volo da diporto o sportivo e responsabilità civile per l'esercizio di attività pericolose, Trento Law and Technology Research Group. Student Paper Series; 40. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-784-6

STUDENT PAPER N. 39

"Attorno al cibo". Profili giuridici e sfide tecnologiche dello Smart Packaging in campo alimentare

BORDETTO, MATTEO (2018), "Attorno al cibo". Profili giuridici e sfide tecnologiche dello Smart Packaging in campo alimentare, Trento Law and Technology Research Group.

Student Paper Series; 39. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-795-2

STUDENT PAPER N. 38

Kitesurf e responsabilità civile

RUGGIERO, MARIA (2018), Kitesurf e responsabilità civile, Trento Law and Technology Research Group. Student Paper Series; 38. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-793-8

STUDENT PAPER N. 37

Giudicare e rispondere. La responsabilità civile per l'esercizio della giurisdizione in Italia, Israele e Spagna

MENEGHETTI HISKENS, SARA (2017), Giudicare e rispondere. La responsabilità civile per l'esercizio della giurisdizione in Italia, Israele e Spagna, Trento Law and Technology Research Group. Student Paper Series; 37. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-778-5

STUDENT PAPER N. 36

Il diritto in immersione: regole di sicurezza e responsabilità civile nella subacquea

CAPUZZO, MARTINA (2017), Il diritto in immersione: regole di sicurezza e responsabilità civile nella subacquea, Trento Law and Technology Research Group. Student Paper Series; 36. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-775-4

STUDENT PAPER N. 35

La privacy by design: un'analisi comparata nell'era digitale

BINCOLETTO, GIORGIA (2017), La privacy by design: un'analisi comparata nell'era digitale, Trento Law and Technology Research Group. Student Paper Series; 35. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-733-4

STUDENT PAPER N. 34

La dimensione giuridica del Terroir

BERTINATO, MATTEO (2017), La dimensione giuridica del Terroir, Trento Law and Technology Research Group. Student Paper Series; 34. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-728-0

STUDENT PAPER N. 33

La gravità del fatto nella commisurazione del danno non patrimoniale: un'indagine (anche) nella giurisprudenza di merito

MARISELLI, DAVIDE (2017), La gravità del fatto nella commisurazione del danno non patrimoniale: un'indagine (anche) nella giurisprudenza di merito, Trento Law and Technology Research Group. Student Paper Series; 33. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-727-3

STUDENT PAPER N. 32

«Edible insects». L'Entomofagia nel quadro delle nuove regole europee sui novel foods

TASINI, FEDERICO (2016), «Edible insects». L'Entomofagia nel quadro delle nuove regole europee sui novel foods = «Edible Insects»: Entomophagy in light of the new European Legislation on novel Foods, Trento Law and Technology Research Group. Student Paper Series; 32. Trento: Università degli Studi di Trento. ISBN 978-88-8443-709-9

STUDENT PAPER N. 31

L'insegnamento dello sci: responsabilità civile e assicurazione per danni ad allievi o a terzi

TAUFER FRANCESCO (2016), L'insegnamento dello sci: responsabilità civile e assicurazione per danni ad allievi o a terzi, Trento Law and Technology Research Group. Student Paper Series; 31. Trento: Università degli Studi di Trento. ISBN 978-88-8443-697-9

STUDENT PAPER N. 30

Incrocio tra Contratti e Proprietà Intellettuale nella Innovazione Scientifica e tecnologica: il Modello del Consortium Agreement europeo

MAGGIOLO ANNA (2016), Incrocio tra Contratti e Proprietà Intellettuale nella Innovazione Scientifica e tecnologica: il Modello del Consortium Agreement europeo, Trento Law and Technology Research Group. Student Paper Series; 30. Trento: Università degli Studi di Trento. ISBN 978-88-8443-696-2

STUDENT PAPER N. 29

La neutralità della rete

BIASIN, ELISABETTA (2016) La neutralità della rete, Trento Law and Technology Research Group. Student Paper Series; 29. Trento: Università degli Studi di Trento. ISBN 978-88-8443-693-1

STUDENT PAPER N. 28

Negotiation Bases and Application Perspectives of TTIP with Reference to Food Law

ACERBI, GIOVANNI (2016) Negotiation Bases and Application Perspectives of TTIP with Reference to Food Law. The Trento Law and Technology Research Group. Student Paper Series; 28. Trento: Università degli Studi di Trento. ISBN 978-88-8443-563-7

STUDENT PAPER N. 27

Privacy and Health Data: A Comparative analysis

FOGLIA, CAROLINA (2016) Privacy and Health Data: A Comparative analysis. The Trento Law and Technology Research Group. Student Paper Series; 27. Trento: Università degli Studi di Trento. ISBN 978-88-8443-546-0

STUDENT PAPER N. 26

Big Data: Privacy and Intellectual Property in a Comparative Perspective

SARTORE, FEDERICO (2016) Big Data: Privacy and Intellectual Property in a Comparative Perspective. The Trento Law and Technology Research Group. Student Paper Series; 26. Trento: Università degli Studi di Trento. ISBN 978-88-8443-534-7

STUDENT PAPER N. 25

Leggere (nel)la giurisprudenza: 53 sentenze inedite in tema di responsabilità civile nelle analisi di 53 annotatori in formazione = Reading (in) the caselaw: 53 unpublished judgemnts dealing with civil liability law analyzed with annotations and comments by 53 students during their civil law course

REMO ANDREOLLI, DALILA MACCIONI, ALBERTO MANTOVANI, CHIARA MARCHETTO, MARIASOLE MASCHIO, GIULIA MASSIMO, ALICE MATTEOTTI, MICHELE MAZZETTI, PIERA MIGNEMI, CHIARA MILANESE, GIACOMO MINGARDO, ANNA LAURA MOGETTA, AMEDEO MONTI, SARA MORANDI, BENEDETTA MUNARI, EDOARDO NADALINI, SERENA NANNI, VANIA ODORIZZI, ANTONIA PALOMBELLA, EMANUELE PASTORINO, JULIA PAU, TOMMASO PEDRAZZANI, PATRIZIA PEDRETTI, VERA PERRICONE, BEATRICE PEVARELLO, LARA PIASERE, MARTA PILOTTO, MARCO POLI, ANNA POLITO, CARLO ALBERTO PULEJO, SILVIA RICCAMBONI, ROBERTA RICCHIUTI, LORENZO RICCO, ELEONORA RIGHI, FRANCESCA RIGO, CHIARA ROMANO, ANTONIO ROSSI, ELEONORA ROTOLA, ALESSANDRO RUFFINI, DENISE SACCO, GIULIA SAKEZI, CHIARA SALATI, MATTEO SANTOMAURO, SILVIA SARTORI, ANGELA SETTE, BIANCA STELZER,

GIORGIA TRENTINI, SILVIA TROVATO, GIULIA URBANIS, MARIA CRISTINA URBANO, NICOL VECCARO, VERONICA VILLOTTI, GIULIA VISENTINI, LETIZIA ZAVATTI, ELENA ZUCCHI (2016) Leggere (nel)la giurisprudenza: 53 sentenze inedite in tema di responsabilità civile nelle analisi di 53 annotatori in formazione = Reading (in) the caselaw: 53 unpublished judgemnts dealing with civil liability law analyzed with annotations and comments by 53 students during their civil law course. The Trento Law and Technology Research Group. Student Paper Series; 25. Trento: Università degli Studi di Trento. ISBN 978-88-8443-626-9

STUDENT PAPER N. 24

La digitalizzazione del prodotto difettoso: stampa 3D e responsabilità civile= The Digital Defective Product: 3D Product and Civil Liability

CAERAN, MIRCO (2016) La digitalizzazione del prodotto difettoso: stampa 3D e responsabilità civile = The Digital Defective Product: 3D Product and Civil Liability. The Trento Law and Technology Research Group. Student Paper Series; 24. Trento: Università degli Studi di Trento. ISBN 978-88-8443-663-4

STUDENT PAPER N. 23

La gestione della proprietà intellettuale nelle università australiane = Intellectual Property Management in Australian Universities

CHIARUTTINI, MARIA OTTAVIA (2015) La gestione della proprietà intellettuale nelle università australiane = Intellectual Property Management in Australian Universities. The Trento Law and Technology Research Group. Student Paper Series; 23. Trento: Università degli Studi di Trento. ISBN 978-88-8443-626-9

STUDENT PAPER N. 22

Trasferimento tecnologico e realtà locale: vecchie problematiche e nuove prospettive per una collaborazione tra università, industria e territorio = Technology Transfer and Regional Context: Old Problems and New Perspectives for a Sustainable Co-operation among Universitiy, Entrepreneurship and Local Economy

CALGARO, GIOVANNI (2013) Trasferimento tecnologico e realtà locale: vecchie problematiche e nuove prospettive per una collaborazione tra università, industria e territorio. The Trento Law and Technology Research Group. Student Paper Series; 22. Trento: Università degli Studi di Trento. ISBN 978-88-8443-525-5

STUDENT PAPER N. 21

La responsabilità dell'Internet Service Provider per violazione del diritto d'autore: un'analisi comparata = Internet Service Provider liability and copyright infringement: a comparative analysis.

IMPERADORI, ROSSELLA (2014) *La responsabilità dell'Internet Service Provider per violazione del diritto d'autore: un'analisi comparata.* Trento Law and Technology Research Group. Student Paper; 21. Trento: Università degli Studi di Trento. ISBN 978-88-8443-572-9

STUDENT PAPER N. 20

Open innovation e patent: un'analisi comparata = Open innovation and patent: a comparative analysis

PONTI, STEFANIA (2014) *Open innovation e patent: un'analisi comparata.* The Trento Law and Technology Research Group. Student Paper Series; 20. Trento: Università degli Studi di Trento. ISBN 978-88-8443-573-6

STUDENT PAPER N. 19

La responsabilità civile nell'attività sciistica

CAPPA, MARISA (2014) La responsabilità civile nell'attività sciistica = Ski accidents and civil liability. Trento Law and Technology Research Group. Student Paper Series, 19. Trento: Università degli Studi di Trento.

STUDENT PAPER N. 18

Biodiversità agricola e tutela degli agricoltori dall'Hold-Up brevettuale: il caso degli OGM

TEBANO, GIANLUIGI (2014) Biodiversità agricola e tutela degli agricoltori dall'Hold-Up brevettuale: il caso degli OGM = Agricultural Biodiversity and the Protection of Farmers from patent Hold-Up: the case of GMOs. Trento Law and Technology Research Group. Student Paper Series; 18. Trento: Università degli Studi di Trento.

STUDENT PAPER N. 17

Produrre e nutrirsi "bio": analisi comparata del diritto degli alimenti biologici

MAFFEI, STEPHANIE (2013) Produrre e nutrirsi "bio" : analisi comparata del diritto degli alimenti biologici = Producing and Eating "Bio": A Comparative Analisys of the Law of Organic Food. Trento Law and Technology Research Group. Student Paper Series; 17. Trento: Università degli Studi di Trento.

STUDENT PAPER N. 16

La tutela delle indicazioni geografiche nel settore vitivinicolo: un'analisi comparata = The Protection of Geographical Indications in the Wine Sector: A Comparative Analisys

SIMONI, CHIARA (2013) La tutela delle indicazioni geografiche nel settore vitivinicolo: un'analisi comparata. The Trento Law and Technology Research Group. Student Papers Series; 16. Trento: Università degli Studi di Trento. Facoltà di Giurisprudenza.

STUDENT PAPER N. 15

Regole di sicurezza e responsabilità civile nelle attività di mountain biking e downhill montano

SALVADORI, IVAN (2013) Regole di sicurezza e responsabilità civile nelle attività di mountain biking e downhill montano. Trento Law and Technology Research Group. Student Paper; 15. Trento: Università degli Studi di Trento.

STUDENT PAPER N. 14

Plagio, proprietà intellettuale e musica: un'analisi interdisciplinare

VIZZIELLO, VIVIANA (2013) Plagio, proprietà intellettuale e musica: un'analisi interdisciplinare. Trento Law and Technology Research Group. Student Paper; 14. Trento: Università degli Studi di Trento.

STUDENT PAPER N.13

The Intellectual Property and Open Source Approaches to Biological Material

CARVALHO, ALEXANDRA (2013) The Intellectual Property and Open Source Approaches to Biological Material. Trento Law and Technology Research Group. Student Paper Series; 13. Trento: Università degli Studi di Trento.

STUDENT PAPER N.12

Per un'archeologia del diritto alimentare: 54 anni di repertori giurisprudenziali sulla sicurezza e qualità del cibo (1876-1930)

TRESTINI, SILVIA (2012) Per un'archeologia del diritto alimentare: 54 anni di repertori giurisprudenziali sulla sicurezza e qualità del cibo (1876-1930) = For an Archeology of Food Law: 54 Years of Case Law Collections Concerning the Safety and Quality of Food (1876-1930). The Trento Law and Technology Research Group. Student Papers Series, 12.

STUDENT PAPER N.11

Dalle Alpi ai Pirenei: analisi comparata della responsabilità civile per attività turistico-ricreative legate alla montagna nel diritto italiano e spagnolo

PICCIN, CHIARA (2012) Dalle Alpi ai Pirenei: analisi comparata della responsabilità civile per attività turistico-ricreative legate alla montagna nel diritto italiano e spagnolo = From the Alps to the Pyrenees: Comparative Analysis of Civil Liability for Mountain Sport Activities in Italian and Spanish Law. The Trento Law and Technology Research Group. Student Papers Series, 11.

STUDENT PAPER N.10

Copynorms: Norme Sociali e Diritto d'Autore

PERRI, THOMAS (2012) Copynorms: Norme Sociali e Diritto d'Autore = Copynorms: Social Norms and Copyright. Trento Law and Technology Research Group. Students Paper Series, 10.

STUDENT PAPER N. 9

L'export vitivinicolo negli Stati Uniti: regole di settore e prassi contrattuali con particolare riferimento al caso del Prosecco

ALESSANDRA ZUCCATO (2012), L'export vitivinicolo negli Stati Uniti: regole di settore e prassi contrattuali con particolare riferimento al caso del Prosecco = Exporting Wines to the United States: Rules and Contractual Practices with Specific Reference to the Case of Prosecco. Trento: Università degli Studi di Trento (Trento Law and Technology Research Group. Students Paper Series 9)

STUDENT PAPER N.8

Equo compenso e diritto d'autore: un'analisi comparata = Fair Compensation and Author's Rights: a Comparative Analysis.

RUGGERO, BROGI (2011) Equo compenso e diritto d'autore: un'analisi comparata = Fair Compensation and Author's Rights: a Comparative Analysis. Trento: Università degli Studi di Trento (TrentoLawand Technology Research Group. Student Papers Series, 8)

STUDENT PAPER N.7

Evoluzione tecnologica e mutamento del concetto di plagio nella musica

TREVISAN, ANDREA (2012) Evoluzione tecnologica e mutamento del concetto di plagio nella musica = Technological evolution and change of the notion of plagiarism in music Trento: Università degli Studi di Trento (Trento Law and Technology Research Group. Students Paper Series 7)

STUDENT PAPER N.6

Il trasferimento tecnologico università-imprese: profili giuridici ed economici

SIRAGNA, SARA (2011) Il trasferimento tecnologico università-imprese: profili giuridici ed economici = University-Enterprises Technological Transfer: Legal and Economic issues Trento: Università degli Studi di Trento (Trento Law and Technology Research Group. Students Paper Series 6)

STUDENT PAPER N.5

Conciliare la responsabilità medica: il modello "generalista" italiano a confronto col modello "specializzato" francese

GUERRINI, SUSANNA (2011) Conciliare la responsabilità medica: il modello "generalista" italiano a confronto col modello "specializzato" francese = Mediation & Medical Liability: The Italian "General Approach" Compared to the Specialized Model Applied in France. Trento: Università degli Studi di Trento (Trento Law and Technology Research Group. Students Paper Series 5)

STUDENT PAPER N.4

"Gun Control" e Responsabilità Civile: una comparazione fra Stati Uniti e Italia

PODETTI, MASSIMILIANO (2011) "Gun Control" e Responsabilità Civile: una comparazione fra Stati Uniti e Italia = Gun Control and Tort Liability: A Comparison

between the U.S. and Italy Trento: Università degli Studi di Trento. (Trento Law and Technology Research Group. Students Paper Series 4)

STUDENT PAPER N.3

Smart Foods e Integratori Alimentari: Profili di Regolamentazione e Responsabilità in una comparazione tra Europa e Stati Uniti

TOGNI, ENRICO (2011) Smart Foods e Integratori Alimentari: Profili di Regolamentazione e Responsabilità in una comparazione tra Europa e Stati Uniti = Smart Foods and Dietary Supplements: Regulatory and Civil Liability Issues in a Comparison between Europe and United States Trento: Università degli Studi di Trento - (Trento Law and Technology Research Group. Students Paper Series; 3)

STUDENT PAPER N.2

Il ruolo della responsabilità civile nella famiglia: una comparazione tra Italia e Francia

SARTOR, MARTA (2010) Il ruolo della responsabilità civile nella famiglia: una comparazione tra Italia e Francia = The Role of Tort Law within the Family: A Comparison between Italy and France Trento: Università degli Studi di Trento - (Trento Law and Technology Research Group. Students Paper Series; 2)

STUDENT PAPER N.1

Tecnologie belliche e danno al proprio combattente: il ruolo della responsabilità civile in una comparazione fra il caso statunitense dell'Agent Orange e il caso italiano dell'uranio impoverito

RIZZETTO, FEDERICO (2010) Tecnologie belliche e danno al proprio combattente: il ruolo della responsabilità civile in una comparazione fra il caso statunitense dell'Agent Orange e il caso italiano dell'uranio impoverito = War Technologies and Home Soldiers Injuries: The Role of Tort Law in a Comparison between the American "Agent Orange" and the Italian "Depleted Uranium" Litigations Trento: Università degli Studi di Trento - (Trento Law and Technology Research Group. Students Paper Series; 1)