



UNIVERSITY
OF TRENTO
Faculty of
Law

**Trento Law and Technology
Research Group
Student Paper n. 90**

**LA DIDATTICA DEL CAPITALISMO
DELLA SORVEGLIANZA: PROFILI
GIURIDICI**

ALICE CATALANO

lawtech

COPYRIGHT © 2023 ALICE CATALANO

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 © 2023 ALICE CATALANO

è pubblicato con Licenza Creative Commons - Attribution - Share Alike 4.0
International. Maggiori informazioni circa la licenza all'URL:

<https://creativecommons.org/licenses/by-sa/4.0/>

About the author

Alice Catalano (catalano.alice14@gmail.com) graduated in Law at University of Trento under the supervision of Prof. Roberto Caso (September 2023).

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

KEY WORDS

*Capitalismo –Sorveglianza–Didattica –
Privacy – Comparazione*

Sull'autrice

Alice Catalano (catalano.alice14@gmail.com) ha conseguito la Laurea in Giurisprudenza presso l'Università di Trento con la supervisione del Prof. Roberto Caso (Settembre 2023).

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

PAROLE CHIAVE

*Capitalismo –Sorveglianza–Didattica –
Privacy – Comparazione*

SURVEILLANCE CAPITALISM EDUCATION: A LEGAL POINT OF VIEW

Abstract

With the declaration of the Covid-19 pandemic by the World Health Organization in March 2020, educational institutions worldwide abandoned physical school and universities spaces for the purpose of virus containment, transitioning to a different model of education known as “distance learning” or “Emergency Remote Teaching”. In order to carry out educational activities, these institutions, both in Italy and beyond, turned to the so-called “proprietary platforms”, which are infrastructure services owned by large companies in the digital market. This thesis carries out a careful analysis of the critical issues related to the possibility that the characteristics of “surveillance capitalism”, brilliantly elucidated by the American academic and sociologist Shoshana Zuboff, may also engulf the realm of education, posing risks to academic freedom, scientific research, and the protection of personal data.

The first chapter analyzes the birth and development of surveillance capitalism. The evolution of this new economic model begins with Google's discovery of the “behavioral surplus”, which becomes a crucial raw material whose “extraction” plays a central role in the activities of digital-era operators. Through the insightful analysis of Zuboff, Pagano, Rikiap, Wu, Khan, and Florio, the chapter will demonstrate how surveillance capitalism has contributed to the emergence of intellectual monopolies and “data-driven intellectual monopoly”, illustrating how even companies operating outside Silicon Valley have recognized the potential of the “behavioral surplus.” The birth of the “data-driven economy” brings with it a series of issues, such as the commodification of individuals, user manipulation, often victimizing consumers through unfair commercial practices, as well as risks to individual self-determination, with serious consequences for democracy. Finally, as surveillance capitalism's activities raise numerous issues regarding the protection of personal data, we will reconstruct the framework for privacy protection, starting from the right to privacy and delving into key concepts of the General Data Protection Regulation (GDPR).

In the second chapter, it will be described how the oligopolistic and monopolistic operators of surveillance capitalism have extended their influence “outside of Silicon Valley” into the field of research and education. Firstly, the chapter will examine how major platforms and scientific publishers have gained a predominant role within university research by seizing control of infrastructure and overseeing the entire research workflow, resulting in a situation of lock-in for much of the research world. It will then discuss the phenomenon of “surveillance publishing” described by Jeff Pooley and the possibility that major publishers can invisibly and strategically influence key decisions in academia. By presenting empirical data, it will be suggested the presence of undue interference by surveillance capitalists in the activities of major publishers. This part will also analyze the phenomenon of Emergency Remote Teaching, “platform education”, and “e-proctoring”, highlighting how Italian educational institutions and most universities have relied on surveillance capitalists' platforms for distance education. In addition to the risks described in the first chapter, there are numerous

issues related to the sharing of specific categories of student and minor data, with the potential development of student performance monitoring systems and of a global educational monoculture dictated by proprietary platforms. The thesis will also explore some alternatives, which were already available during the pandemic, such as the Italian open-source platform GARR and the French choice to implement a government portal for educational purposes. Furthermore, it will introduce two European-level measures: the European open-source infrastructure GAIA-X, not originally designed for educational purposes but potentially useful for education, and the European education space, which encompasses the digital education action plan for 2021-2027.

The third chapter will conduct an examination of the problematic aspects of distance learning in relation to the GDPR. This will be followed by a partial analysis of some privacy policies of the most used platforms during the Emergency Remote Teaching experience. First, the analysis will cover the privacy policy formulated during the implementation of distance learning in March 2020, then they will be compared with current privacy policies. Many of the issues that will arise also relate to the phenomenon of e-proctoring, so we will analyze the decision of the Italian Data Protection Authority to sanction a well-known Milanese university for the use of such software, examining how the Italian Authority's observations have not always been shared by European counterparts. Since the phenomenon of distance learning has largely impacted children and minors, the thesis will propose a greater application of the "privacy by design" principle and the mandatory assessment of the impact on the protection of personal data when handling the personal data of minors. Finally, the chapter will look at a new challenge shared by the education sector and the GDPR: artificial intelligence, particularly the Chatbot ChatGPT, whose use in education is highly controversial.

In the fourth chapter, it will be hypothesized the joint use of antitrust legislation and the GDPR to erode the monopolies and oligopolies that surveillance capitalists have built in digital markets through their data extraction activities. These two regulatory frameworks are considered suitable for protecting the vulnerable condition of student-users, understood as a combination of consumers and data subjects. The chapter will also examine the judicial and non-judicial developments that recognize the value of Big Data as market assets. Finally, it will be analyzed the European data strategy, especially the Digital Markets Act, a regulation aimed at reconciling antitrust and personal data protection. Subsequently, it will briefly introduce the Digital Services Act, the Data Governance Act, and the Data Act proposal. While none of these legislative acts specifically targets the education sector, the final chapter will consider their potential application in efforts to counter the practices of surveillance capitalism in the provision of distance education.

LA DIDATTICA DEL CAPITALISMO DELLA SORVEGLIANZA: PROFILI GIURIDICI

Abstract

Con la dichiarazione da parte dell'Organizzazione Mondiale della Sanità della pandemia da Covid-19 nel marzo 2020, gli istituti scolastici e universitari di quasi tutto il globo hanno abbandonato gli spazi fisici della scuola e dell'Università per finalità di contenimento del virus, passando a un diverso modello di didattica denominato «didattica a distanza» o «Emergency Remote Teaching». Ai fini dello svolgimento delle attività didattiche gli istituti scolastici e quasi tutte le Università italiane – e non solo – hanno fatto ricorso alle cosiddette «piattaforme proprietarie», ovvero servizi di infrastruttura proprietà di grandi imprese nel mercato digitale. Nella presente tesi si è scelto di procedere ad un'attenta analisi delle criticità legate alla possibilità che le logiche del «*capitalismo della sorveglianza*», brillantemente illustrate dall'accademica e sociologa statunitense Shoshana Zuboff, possano inglobare anche il mondo dell'istruzione, cagionando rischi per la libertà di insegnamento e ricerca scientifica e per la tutela dei dati personali.

Nel primo capitolo si analizzerà la nascita e lo sviluppo del capitalismo della sorveglianza. L'evoluzione di questo nuovo modello economico è raccontata a partire dalla scoperta, da parte di Google, del «*surplus comportamentale*», che diviene un'importante materia prima la cui «estrazione» ha un ruolo centrale per l'attività degli operatori dell'era digitale. Grazie alla sapiente analisi di Zuboff, Pagano, Rikiap, Wu, Khan e Florio, si dimostrerà come il capitalismo della sorveglianza abbia contribuito alla nascita di monopoli intellettuali e «*data-driven intellectual monopoly*», illustrando come ormai anche imprese operanti fuori dalla Silicon Valley abbiano compreso le potenzialità del «*surplus comportamentale*». La nascita della «*data-driven economy*» porta con sé una serie di criticità, come la mercificazione della persona e la manipolazione degli utenti, spesso vittime, in quanto consumatori, di pratiche commerciali scorrette, nonché rischi per la capacità di autodeterminazione dell'individuo, con gravi conseguenze per la democrazia. Infine, dal momento che l'attività del capitalismo della sorveglianza solleva numerosi problemi in materia di tutela dei dati personali, si procederà alla ricostruzione della tutela della privacy, a partire dalla tutela del diritto alla riservatezza fino alla descrizione dei concetti chiave del General Data Protection Regulation (GDPR).

Nel secondo capitolo si descriverà come gli operatori oligopolistici e monopolistici del capitalismo della sorveglianza abbiano ormai compiuto un ulteriore «passo fuori dalla Silicon Valley» nel mondo della ricerca e dell'istruzione. *In primis* si guarderà come le grandi piattaforme e i grandi editori scientifici abbiano ottenuto un ruolo predominante all'interno della ricerca universitaria impadronendosi dell'infrastruttura e controllando l'intero *workflow* dell'attività di ricerca, cagionando una situazione di *lock-in* per gran parte del mondo della ricerca. Si illustrerà poi il fenomeno di «*surveillance publishing*» descritto da Jeff Pooley e la possibilità che i grandi editori influenzino invisibilmente e strategicamente le decisioni chiave dell'Università. Riportando alcuni dati empirici, si ipotizzerà la presenza di indebite ingerenze dei capitalisti della sorveglianza nelle attività dei grandi editori. Si analizzerà poi il fenomeno dell'Emergency Remote Teaching, dell'«*istruzione delle piattaforme*» e dell'«e-

proctoring», rilevando come, complici atteggiamenti deferenti dell’Autorità Garante dei dati personali e del Governo, gli istituti scolastici e la quasi totalità degli istituti universitari italiani abbiano fatto affidamento sulle piattaforme dei capitalisti della sorveglianza per lo svolgimento della didattica a distanza. Ai rischi descritti nel primo capitolo, si somma tutta una serie di criticità legate alla condivisione di categorie particolari di dati di studenti e minori, con la possibilità che si sviluppino sistemi di sorveglianza della performance degli studenti e che si sviluppi una monocultura didattica globale dettata dalle piattaforme proprietarie. Si analizzeranno poi alcune alternative, in verità già disponibili al tempo dell’emergenza pandemica, come la piattaforma *open source* del GARR o la scelta della Francia di implementare un portale governativo per finalità didattiche. Si illustreranno poi due misure implementate a livello europeo: l’infrastruttura *open source* europea GAIA-X, non nata per esigenze didattiche ma il cui utilizzo è facilmente ipotizzabile anche per il mondo dell’istruzione, e lo spazio europeo dell’istruzione, all’interno del quale si colloca il piano d’azione per l’istruzione digitale 2021-2027.

Nel terzo capitolo si procederà ad una disamina degli elementi di problematicità della didattica a distanza rispetto al GDPR. Seguirà poi un’analisi parziale di alcune informative privacy, così come formulate durante lo svolgimento della didattica a distanza a marzo del 2020, che verranno poi confrontate con le privacy policy attuali. Alcuni punti critici della didattica a distanza si collegano anche alla possibilità di trasferimento dei dati personali negli Stati Uniti. Pertanto, si illustrerà l’evoluzione normativa e giurisprudenziale in materia. Molti dei problemi che emergeranno riguardano anche il fenomeno di *e-proctoring*, sicché si analizzerà la decisione dell’Autorità Garante per la protezione dei dati personali di sanzionare un celebre ateneo milanese per l’utilizzo di tali software, guardando come tuttavia non sempre le osservazioni del Garante italiano siano state condivise dalle omologhe autorità europee. Dal momento che il fenomeno della didattica a distanza ha riguardato in gran parte bambini e minori, si ipotizzerà una maggiore applicazione del principio di *privacy by design* e l’obbligatorietà della valutazione di impatto sulla protezione dei dati personali in presenza di un trattamento di dati personali di minori. Si guarderà infine a una nuova sfida in comune tra mondo dell’istruzione e GDPR: l’intelligenza artificiale, in particolare il Chatbot ChatGPT, il cui uso nel mondo dell’istruzione è estremamente controverso.

Nel quarto capitolo, infine, si ipotizzerà un utilizzo congiunto di normativa antitrust e GDPR per erodere i monopoli e gli oligopoli che i capitalisti della sorveglianza hanno costruito nei mercati digitali grazie alla loro attività di estrazione di dati personali. Le due normative sono ritenute infatti idonee a tutelare la condizione di vulnerabilità degli utenti-studenti, intesi come *summa* di consumatore e soggetto interessato al trattamento. Si guarderà poi all’evoluzione giurisprudenziale e non in materia, che riconosce il valore dei *Big Data* quali *market asset*. Infine, si analizzerà la strategia europea dei dati, in particolare il Digital Markets Act, Regolamento che ha l’obiettivo di coniugare l’antitrust e la tutela dei dati personali. Successivamente, verranno brevemente illustrati anche il Digital Services Act, il Data Governance Act e la proposta del Data Act. Sebbene nessuno di questi atti normativi sia specificamente indirizzato al mondo dell’istruzione, si ipotizzerà un’eventuale applicazione di questi ultimi

nell'attività di contrasto alle pratiche del capitalismo della sorveglianza nell'erogazione della didattica a distanza.

INDICE

INTRODUZIONE.....	1
I CAPITOLO.....	5
IL CAPITALISMO DELLA SORVEGLIANZA	5
1.1 CONCETTI DI BASE E DIFFICOLTÀ DEFINITORIE	5
1.1.1 L'era digitale e il metodo Law&Technology	5
1.1.2 Big Data	9
1.1.3 Intelligenza artificiale	11
1.1.4 Algoritmo	12
1.2 DAL CAPITALISMO AL "CAPITALISMO DELLA SORVEGLIANZA"	13
1.3 MONOPOLI E OLIGOPOLI.....	17
1.3.1 La monopolizzazione degli utenti	17
1.3.2 «La guerra dell'estrazione»	19
1.3.3 Il capitalismo dei monopoli intellettuali.....	20
1.3.3 Caratteristiche di monopoli e oligopoli: cenni	24
1.4. FUORI DALLA SILICON VALLEY	25
1.4.1 Internet of Things	26
1.4.2 Possibili applicazioni future: il mercato assicurativo	28
1.5 ALCUNE CONSIDERAZIONI CRITICHE	29
1.5.1 Data-driven economy e mercificazione della persona.....	29
1.5.2 Rischi per gli utenti come consumatori: cenni	32
1.5.3 La manipolazione degli utenti	34
1.5.4 I rischi per la democrazia: il caso Cambridge Analytica	35
1.6 LA TUTELA DEI DATI PERSONALI	37
1.6.1 Excursus storico: la privacy negli USA e la riservatezza in Italia.....	38
1.6.2 La tutela dei dati personali: la disciplina europea.....	43
1.6.3 I concetti chiave del GDPR.....	46
1.7. CONSIDERAZIONI DI SINTESI.....	51

II CAPITOLO.....	53
GLI OLIGOPOLI NELLA DIDATTICA DEL CAPITALISMO DELLA SORVEGLIANZA	53
2.1 OPERATORI OLIGOPOLISTICI NEL MONDO DELL'ISTRUZIONE	53
2.2. OLIGOPOLI E UNIVERSITÀ.....	54
2.2.1 L'editoria scientifica.....	54
2.2.2 Il ruolo del capitalismo della sorveglianza nel mondo della ricerca universitaria	58
2.2.3 L'esperimento di Cody Hanson.....	62
2.3 IL MONDO DELL'ISTRUZIONE	63
2.3.1 Emergency remote teaching e capitalismo della sorveglianza	63
2.3.2 Il fenomeno dell'e-proctoring	69
2.4 LE CASE EDITRICI DELLA SORVEGLIANZA E I LIBRI DI TESTO	71
2.5 ALTERNATIVE: INFRASTRUTTURE OPEN SOURCE	71
2.4.1. L'esperienza italiana: GARR e il Politecnico di Torino	72
2.5.2 Il mondo della scuola.....	74
2.5.3 Spunti comparatistici: l'esempio francese	74
2.5.4 Verso una soluzione europea: GAIA-X.....	75
2.6 LO SPAZIO EUROPEO DELL'ISTRUZIONE E IL PIANO D'AZIONE PER L'ISTRUZIONE DIGITALE	79
III CAPITOLO.....	81
IL TRATTAMENTO DEI DATI PERSONALI DELLA DIDATTICA A DISTANZA	81
3.1 GENERAL DATA PROTECTION REGULATION E MONDO DELL'ISTRUZIONE: L'ORDINE DEL RAGIONAMENTO	81
3.2 TITOLARE E RESPONSABILE DEL TRATTAMENTO NELLA DIDATTICA A DISTANZA.....	82
3.3 OSSERVAZIONI SULLE PRIVACY POLICY DELLE PIATTAFORME MAGGIORMENTE DIFFUSE IN AMBITO DI DIDATTICA A DISTANZA	87
3.3.1 La base giuridica e la finalità del trattamento nella didattica a distanza.....	87
3.3.2 Alcune osservazioni critiche sulle privacy policy delle piattaforme della DaD	88

3.3.3 Come le privacy policy delle piattaforme DaD descrivono i diritti dell'interessato previsti del GDPR	90
3.3.4. Analisi delle privacy policy attuali	93
3.4 LA DISCIPLINA DEL TRASFERIMENTO DEI DATI PERSONALI DELLA DIDATTICA AI SENSI DEL GDPR ..	97
3.4.1 Il trasferimento transfrontaliero nella direttiva 95/46/CE e nel GDPR.....	97
3.4.2 Il trasferimento negli Stati Uniti: il Datagate.....	105
3.4.3 La decisione di adeguatezza Safe Harbor e la pronuncia Schrems I	106
3.4.4 La decisione Privacy Shield e Schrems II	110
3.4.5 Il trasferimento verso gli Stati Uniti dopo la pronuncia Schrems II: la decisione di adeguatezza Data Privacy Framework	113
3.4.6 Il trasferimento dei dati personali della didattica a distanza dopo Schrems II	120
3.5. LA COMPATIBILITÀ AL GDPR DEI SOFTWARE DI E-PROCTORING.....	122
3.5.1 La decisione dell'Autorità Garante per la protezione dei dati personali italiana	122
3.5.2 Spunti comparatistici	126
3.6 LA TUTELA DEI DATI PERSONALI DI BAMBINI E MINORI	129
3.7 NUOVE SFIDE PER IL MONDO DELL'ISTRUZIONE	133
3.8 CONSIDERAZIONI DI SINTESI	137
IV CAPITOLO.....	143
POSSIBILI SOLUZIONI: LA DISCIPLINA ANTITRUST E LA STRATEGIA EUROPEA DEI DATI	143
4.1 IL RUOLO DELLA NORMATIVA ANTITRUST E L'ORDINE DEL RAGIONAMENTO	143
4.1.1 Brevi cenni sulla normativa in materia di concorrenza e tutela del consumatore.....	145
4.2 DATA PROTECTION E ANTITRUST: PERCHÉ È NECESSARIO UN APPROCCIO CONGIUNTO	147
4.3 LA TUTELA DELLA VULNERABILITÀ DELL'INDIVIDUO TRA DATA PROTECTION E ANTITRUST.....	150
4.4 L'EVOLUZIONE GIURISPRUDENZIALE IN MATERIA	152
4.4.1 L'evoluzione nel panorama europeo.....	152
4.4.2 Il Bundeskartellamt tedesco contro Facebook.....	154

4.4.3 L'esperienza italiana	157
4.5 IL DIGITAL MARKETS ACT	161
4.5.1 L'ambito di applicazione e alcune criticità	162
4.5.2 Gli obblighi delle piattaforme con gatekeeping power.....	165
4.6 ALTRI INTERVENTI NORMATIVI DELL'UNIONE EUROPEA NELL'AMBITO DELLA STRATEGIA EUROPEA DEI DATI: CENNI	169
4.6.1 Il Digital Services Act.....	170
4.6.2 Il Data Governance Act e la proposta del Data Act	174
4.6.3 Considerazioni di sintesi sulla strategia europea dei dati e le criticità legate alla didattica a distanza	178
CONCLUSIONI	181
BIBLIOGRAFIA	185

INTRODUZIONE

Con la dichiarazione da parte dell'Organizzazione Mondiale della Sanità della pandemia da Covid-19 nel marzo 2020, gli istituti scolastici e universitari di quasi tutto il globo hanno abbandonato gli spazi fisici della scuola e dell'Università per finalità di contenimento del virus, passando a un diverso modello di didattica denominato «didattica a distanza» o «Emergency Remote Teaching». Ai fini dello svolgimento delle attività didattiche gli istituti scolastici e quasi tutte le Università italiane – e non solo – hanno fatto ricorso alle cosiddette «piattaforme proprietarie», ovvero servizi di infrastruttura proprietà di grandi imprese nel mercato digitale.

Nella presente tesi si è scelto di procedere ad un'attenta analisi delle criticità legate alla possibilità che le logiche del «*capitalismo della sorveglianza*», brillantemente illustrate dall'accademica e sociologa statunitense Shoshana Zuboff, possano inglobare anche il mondo dell'istruzione, cagionando rischi per la libertà di insegnamento e ricerca scientifica e per la tutela dei dati personali.

Nel primo capitolo si analizzerà la nascita e lo sviluppo del capitalismo della sorveglianza, non senza prima aver illustrato i concetti alla base del fenomeno - *Big Data, intelligenza artificiale e algoritmo* – attraverso il metodo interdisciplinare *Law & Technology*. L'evoluzione di questo nuovo modello economico è raccontata a partire dalla scoperta, da parte di Google, del «*surplus comportamentale*», che diviene un'importante materia prima la cui «estrazione» ha un ruolo centrale per l'attività degli operatori dell'era digitale. Si descriverà il processo di «monopolizzazione degli utenti» e in che termini gli operatori dei mercati digitali possano ritenersi operatori oligopolistici o monopolistici. Grazie alla sapiente analisi di Zuboff, Pagano, Rikiap, Wu, Khan e Florio, si dimostrerà come il capitalismo della sorveglianza abbia contribuito alla nascita di monopoli intellettuali e «*data-driven intellectual monopoly*», illustrando come ormai anche imprese operanti fuori dalla Silicon Valley, come quelle operanti nel settore assicurativo, abbiano compreso le potenzialità del «*surplus comportamentale*». La nascita della «*data-driven economy*» porta con sé una serie di criticità, come la mercificazione della persona e la manipolazione degli utenti, spesso vittime, in quanto consumatori, di pratiche commerciali scorrette, nonché rischi per la capacità di autodeterminazione dell'individuo, con gravi conseguenze per la democrazia. Infine, dal momento che l'attività del capitalismo della sorveglianza solleva numerosi problemi in materia di tutela dei dati personali, si procederà alla ricostruzione della tutela della privacy, a partire dalla tutela del diritto alla riservatezza fino alla descrizione dei concetti chiave del General Data Protection Regulation (GDPR).

Nel secondo capitolo si descriverà come gli operatori oligopolistici e monopolistici del capitalismo della sorveglianza abbiano ormai compiuto un ulteriore «passo fuori dalla Silicon Valley» nel mondo della ricerca e dell'istruzione. *In primis* si guarderà come le grandi piattaforme e i grandi editori scientifici abbiano ottenuto un ruolo predominante all'interno della ricerca universitaria impadronendosi dell'infrastruttura e controllando l'intero *workflow* dell'attività di ricerca, cagionando una situazione di *lock-in* per gran parte del mondo della ricerca. Si illustrerà poi il fenomeno di «*surveillance publishing*» descritto da Jeff Pooley, analizzando la progressiva

trasformazione dell'attività dei grandi editori da quella di fornitura di contenuti a quella di *data analytics*, con la possibilità che i grandi editori influenzino invisibilmente e strategicamente le decisioni chiave dell'Università. Riportando alcuni dati empirici, si ipotizzerà la presenza di indebite ingerenze dei capitalisti della sorveglianza nelle attività dei grandi editori. Si analizzerà poi il fenomeno dell'Emergency Remote Teaching, dell'«istruzione delle piattaforme» e dell'«e-proctoring», rilevando come, complici atteggiamenti deferenti dell'Autorità Garante dei dati personali e del Governo, gli istituti scolastici e la quasi totalità degli istituti universitari italiani abbiano fatto affidamento sulle piattaforme dei capitalisti della sorveglianza per lo svolgimento della didattica a distanza. Ai rischi descritti nel primo capitolo, si somma tutta una serie di criticità legate alla condivisione di categorie particolari di dati di studenti e minori, con la possibilità che si sviluppino sistemi di sorveglianza della performance degli studenti e che si sviluppi una monocultura didattica globale dettata dalle piattaforme proprietarie. Si analizzeranno poi alcune alternative, in verità già disponibili al tempo dell'emergenza pandemica, come la piattaforma *open source* del GARR o la scelta della Francia di implementare un portale governativo per finalità didattiche. Si illustreranno poi due misure implementate a livello europeo: l'infrastruttura *open source* europea GAIA-X, non nata per esigenze didattiche ma il cui utilizzo è facilmente ipotizzabile anche per il mondo dell'istruzione, e lo spazio europeo dell'istruzione, all'interno del quale si colloca il piano d'azione per l'istruzione digitale 2021-2027.

Nel terzo capitolo si procederà ad una disamina degli elementi di problematicità della didattica a distanza rispetto al GDPR, analizzando i ruoli di titolare e responsabile del trattamento, la base giuridica, la finalità del trattamento e i diritti dell'interessato. Seguirà poi un'analisi parziale di alcune informative privacy, così come formulate durante lo svolgimento della didattica a distanza a marzo del 2020, che verranno poi confrontate con le privacy policy attuali. Alcuni punti critici della didattica a distanza si collegano anche alla possibilità di trasferimento dei dati personali negli Stati Uniti. Pertanto, si illustrerà l'evoluzione normativa e giurisprudenziale in materia, partendo dal *Datagate* fino alle recenti evoluzioni. Molti dei problemi che emergeranno riguardano anche il fenomeno di *e-proctoring*, sicché si analizzerà la decisione dell'Autorità Garante per la protezione dei dati personali di sanzionare un celebre ateneo milanese per l'utilizzo di tali software, guardando come tuttavia non sempre le osservazioni del Garante italiano siano state condivise dalle omologhe autorità europee. Dal momento che il fenomeno della didattica a distanza ha riguardato in gran parte bambini e minori, si ipotizzerà una maggiore applicazione del principio di *privacy by design* e l'obbligatorietà della valutazione di impatto sulla protezione dei dati personali in presenza di un trattamento di dati personali di minori. Si guarderà infine a una nuova sfida in comune tra mondo dell'istruzione e GDPR: l'intelligenza artificiale, in particolare il Chatbot ChatGPT, il cui uso nel mondo dell'istruzione è estremamente controverso.

Nel quarto capitolo, infine, si ipotizzerà un utilizzo congiunto di normativa antitrust e GDPR per erodere i monopoli e gli oligopoli che i capitalisti della sorveglianza hanno costruito nei mercati digitali grazie alla loro attività di estrazione di dati personali. Le due normative sono ritenute infatti idonee a tutelare la condizione di vulnerabilità degli utenti-studenti, intesi come *summa* di consumatore e soggetto interessato al trattamento. Si guarderà poi all'evoluzione giurisprudenziale e non in materia, che

riconosce il valore dei *Big Data* quali *market asset*. Infine, si analizzerà la strategia europea dei dati, in particolare il Digital Markets Act, Regolamento che ha l'obiettivo di coniugare l'antitrust e la tutela dei dati personali. Successivamente, verranno brevemente illustrati anche il Digital Services Act, il Data Governance Act e la proposta del Data Act. Sebbene nessuno di questi atti normativi sia specificamente indirizzato al mondo dell'istruzione, si ipotizzerà un'eventuale applicazione di questi ultimi nell'attività di contrasto alle pratiche del capitalismo della sorveglianza nell'erogazione della didattica a distanza.

I CAPITOLO

IL CAPITALISMO DELLA SORVEGLIANZA

1.1 Concetti di base e difficoltà definitorie

L'obiettivo del presente capitolo è di introdurre e sintetizzare il fenomeno del capitalismo della sorveglianza ideato da Shoshana Zuboff,¹ descrivendo in primo luogo i concetti che sono posti alla sua base: era digitale, *Big Data*, intelligenza artificiale e algoritmi. Se da un lato fornire delle definizioni chiare ed esaustive è certamente fondamentale per una migliore comprensione del fenomeno, in questa sede non si può ignorare la caducità, ed inevitabile obsolescenza, delle definizioni stesse. L'innovazione tecnologica nell'era digitale procede spedita, e il legislatore accumula un ritardo fisiologicamente dovuto alla natura stessa delle democrazie occidentali, in cui il ruolo di legiferare è delegato al Parlamento, ed a tutte le difficoltà che da questa attribuzione derivano. Tutto ciò porta ad una sostanziale impossibilità di reperire delle definizioni normative delle tecnologie fondamentali. Anche quando organismi di ricerca e accademici elaborano una definizione, difficilmente questa incontra un consenso unanime, poiché non sempre questi sono concordi circa la rilevanza di uno o dell'altro elemento caratterizzante il particolare concetto.

Si condivide pertanto la scelta oculata della sociologa e accademica Shoshana Zuboff di descrivere le tecnologie coinvolte con termini quanto più neutri possibili rispetto alle incalzanti novità nell'orizzonte tecnologico, ovvero «*intelligenza delle macchine*».

1.1.1 L'era digitale e il metodo Law&Technology

Nella modernità, la storia delle rivoluzioni industriali è scandita dalla comparsa di nuove *general purpose technologies*, ovvero tecnologie di portata generale. La peculiarità di queste ultime risiede nel fatto che esse non rappresentano un'innovazione in campi tecnologici isolati, ma hanno la capacità di impattare in modo significativo diversi campi dell'economia e dalla vita umana.²

Riferendosi alla Prima rivoluzione industriale (1760-1849), la tecnologia di portata generale determinante fu la macchina a vapore, mentre per la Seconda rivoluzione industriale (1870-1900) determinante fu l'invenzione dell'energia elettrica, l'acqua corrente e il motore a combustione interna.³

¹ S. Zuboff, «Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri», Roma, Luiss University Press, 2019.

² A. Quarta, G. Smorto, «Diritto privato dei mercati digitali», Milano, Mondadori - Le Monnier Università, 2020, p. 1.

³ Ibidem, p. 2.

Quando si pensa agli anni che vanno dal 1960 al 1990 si è invece soliti qualificare questa rivoluzione quale «rivoluzione digitale», oppure, per gli anni direttamente successivi fino ai giorni nostri, «era digitale».⁴

La parola «digitale» deriva dal latino «*digitus*», ovvero «dito», da cui poi si ottiene il termine inglese «*digit*», ovvero digitare: centrale è il concetto di numero, il termine si rifà infatti a «*una misurazione o una rappresentazione di fenomeno attraverso i numeri*».⁵ Allo stesso tempo, digitale si contrappone ad analogico.⁶ Semplificando, se nell'analogico un messaggio viene riprodotto per analogia, nel sistema digitale centrale è invece il codice binario. Stando alla definizione fornita dall'Enciclopedia Treccani, esso è

*«codice basato su due soli simboli, usualmente 0 e 1. Un codice binario permette la trasmissione di dati e istruzioni mediante una sequenza di 0 e 1, che può essere realizzata con un circuito formato da un dispositivo capace di assumere due stati diversi di tensione (tipicamente acceso e spento)».*⁷

Il codice binario è il linguaggio dei calcolatori, e dunque del computer. Il valore di 0 o 1 viene espresso tramite un'unità di informazione minima che prende il nome di *bit*, abbreviazione di *binary digit*. Tramite un bit, è possibile dare un comando elementare, come acceso/spento. Inoltre, grazie all'interazione di un certo numero di bit, è possibile rappresentare qualsiasi dato della realtà.⁸

I computer nascono come calcolatori, ma è con la digitalizzazione delle informazioni che i computer iniziano a diventare le macchine che oggi permeano la nostra quotidianità. Tramite il processo di digitalizzazione, infatti, vi è una vera e propria conversione dall'analogico al digitale, tramite la codificazione in bit di tutta una serie di informazioni, raggruppandole dunque in *file*. Queste informazioni digitali sono poi state trasformate in dati, tramite la datizzazione (dall'inglese *datification*). Se da un lato la digitalizzazione trasforma dall'analogico al digitale, la datizzazione descrive «*il procedimento attraverso il quale l'informazione digitalizzata è processata dalla macchina per estrarne ulteriori informazioni*».⁹

Nelle innovazioni che caratterizzano l'era digitale, un ruolo fondamentale è ricoperto dall'invenzione di *Internet* e del *World Wide Web*. Sebbene ad oggi questi termini siano comunemente utilizzati in maniera intercambiabile, è bene sin da subito sottolineare che si tratta, in realtà, di due fenomeni differenti.

Stando alla definizione di Quarta¹⁰ e Smorto¹¹, Internet è «*una rete di collegamenti informatici su scala globale che consente di connettere tra loro computer e dispositivi, più genericamente, 'nodi', ciascuno dei quali con capacità di ricevere e trasmettere*

⁴ Ibidem.

⁵ G. Pascuzzi, «Il diritto dell'era digitale», Bologna, Il Mulino 2020, p. 21.

⁶ A. Quarta, G. Smorto, «Diritto privato dei mercati digitali», p. 3.

⁷ Definizione disponibile al seguente link: <https://www.treccani.it/enciclopedia/codice-binario/>.

⁸ A. Quarta, G. Smorto, «Diritto privato dei mercati digitali», p. 4.

⁹ Ibidem, p. 10.

¹⁰ Alessandra Quarta è ricercatrice di diritto privato all'Università di Torino, dove coordina il progetto di ricerca gE.CO Living Lab finanziato dal programma dell'UE Horizon 2020.

¹¹ Guido Smorto è professore ordinario di diritto privato comparato all'Università di Palermo.

dati».¹² Nato come uno strumento di comunicazione militare con il nome di ARPANET, già negli anni Settanta inizia ad essere impiegato anche per usi civili. Il punto di svolta si ha poi con l'invenzione del World Wide Web a opera di Tim Berners-Lee, ricercatore del CERN di Ginevra. In estrema sintesi, il World Wide Web si basa sulla possibilità di presentare un qualsiasi file presente su uno dei nodi come «pagina web», a loro volta raggruppabili in «siti», collegati tra loro tramite «hyperlink», o – secondo un termine generalmente più utilizzato oggi – «link». Si crea presto un ecosistema in cui tutte le informazioni presenti sul web sono collegate e accessibili.¹³

La nascita del *World Wide Web* porta con sé la promessa ideologica per cui la rete, intesa come luogo virtuale, è lo spazio in cui gli individui possono godere a pieno delle loro libertà individuali. La struttura della rete e la refrattarietà dei bit creano un luogo non regolabile, in cui non trovano spazio forme di regolamentazione da parte degli Stati o di soggetti terzi. Questo perché l'individuo, in rete, è considerato libero di scegliere a quali regole sottoporsi.¹⁴

In un primo momento, questa promessa sembra realizzarsi: la connotazione intrinseca della rete rende estremamente complicato comprendere, per dirla come Quarta e Smorto, «*chi fa cosa e dove*»;¹⁵ tuttavia vengono ben presto ideate tecnologie che permettono l'identificazione dei soggetti; citandone alcune, basti pensare all'indirizzo IP¹⁶ o ai cookie.¹⁷

Negli anni Novanta si inizia dunque presto a interrogarsi circa la necessità di regolare il mondo del web attraverso un'apposita branca del diritto, detta *cyberlaw*. Sarebbe tuttavia un errore credere che il primo momento in cui il diritto incontra la tecnologia sia la fine del Novecento: in realtà, diritto e tecnologia sono in relazione sin dall'invenzione della scrittura, della penna e del linguaggio.¹⁸

Il tentativo di adattare schemi preesistenti all'era digitale si rileva presto un'attività non semplice, infatti, come sapientemente affermato da Rodotà¹⁹:

«[Sono] i temi della tecnica quelli che meglio definiscono le prospettive e le angosce del nostro tempo. L'intreccio tra innovazione tecnologica, mutamento sociale e soluzioni giuridiche pone ogni giorno problemi di fronte ai quali spesso appaiono del tutto improponibili i vecchi criteri, le ricette conosciute».

¹² A. Quarta, G. Smorto, «Diritto privato dei mercati digitali», p. 12.

¹³ Ibidem, p. 13.

¹⁴ Ibidem, p. 53.

¹⁵ Ibidem, p. 54.

¹⁶ L'indirizzo IP è una sequenza di numeri o di caratteri alfabetici che permette di individuare un elaboratore connesso in rete, indispensabile sia per ricevere sia per inviare dati; si basa sul protocollo IP (Internet protocol), che regola l'interconnessione tra reti. Si v.

https://www.treccani.it/enciclopedia/indirizzo-ip_%28Lessico-del-XXI-Secolo%29/.

¹⁷ Un cookie è file di servizio che viene inviato da un sito Internet all'utente che si colleghi con esso, allo scopo di registrarne l'accesso e di rilevare altri dati; è usato in alcuni casi per favorire l'interattività, in altri per ottenere informazioni in modo surrettizio.

<https://www.treccani.it/vocabolario/cookie/>.

¹⁸ G. Pascuzzi, «Il diritto dell'era digitale», Bologna, Il Mulino 2020, p. 21.

¹⁹ S. Rodotà, «Tecnologie e diritti», Bologna, Il mulino, 1995, p. 9.

In altre parole, diritto e tecnologia viaggiano a due velocità differenti. Come è stato brillantemente osservato, «*la tecnologia corre, il diritto statale insegue*». ²⁰ La regolazione cosiddetta dall'«esterno» da parte del legislatore incontra gli ostacoli delle caratteristiche fisiologiche della rete stessa. Nasce così l'idea di cercare una regolazione dall'interno, una sorta di «*lex informatica*» che possa fare della tecnica vero e proprio diritto. ²¹

È in questi confini che si colloca la celeberrima intuizione del giurista statunitense Lawrence Lessig ²² «*code is law*», ovvero il codice informatico è visto come norma, diritto, è regolazione. Per comprendere a pieno la lettura di Lessig, gioverà fornire una definizione di cosa sia la regolazione. Secondo la definizione di Quarta e Smorto ²³:

«[Essa] comprende in sé un complesso e variegato sistema di incentivi e disincentivi, accumulati dalla capacità di orientare i comportamenti e di sanzionare eventuali deviazioni. Così declinata, l'espressione 'regolazione' include tutte le forme di controllo sociale idonee a influenzare i comportamenti dei consociati».

All'interno della regolazione ideata da Lessig, coesistono il diritto statale, le norme sociali, le regole dettate dal mercato e quelle dettate dall'architettura digitale, ovvero il codice informatico. La potenza pervasiva dell'architettura digitale sta nel fatto che essa è in grado di auto-eseguirsi: in altre parole, se una norma imposta dal legislatore è sempre passibile di violazione, l'architettura pone delle barriere fisiche che non possono essere superate. ²⁴ Come un muro vieta l'accesso a un terreno, così il codice informatico condiziona il comportamento umano analogamente a quanto avviene tramite le norme statali.

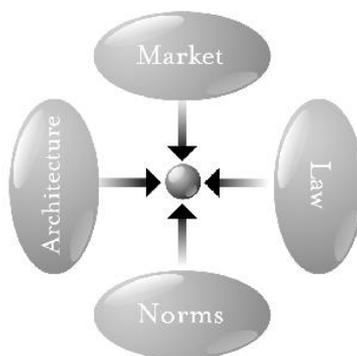


Figura 1: Code and other laws of cyberspace. FONTE: Wikipedia, CC-BY-SA 2.5

²⁰ R. Caso, «La società della mercificazione e della sorveglianza: dalla persona ai dati», versione 1.0, Zenodo, 2021, p.71. <https://doi.org/10.5281/ZENODO.4603174>.

²¹ Si v. J. R. Reidenberg, «Lex Informatica: The formulation of Information Policy Rules through Technology», 76 Tex. L. Rev., 1997-1998, pp. 553-593.

²² L. Lessig, «Code and other Laws of Cyberspace», New York, Basic Books, 1999.

²³ A. Quarta, G. Smorto, «Diritto privato dei mercati digitali» p. 60.

²⁴ Ibidem, p. 61.

Da queste sapienti osservazioni, nasce il metodo *Law&Technology*.²⁵ Al centro, vi è la comparazione intesa come processo cognitivo²⁶, ma si sceglie di comparare non solo all'interno del diritto, ma di aprire il dialogo nei confronti di altri saperi.²⁷ Scrive, infatti, Pascuzzi²⁸:

«La comparazione ci fa vedere come sono nati gli istituti giuridici e come si sono evoluti. Essa pertanto indaga: aspetti storici, aspetti sociologici, aspetti economici. Il comparatista combatte gli steccati disciplinari. Il comparatista padroneggia, tra gli altri, gli skills del lavoro interdisciplinare. [...] La comparazione fa del mutamento e dell'innovazione degli oggetti privilegiati di indagine. La comparazione studia le tecniche dell'innovazione giuridica».

L'obiettivo di fondo che si perseguirà in questo lavoro sarà dunque quello di tracciare il collegamento esistente tra evoluzione tecnologica e universo del diritto. Si intende guardare come le innovazioni tecnologiche come *Big Data*, algoritmi e intelligenza artificiale abbiano sollevato nuove criticità proprie dell'era digitale, come il problema del *capitalismo della sorveglianza*, brillantemente ipotizzato e descritto dalla professoressa statunitense Shoshana Zuboff.²⁹ Attraverso un'analisi dei problemi giuridici emergenti dal capitalismo della sorveglianza applicato al mondo della didattica a distanza, si cercherà di utilizzare il dialogo tra saperi quale metodo principale per fornire una lettura quanto più possibile olistica delle problematicità dell'era digitale.

La scelta di utilizzare questo metodo interdisciplinare potrà inoltre rappresentare un prezioso aiuto nel tentativo di fornire delle definizioni quanto più esaustive dei concetti che guidano l'era digitale, nonostante permangano le difficoltà sopra descritte.

1.1.2 Big Data

Come verrà illustrato nel paragrafo 1.2, i *Big Data* sono la fonte del surplus comportamentale e dunque il motore del capitalismo della sorveglianza.³⁰ Non esiste una definizione univoca di *Big Data*, ma è possibile descriverli, in primissima approssimazione, «*come grandi quantità di dati di tipo diverso prodotti a grande velocità da numerosi tipi di fonti*».³¹

²⁵ Il metodo che insiste sul rapporto tra diritto e tecnologia è diffuso già da alcuni decenni in Canada e negli Stati Uniti. Ad esempio, si pensi rispettivamente al Centre for Intellectual Property Policy presso l'Università McGill, oppure al Berkman Klein Center for Internet & Society presso l'Harvard Law School.

²⁶ G. Pascuzzi, «Il problem solving nelle professioni legali», Bologna, il Mulino, 2017.

²⁷ R. Caso, «La società della mercificazione e della sorveglianza: dalla persona ai dati», p.61.

²⁸ G. Pascuzzi, «Il problem solving nelle professioni legali», p. 122.

²⁹ S. Zuboff, «Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri».

³⁰ Per un'analisi approfondita sul concetto di *Big Data*, si veda J. M. Cavanillas, E. Curry, W. Wahlster, a c. di, «New Horizons for a Data-Driven Economy», Cham, Springer International Publishing, 2016. <https://doi.org/10.1007/978-3-319-21569-3>.

³¹ Commissione europea, Comunicazione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, Verso una florida economia basata sui dati, 2 luglio 2014, consultabile al link: <https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:52014DC0442>.

Non è mancato anche chi ha definito i *Big Data* come il nuovo petrolio³², e chi invece ha insistito sulla possibilità di equipararli al capitale.³³

Con riferimento ai *Big Data*, particolare rilievo assumono le loro caratteristiche di volume (convenzionalmente, seppur non univocamente, 500 megabyte di dati), varietà (i *Big Data* riguardano diverse tipologie di file), e velocità.³⁴

I *Big Data* sono poi eterogenei, dal momento che rappresentano il risultato dei comportamenti casuali degli utenti.³⁵ La loro rilevanza dipende poi dalla possibilità di aggregazione, ovvero dalla possibilità di ricavare, da un grande insieme di set di dati tendenzialmente *non strutturato*, pattern o relazioni tra di essi, mentre risultano senz'altro poco utili quando analizzati singolarmente.³⁶

Come conseguenza di questa loro caratteristica, i dati aggregati sono anche *agnostic*: non risultano valutabili e classificabili alla luce di quelle che sono le tecniche tradizionali manageriali o di marketing, dal momento che promanano dalla quotidiana attività degli utenti online e non sono quindi organizzabili secondo i criteri standard delle discipline economiche.³⁷ Inoltre, mentre il marketing e l'attività manageriale usano tradizionalmente insieme di dati prettamente alfanumerici, i *Big Data*, soprattutto i *social data*, esulano da questa caratteristica, potendosi invece qualificare come *trans-semiotic*, ovvero mettono insieme diverse combinazioni di formati di dati, come per esempio testo, suono e immagine.³⁸

Infine, il grande valore dei *Big Data* dipende dal continuo aggiornamento degli stessi, caratteristica immanente del sistema di internet.³⁹

I dati possono essere offerti volontariamente e intenzionalmente da un utente di un determinato servizio o prodotto, possono essere osservati, ovvero rilevati automaticamente dalle attività degli utenti e delle macchine, ma esistono anche dati che vengono dedotti da quelli offerti volontariamente o osservati.⁴⁰

L'autrice del concetto di *surveillance capitalism* rigetta una definizione di *Big Data* che li avvicini ad una tecnologia o ad un prodotto della stessa, piuttosto, essi vanno considerati come qualcosa che si origina nella dimensione sociale: sono la componente fondamentale della nuova logica di accumulazione del capitalismo della sorveglianza.⁴¹

³² The Economist, «The world's most valuable resource is no longer oil, but data», maggio 2017, <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>.

³³ J. Pooley, «Surveillance Publishing», *The Journal of Electronic Publishing* 25, fasc. 1, 6 aprile 2022, pp. 39-49, p. 42.

<https://doi.org/10.3998/jep.1874>.

³⁴ G. Pascuzzi, «Il diritto dell'era digitale».

³⁵ I.D. Constantiou, J. Kallinikos, «New Games, New Rules: Big Data and the Changing Context of Strategy», *Journal of Information Technology* 30, fasc. 1, marzo 2015, pp. 44-57, p. 12.

<https://doi.org/10.1057/jit.2014.17>.

³⁶ *Ibidem*, p. 14.

³⁷ *Ibidem*.

³⁸ *Ibidem*.

³⁹ *Ibidem*, p. 15.

⁴⁰ A. Stazi, F. Corrado, «Datificazione dei rapporti socio-economici e questioni giuridiche: profili evolutivi in prospettiva comparatistica», *Il diritto dell'informazione e dell'informatica*, 2019, pp. 443-487, p. 445-446.

⁴¹ S. Zuboff, «Big Other: Surveillance Capitalism and the Prospects of an Information Civilization», *Journal of Information Technology* 30, fasc. 1, marzo 2015, pp. 75-89, p. 79.

Shoshana Zuboff individua le diverse fonti da cui promanano i *Big Data* nelle computer-mediated transactions⁴², ma anche dai sensori apposti negli oggetti (cosiddetti «*smart objects*»), dai database governativi e dalle telecamere di sorveglianza sia pubbliche che private. I *Big Data* derivano anche dall'attività quotidiana degli utenti: la frase «*nothing is too trivial or ephemeral for this harvesting*»⁴³ esprime con chiarezza l'immagine dell'enorme quantitativo di dati ottenuto dalle più casuali attività svolte dagli utenti in ogni minima interazione.

L'attività di estrazione di dati descritta da Shoshana Zuboff viene ad oggi generalmente descritta con l'espressione *data mining*, ovvero «*un processo computazionale che crea modelli analizzando i dati da diverse prospettive e dimensioni, classificandoli ed enucleando potenziali relazioni e impatti*».⁴⁴ Secondo Zuboff, l'attività di estrazione perpetrata dai capitalisti della sorveglianza si declina in un'attività a senso unico, nella quale gli operatori come Google si pongono in un atteggiamento di indifferenza formale nei confronti degli utenti: le intenzioni dietro le attività da cui si estrae il surplus comportamentale vengono del tutto ignorate.⁴⁵

L'analisi dei *Big Data* permette la valutazione di correlazione tra fenomeni, che vengono posti in un'ottica di correlazione statistica. Inoltre, essi possono essere impiegati e rivalutati più volte, con un potenziale di riutilizzo illimitato.⁴⁶

1.1.3 Intelligenza artificiale

Anche il termine intelligenza artificiale (spesso solamente abbreviata in IA) non si presta ad una definizione univoca.⁴⁷ Stando alla definizione dell'enciclopedia Treccani⁴⁸, essa può essere descritta come

«Disciplina che studia se e in che modo si possano riprodurre i processi mentali più complessi mediante l'uso di un computer. Tale ricerca si sviluppa secondo due percorsi complementari: da un lato l'i. artificiale cerca di avvicinare il funzionamento dei computer alle capacità dell'intelligenza umana, dall'altro usa le simulazioni informatiche per fare ipotesi sui meccanismi utilizzati dalla mente umana».

Ricostruendo brevemente la sua storia, il concetto nasce dal 1956 dall'entusiasmo di un gruppo di scienziati che, dopo essersi riunito per sei settimane presso il College Dartmouth, ritenne di poter affermare con certezza che la macchina fosse in grado di

<https://doi.org/10.1057/jit.2015.5>.

⁴² Per un approfondimento, si v. il paragrafo 1.4.2 del presente lavoro.

⁴³ S. Zuboff, «Big Other: Surveillance Capitalism and the Prospects of an Information Civilization», p. 79.

⁴⁴ A. Quarta, G. Smorto, «Diritto privato dei mercati digitali», pag. 265.

⁴⁵ S. Zuboff, «Big Other: Surveillance Capitalism and the Prospects of an Information Civilization», p.79.

⁴⁶ A. Quarta, G. Smorto, «Diritto privato dei mercati digitali», p.21.

⁴⁷ Si v. P.M. Krafft, M. Young, M. Katell, K. Huang, G. Bugingo, «Defining AI in Policy versus Practice in Proceedings of the 2020 AAAI/ACM Conference on AI, Ethics, and Society», New York, NY, USA, 2020, pp. 72-78.

⁴⁸ La definizione è consultabile al seguente link: <https://www.treccani.it/enciclopedia/intelligenza-artificiale>.

emulare la conoscenza e l'intelligenza umana.⁴⁹ In questo senso, la definizione appena fornita dell'enciclopedia Treccani sembra ancora oggi abbracciare la lettura fiduciosa degli scienziati finanziati dalla Rockefeller Foundation.

La prima fase dell'intelligenza artificiale è senza dubbio pionieristica se paragonata agli sviluppi ad oggi noti e particolarmente cari al capitalismo della sorveglianza. Inizialmente, infatti, l'intelligenza artificiale funzionava come dei semplici «sistemi esperti» retti da un meccanismo che prende il nome di *if then*.⁵⁰ In particolar modo, il meccanismo dei sistemi esperti si basa sull'idea per cui ad ogni condizione corrisponde un'azione.⁵¹

Ad oggi, una tipologia di intelligenza artificiale considerata fondamentale nell'età del capitalismo della sorveglianza è il *machine learning*. La peculiarità del *machine learning* è tutta nella sua capacità di apprendere dall'esperienza, e da questa migliorarsi. Il motivo del passaggio da un tipo di intelligenza artificiale all'altro si riconduce al fatto che il modello *if then* non è ritenuto adatto a processare l'enorme quantitativo di dati ad oggi prodotti dalle tecnologie dell'era digitale.⁵²

Il *machine learning*, in particolare una sua peculiare declinazione detta *deep learning*, opera come su delle cosiddette «*neural network*», seguendo l'esempio dell'anatomia della mente umana. In questo *neural network* esistono tutta una serie di «nodi» o «neuroni artificiali», posizionati uno sopra l'altro, in grado di comunicare tra loro in senso verticale. Durante questo processo di comunicazione, ogni dato ottiene uno specifico valore, e, affinché il dato possa passare da uno strato all'altro, è necessario che abbia un certo valore, altrimenti è scartato.⁵³

Un esempio potrà aiutare a comprendere più a fondo la differenza tra sistemi esperti e *machine learning*: la prima intelligenza artificiale poteva essere utilizzata per creare un programma per il computer in grado di sostenere una partita di scacchi sulla base delle informazioni raccolte (si è soliti dire «*fed*», ovvero «nutrita») dalle partite dei campioni. Con il *machine learning*, invece, ogni partita genera un quantitativo di dati nuovi che permette alla macchina di migliorarsi, di inventare nuove mosse, senza dover necessariamente seguire dei comandi che vengono determinati a monte, come appunto nel caso dei sistemi esperti.⁵⁴

1.1.4 Algoritmo

⁴⁹ J. Mc Carthy, M.L. Minsky, N. Rochester, C.E. Shannon, «A proposal for the Dartmouth Summer Research Project on Artificial Intelligence», 1955.

⁵⁰ A. Quarta, G. Smorto, «Diritto privato dei mercati digitali», p.16.

⁵¹ Si v. J. Kaplan, «Artificial Intelligence. What everyone needs to know», New York, Oxford University Press USA, 2016.

⁵² E. Bassoli, «La Ciber-Etica: luci e ombre della predittività algoritmizzata» in Liber Amicorum per Pasquale Costanzo, 2020,

http://www.giurcost.org/LIBERAMICORUM/bassoli_scrittiCostanzo.pdf.

⁵³ A. Quarta, G. Smorto, «Diritto privato dei mercati digitali», p. 17.

⁵⁴ Ibidem.

L'intelligenza artificiale funziona tramite algoritmi. L'algoritmo è un concetto matematico risalente nel tempo, con cui si descrive una sequenza finita o ordinata di istruzioni che produce un risultato specifico.⁵⁵

Il tipo di algoritmo che assume rilievo nell'IA è quello inteso secondo il linguaggio informatico, ovvero «*un procedimento per la soluzione di un problema mediante l'applicazione di una sequenza finita di istruzioni, tale da essere implementate sotto forma di programma*».⁵⁶ In altre parole, un algoritmo è l'insieme di singoli passaggi logici di una certa procedura per la risoluzione di un dato problema. L'algoritmo interagisce con la macchina grazie al *coding*, ovvero una particolare tecnica consistente in un programma che traduce la sequenza di passaggi dell'algoritmo in una serie di comandi rivolti al computer.⁵⁷

1.2 Dal capitalismo al “capitalismo della sorveglianza”

Il concetto di «*capitalismo della sorveglianza*» ha visto la luce per la prima volta nel 2019, grazie alla preziosa riflessione della già menzionata accademica statunitense Shoshana Zuboff, nella sua celeberrima opera «*Surveillance Capitalism: The Fight for a Human Future at a New Frontier of Power*».

Si tratta di un fenomeno protagonista dell'era digitale come il capitalismo industriale è stato protagonista nel Novecento, il quale mira a trasformare la vita delle persone in un enorme quantitativo di dati estratti dagli stessi comportamenti umani. Questi dati, se da un lato vengono utilizzati per migliorare i prodotti o i servizi offerti, dall'altro diventano *surplus comportamentale*, che, sottoposto a sofisticati algoritmi di intelligenza artificiale, genera veri e propri prodotti predittivi, a loro volta successivamente scambiati su un nuovo tipo di mercato, che Shoshana Zuboff identifica come «*mercato dei comportamenti futuri*».

Per il capitalismo della sorveglianza l'utilizzo di tecnologie innovative ricopre un ruolo fondamentale, e non sono mancati, da parte dei grandi operatori, tentativi di far passare l'idea per cui l'attività che va dall'estrazione dei dati personali al loro utilizzo per prodotti predittivi sia insita all'interno delle tecnologie stesse. In realtà, secondo l'autrice, questa attività è il frutto di una precisa scelta economica che muove le fila dell'utilizzo di piattaforme, algoritmi e intelligenza artificiale a suo piacere.⁵⁸

A parere di Zuboff, il capitalismo della sorveglianza è nato in California, precisamente nella Silicon Valley, grazie ad una brillante intuizione ad opera di Amit Patel, giovane laureato di Stanford impiegato da Google.

Si tratta dunque di un'invenzione americana, che ha tuttavia in breve tempo influenzato l'intero globo. Google rappresenta dunque l'azienda che ha «*guidato, scoperto, elaborato, sperimentato, messo in pratica e diffuso il capitalismo della sorveglianza*».⁵⁹

⁵⁵ Per una definizione di algoritmo di veda Enciclopedia Treccani:

<https://www.treccani.it/vocabolario/algoritmo/>.

⁵⁶ A. Quarta, G. Smorto, «Diritto privato dei mercati digitali», p. 14.

⁵⁷ Ibidem.

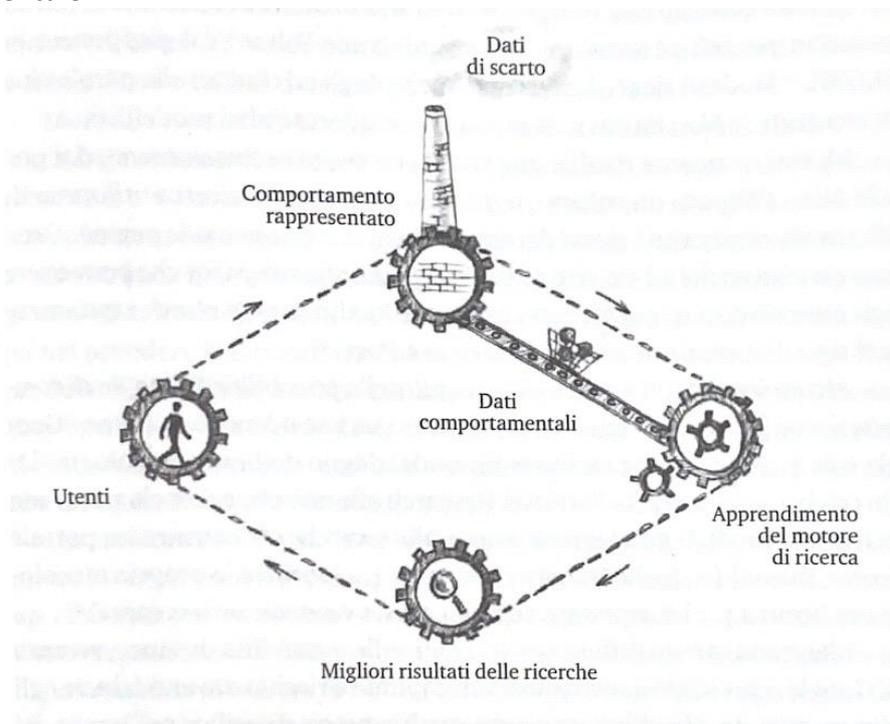
⁵⁸ S. Zuboff, «Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri», p. 25.

⁵⁹ Ibidem, p. 73.

Google è nato nel 1988 dall'idea di Larry Page e Sergey Brin come un motore di ricerca che sfrutta un algoritmo, detto *Page Rank*, già noto al mondo dell'editoria scientifica ed al mondo accademico grazie al sistema degli indici citazionali ideato da Eugene Garfield. L'idea di fondo era quella di poter sviluppare un motore di ricerca che proponesse agli utenti dei risultati posti in ordine in base alla loro rilevanza, calcolata in base al numero di click che di cui ogni pagina godeva.

Amit Patel fu il primo a comprendere il valore nascosto dei dati collaterali, inizialmente intesi come veri e propri dati di scarto, che si creano ogni volta che viene effettuata una ricerca. Questi dati, che comprendono localizzazione, tempo di sosta, spelling o semplicemente numero e pattern dei termini cercati, forniscono dei rilevatori del comportamento umano, che permettono l'implementazione di importanti innovazioni tecnologiche, come ad esempio il controllo dello spelling o il riconoscimento vocale. Grazie a queste intuizioni, fu sviluppato il celeberrimo motore di ricerca Google Search.

Il rapporto iniziale tra Google e gli utenti era, secondo Zuboff, simbiotico e in equilibrio: da un lato, Search apprendeva e migliorava grazie ai dati collaterali degli utenti, dall'altro, gli utenti apprendevano da questo motore di ricerca che si apprestava a diventare un'intelligenza artificiale onnicomprensiva. Google, negli anni iniziali, poteva ancora essere qualificata come un'azienda operante nel semplice capitalismo industriale e manageriale: i dati comportamentali venivano raccolti con il permesso dell'utente, perseguendo lo scopo precipuo di miglioramento dei propri prodotti e servizi. Attraverso l'estrazione e l'analisi di questi dati era infatti possibile migliorare la *user experience*, in un processo che Shoshana Zuboff definisce «*ciclo di reinvestimento del valore comportamentale*».⁶⁰



⁶⁰ Ibidem, p. 79.

Figura 2: Il ciclo di reinvestimento del valore comportamentale. FONTE: Shoshana Zuboff, «Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri», Roma, Luiss University Press, 2019, p. 81.

Questo particolare ciclo è rivolto all'individuo come soggetto, in un contesto in cui le innovazioni tecnologiche e l'era digitale spostavano l'obiettivo dal consumo di massa a quello individuale.

Ben presto tuttavia si comprese l'enorme fallacia di questo sistema: mancava infatti la possibilità di trasformare gli investimenti in ricavi. Il fatto di aver creato un motore di ricerca eccellente, in grado di soddisfare il desiderio di conoscenza degli utenti, nutrendosi per migliorarsi dei dati degli utenti stessi, non portava in ultima istanza alcun profitto. I dati comportamentali rimanevano all'interno di un circolo virtuoso che forniva senz'altro benefici agli utenti, ma che non permetteva a Google di affermarsi dal punto di vista economico.

Nell'aprile del 2000, l'azienda della Silicon Valley che era stata in grado di implementare il miglior motore di ricerca in circolazione, si trovò a dover fare i conti con la «bolla dot-com», ovvero una profonda crisi finanziaria che attraversò il mondo delle start-up e che portò i prezzi delle azioni ad un prezzo minimale, soprattutto se considerata la grande speculazione precedente.⁶¹

Davanti al rischio che gli investitori più importanti si tirassero indietro, Google dovette prendere la difficile scelta di investire sulla pubblicità. Se infatti in un primo momento l'advertising era considerato dai fondatori di Google uno strumento lesivo delle esigenze dei consumatori e sbilanciato a favore degli inserzionisti, in questo clima di grande retrocessione finanziaria Google rivalutò la pubblicità quale fonte di profitto. La pubblicità implementata da Google presentava, però, una novità fondamentale: era «targettizzata», ovvero era in grado di raggiungere gli individui target con maggiore precisione, rappresentando quindi un'importante fonte di reddito non solo per Google, ma per gli inserzionisti stessi. Tutto ciò era possibile grazie all'utilizzo del «surplus comportamentale», che da quel momento in poi non aveva più il semplice compito di nutrire il ciclo di reinvestimento del valore comportamentale. Google mirava a utilizzare i dati collaterali lasciati come tracce delle attività online per implementare degli *ads* che combaciassero perfettamente con gli interessi degli utenti.⁶²

Secondo Shoshana Zuboff, questa nuova modalità di utilizzo dei dati comportamentali segnò il passaggio dal semplice capitalismo al capitalismo della sorveglianza.⁶³

Il surplus comportamentale è quindi una vera e propria materia prima per questa nuova logica di accumulazione sottesa al nuovo fenomeno, e Google ha ben presto realizzato di essere in grado di aumentare i suoi ricavi solamente aumentando il surplus comportamentale a sua disposizione. Google ha quindi investito in tecnologie in grado di estrarre quanta più materia prima possibile. Shoshana Zuboff chiama questo

⁶¹ Ibidem, p. 80 e ss.

⁶² Ibidem, p. 84.

⁶³ Ibidem, p. 85.

fenomeno «*imperativo dell'estrazione*»⁶⁴, sottolineando come il capitalismo della sorveglianza necessiti un'economia di scala in materia di estrazione di surplus comportamentale.

Un esempio di misure finalizzate ad arginare la necessità di ulteriore materia prima è rappresentato, secondo Zuboff, dai moltissimi brevetti registrati da Google in quegli anni, come, ad esempio, quello finalizzato a «*generare informazioni sugli utenti per usarle nell'advertising mirato*», che non solo trasformava la query digitata in un ad, ma era in grado di identificare *user profile information*, ovvero nuovi set di dati che rendevano l'attività pubblicitaria, tradizionalmente incerta, un'attività vicina ad una scienza esatta, così da assicurare risultati profittevoli per gli inserzionisti.⁶⁵

Quindi, se in un primo momento Google semplicemente sfruttava i dati di scarto che fisiologicamente venivano creati, in un secondo momento ha iniziato a cercare nuove modalità per procacciarsi la materia prima di questo nuovo capitalismo della sorveglianza. Questa nuova ricetta, fatta di surplus comportamentale e brevetti, ha comportato non solo il superamento della crisi, ma anche un aumento esponenziale degli introiti di Google, che passarono da 86 milioni di dollari nel 2001 a 3,2 miliardi nel 2004.⁶⁶

In altre parole, secondo Zuboff, oggi Google, dopo aver ricavato il surplus comportamentale prodotto dagli utenti, decide di «darlo in pasto» ai mezzi di produzione più innovativi, tra cui figura anche l'intelligenza artificiale e in particolar modo il *machine learning*. Nutrita di surplus comportamentale, l'intelligenza delle macchine crea dei prodotti predittivi sulle preferenze degli utenti, che vengono poi venduti sul mercato dei comportamenti futuri.

⁶⁴ Ibidem, p. 98.

⁶⁵ Ibidem.

⁶⁶ Per approfondire l'evoluzione dal capitalismo al capitalismo della sorveglianza, si v. S. Zuboff, «Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri», capitolo III, p. 80-108.

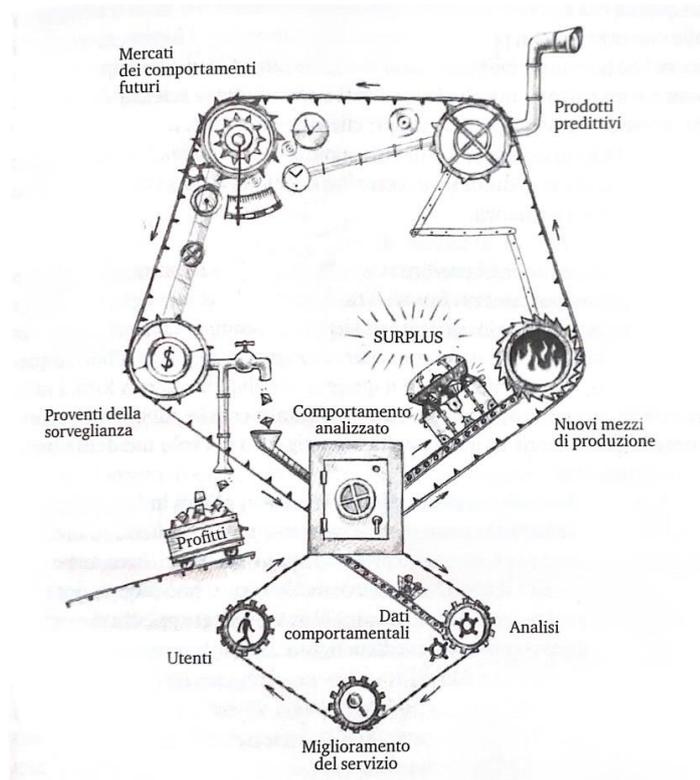


Figura 3: La scoperta del surplus comportamentale. FONTE: Shoshana Zuboff, «Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri», Roma, Luiss University Press, 2019, p.107.

1.3 Monopoli e oligopoli

1.3.1 La monopolizzazione degli utenti

Si è ormai diffusa tra la generalità dei consociati l'immaginifica citazione «*se non paghi per il prodotto, il prodotto sei tu*», segno di una progressiva presa di consapevolezza degli utenti delle criticità di base collegate all'era della digitalizzazione. Tuttavia, in questa sede, si sceglie di adottare una diversa chiave di lettura per ricostruire il ruolo ricoperto dagli utenti nell'era del capitalismo della sorveglianza.

Shoshana Zuboff,⁶⁷ infatti, descrive gli utenti come le fonti della materia prima. L'imperativo dell'estrazione impone che si ricerchi sempre più surplus comportamentale, affinché sia possibile sviluppare prodotti predittivi da sfruttare a vantaggio degli inserzionisti. In questa ottica, dunque, gli utenti sono un mezzo per uno scopo, quello degli inserzionisti, che sono i veri clienti di Google.

Affinché questo sistema funzioni, e affinché aumentino i profitti, l'imperativo dell'estrazione chiede sempre più materia prima: Google quindi inizia a sviluppare nuovi servizi e strumenti che gli permettano di acquisire quanto più surplus comportamentale possibile. Nel 2003, Google era l'unica azienda in grado di vantare un sistema in grado di estrarre un così grande quantitativo di surplus comportamentale. La ricerca

⁶⁷ S. Zuboff, «Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri», p. 79 e ss.

dell'esclusività guida l'attività di estrazione del colosso della Silicon Valley, che presto inizia a porsi sul mercato in una posizione di vero e proprio monopolio.

Tuttavia, il monopolio del capitalismo della sorveglianza presenta delle caratteristiche *sui generis*: se infatti nella concezione tradizionale i monopoli cercano di eliminare la concorrenza così da poter praticare prezzi più alti, il monopolio di Google nel capitalismo della sorveglianza cerca di raccogliere tutte le materie prime. Se i monopoli del capitalismo industriale vogliono proteggere la loro nicchia e mantenere il dominio del mercato, Google vuole estrarre tutto il surplus comportamentale esistente. Dal momento che questa materia prima è fornita dagli utenti, che sono l'oggetto da cui il surplus comportamentale viene estratto, è possibile in ultima istanza leggere questo processo di monopolizzazione come una monopolizzazione degli utenti stessi.⁶⁸

Se il capitalismo industriale era caratterizzato da una produzione di massa, grazie allo sviluppo di nuove tecnologie di analisi di dati, nel capitalismo della sorveglianza ci si trova davanti a un fenomeno di «*personalizzazione di massa*»⁶⁹: si cerca la produzione di un sempre più ampio numero di servizi pensati come un «abito su misura» per i singoli utenti, affinché possano combaciare con i loro interessi, preferenze e stile di vita, anticipandoli ancor prima che si manifestino. Beneficiando di un sempre crescente numero di servizi, gli utenti forniscono, direttamente o indirettamente, un feedback che continua a nutrire l'algoritmo affinché il servizio continui, inesorabilmente, a migliorarsi.⁷⁰

Per comprendere l'attività di monopolizzazione degli utenti compiuta da Google, gioverà ricostruire la storia del sistema operativo per smartphone, tablet e in generale dispositivi mobili ideato da Google: *Android*. Prima che lo smartphone irrompesse nell'attività quotidiana di una grande fetta della popolazione, Google riusciva a mantenere alto il livello di rifornimento di materia prima grazie al suo motore di ricerca. Con l'ascesa degli smartphone, Google ha dovuto cercare nuove fonti da cui estrarre il surplus comportamentale. La scelta strategica è stata quella di implementare e fornire tramite licenza gratuita ai produttori di dispositivi portatili il sistema operativo Android. Al centro vi era – e vi è tutt'ora – il *Google Play Store*, portale deputato al download delle applicazioni necessarie per l'utilizzo dello smartphone. Google, se da un lato forniva gratuitamente *Play Store* alle aziende produttrici di smartphone e tablet, dall'altro imponeva che i servizi principali fossero forniti esclusivamente da Google. In altre parole, lo smartphone o il tablet, appena acceso e configurato, già conosceva come motore di ricerca Google Search, come sistema di posta elettronica Gmail, YouTube quale piattaforma di condivisione di video, Google Maps come navigatore.⁷¹ Così facendo, Google ha monopolizzato una grande fetta di utenti, per estrarre quanto più surplus comportamentale possibile e mantenere la sua posizione di vantaggio,⁷² confermando il suo dominio anche nel passaggio dal personal computer allo smartphone.

⁶⁸ Ibidem, p. 142 e ss.

⁶⁹ Si v. K. Yeung, «Five Fears about Mass Predictive Personalization in an Age of Surveillance Capitalism», *International Data Privacy Law* 8, fasc. 3, 1 agosto 2018, pp.258-269, p. 259. <https://doi.org/10.1093/idpl/ipy020>.

⁷⁰ Ibidem.

⁷¹ A. Quarta, G. Smorto, «Diritto privato dei mercati digitali», p.169.

⁷² Ibidem.

1.3.2 «La guerra dell'estrazione»⁷³

La brillante intuizione di Amit Patel è stata ben presto apprezzata anche da altre aziende del mondo di internet, che hanno fatto dell'imperativo dell'estrazione e della monopolizzazione degli utenti la loro maggiore fonte di profitto. In questa sede si è scelto di riportare, a titolo esemplificativo, alcune delle strategie di estrazione di surplus comportamentale messe in atto da *Meta* e *Microsoft*⁷⁴, quali grandi aziende del settore.

Il social network Facebook,⁷⁵ nato dalla creatività del giovane studente di Harvard Mark Zuckerberg come uno strumento di connessione e comunicazione tra studenti universitari, ha ben presto rivelato le sue potenzialità in materia di estrazione di surplus comportamentale quando è divenuto accessibile a tutti nel 2007.

Il grandissimo vantaggio detenuto da Facebook risiede nel fatto che gli utenti pubblicano volontariamente tutta una serie di informazioni personali, come l'ubicazione, lo status sentimentale, il grado di istruzione, fornendo tutta una serie di dati che possono essere considerati reali, e non dedotti, come nel caso di Google.

Un ingente quantitativo di dati, poi, è frutto di un processo di deduzione, con una strategia che sembra ricalcare la strategia di Google: Facebook ha registrato una serie di brevetti riguardanti modalità per tracciare gli utenti, così da creare profili per ogni utente, ottenere feedback da parti terze e, in ultima istanza, utilizzare queste informazioni per finalità di advertising. Uno strumento preziosissimo per questa attività è il pulsante «like», che permette l'installazione di cookie nei computer degli utenti, a prescindere dal fatto che tale pulsante sia stato cliccato o meno, e a prescindere dal fatto che l'utente sia effettivamente iscritto a Facebook. I cookie, infatti, invisibili all'utente, vengono inseriti da terzi e permettono a chi li scarica di ricordare le attività dell'utente, comprese le sue preferenze. Si è così aperta una grandissima possibilità di estrarre surplus comportamentale dall'intera popolazione di Internet.⁷⁶

Facebook, così come Google, può essere anche definito una «rete a doppia faccia»⁷⁷, ovvero una rete in cui due gruppi di utenti, interagendo con la piattaforma, creano un valore reciproco: da un lato ci sono gli utenti, da cui si estraggono i dati, dall'altro gli inserzionisti che acquistano questi dati che vengono meticolosamente aggregati da Facebook, con la finalità di personalizzare le pubblicità e i servizi offerti. Per meglio comprendere la portata di questa attività, basti pensare che circa il 98% degli introiti di Facebook è rappresentato dall'attività di pubblicità.⁷⁸

⁷³ S. Zuboff, «Il capitalismo della sorveglianza», capitolo V, p. 168 e ss.

⁷⁴ Per un approfondimento sull'attività di estrazione del surplus comportamentale di Facebook e Microsoft sintetizzata nel presente paragrafo, si v. S. Zuboff, «Il capitalismo della sorveglianza».

⁷⁵ Oggi Facebook fa parte della società Meta Platforms Inc.

⁷⁶ A. Roosendaal, «Facebook Tracks and Traces Everyone: Like This!», SSRN Electronic Journal, 2010, <https://doi.org/10.2139/ssrn.1717563>.

⁷⁷ Si v. D.F. Spulber, «The economics of markets and platforms» *Journal of Economics & Management Strategy*, vol. 28, no. 1, 2018, pp. 159–72.

⁷⁸ M. J. Conyon, «Big Technology and Data Privacy», *Cambridge Journal of Economics* 46, fasc. 6, 31 dicembre 2022, pp. 1369-1385, p. 1375. <https://doi.org/10.1093/cje/beac052>.

Durante il processo di monopolizzazione degli utenti, Facebook ha eliminato ogni qualsivoglia concorrenza acquistando le aziende che riuscivano ad implementare modalità di estrazione di surplus comportamentale migliori. Ad oggi Meta, infatti, è proprietaria, non solo di Facebook e Facebook Messenger App – rispettivamente 2.7 e 1.3 miliardi di utenti – ma anche di *Instagram* dal 2012, che vanta circa 1.2 miliardi di utenti, e WhatsApp dal 2014, con circa due miliardi di utenti, detenendo quindi quattro dei cinque più utilizzati social network.⁷⁹

La stessa strada è stata seguita dall'azienda tecnologica multinazionale Microsoft. Nonostante un'inerzia iniziale, nel 2014 Microsoft ha cominciato a comprendere l'enorme valore di mercato del surplus comportamentale, e ha iniziato una progressiva attività finalizzata alla produzione di servizi che potessero portare abbondante materia prima. Microsoft ha inaugurato dunque il suo motore di ricerca, Bing, per emulare i risultati che Google era riuscito ad ottenere grazie a Google Search; poco dopo, invece, ha scelto di implementare l'assistente vocale *Cortana*, ma è stato il lancio del sistema operativo Windows 10 che ha segnato definitivamente la volontà di Google di porsi come potenza del capitalismo della sorveglianza.⁸⁰ Questo sistema operativo, ad esempio, riesce a collegarsi con i server di Microsoft anche quando si disattiva lo strumento dell'assistente vocale di Cortana e la possibilità di fare una ricerca sul web ogni volta che si digiti una parola nel menu start del sistema operativo. Infatti, digitando una parola sul menu start, viene comunque mandato un segnale al motore di ricerca Bing, che riesce a creare un file contenente informazioni su Cortana, anche se disattivata. Parte di questi dati, non è chiaro quali, vengono poi mandati periodicamente a un server di Microsoft. In altre parole, l'utente potrebbe credere che, visto che si è disabilitato il collegamento internet e Cortana, le ricerche effettuate rimangano estranee al web ed a Microsoft, ma non è così.⁸¹

Anche Microsoft, poi, ha iniziato a monopolizzare i suoi utenti acquistando la concorrenza: nel 2016 ha acquistato LinkedIn, social network professionale, da cui Microsoft ha potuto estrarre tutta una serie di dati personali volontariamente resi pubblici dagli utenti stessi.

1.3.3 Il capitalismo dei monopoli intellettuali

Grazie all'attività di monopolizzazione degli utenti descritta nei paragrafi precedenti, si delinea quello che Shoshana Zuboff chiama «*problema dei due testi*»,⁸² genesi di una divisione dell'apprendimento che si prospetta sempre più ingiusta. Il primo testo è chiaro, e gli utenti ne sono autori quanto lettori, in quanto contribuiscono alla sua formazione tramite la loro scelta di condivisione. Il problema risiede nel fatto che questo primo testo fornisce surplus comportamentale ad un secondo testo: il testo ombra. Il testo ombra non è accessibile a tutti, ma solo a quello che Zuboff definisce «/

⁷⁹ Il secondo social network per diffusione è invece YouTube, di proprietà di Google. Fonte: Statista.

⁸⁰ S. Zuboff, «Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri», p. 173.

⁸¹ Ars Technica, «Even When Told Not to, Windows 10 Just Can't Stop Talking to Microsoft», 13 agosto 2015, <https://arstechnica.com/information-technology/2015/08/even-when-told-not-to-windows-10-just-cant-stop-talking-to-microsoft/>.

⁸² S. Zuboff, «Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri», p.197.

nuovo clero»⁸³: gli operatori, ormai oligopolistici, del capitalismo della sorveglianza, che utilizzano il testo ombra per guidare in maniera occulta i contenuti che vengono mostrati agli utenti stessi.

Così come l'invenzione della stampa da parte di Gutenberg aveva messo la religione in mano alle masse, si è creduto che Internet potesse diffondere universalmente l'informazione.⁸⁴ Ad oggi, invece, l'orizzonte del capitalismo della sorveglianza è dominato da «*uno stretto clero di specialisti informatici che lavorano per privati con macchine private che imparano per i loro interessi economici*». ⁸⁵ La conoscenza, che dovrebbe essere un bene pubblico, dunque non rivale e non escludibile, è stata oggetto di un progressivo processo di mercificazione e assetizzazione.⁸⁶

Ecco che l'universo GAFAM (Google, Amazon, Facebook - ormai Meta -, Apple e Microsoft) è costituito dal «*più grande oligopolio della conoscenza mai apparso sul pianeta, in grado di gestire i flussi di dati, informazioni, conoscenze e costruire l'accesso (selettivo, ovviamente) alle nostre culture, lingue e memorie, personali e collettive*». ⁸⁷

Ugo Pagano ⁸⁸ ha chiamato questo fenomeno «*capitalismo dei monopoli intellettuali*», dal momento che pochi operatori economici detengono una «*quota sproporzionata della conoscenza*»⁸⁹ che diventa il bene «*più prezioso dell'azienda*». ⁹⁰

Il processo di rafforzamento dei diritti di proprietà intellettuale iniziato con la creazione della *World Economic Property Organisation (Wipo)* e con la stipulazione di *Agreement on Trade Related Aspect of Intellectual Property Rights (TRIPs)* ha rappresentato il terreno fertile per la nascita di questa «*nuova era del mondo dell'economia*». ⁹¹ Secondo Pagano, infatti, il tentativo di utilizzare i diritti di proprietà intellettuale come incentivi allo sviluppo della conoscenza è sfociato, dal 2000 in poi, in veri e propri processi di privatizzazione della conoscenza stessa. Se da un lato, infatti, il rafforzamento dei diritti di proprietà intellettuale può rendere maggiormente convenienti gli investimenti innovativi, questi permettono di conquistare posizioni di rendita monopolista. Queste ultime posizioni, infatti, diventano un disincentivo per i nuovi investimenti innovativi stessi, perché è possibile che i detentori dei diritti di

⁸³ Ibidem, p.198.

⁸⁴ Ibidem.

⁸⁵ Ibidem.

⁸⁶ C. Franch, «Il capitalismo dei monopoli intellettuali e l'editoria della sorveglianza. Un'analisi delle politiche europee sull'open science e sulla regolazione dei dati», Zenodo, 2023, p. 59.
<https://doi.org/10.5281/zenodo.7770242>.

⁸⁷ D. Fiormente, P. Sordini, «Geopolitica della conoscenza digitale. Dal web aperto all'impero di GAFAM», DigitCult. Scientific Journal on Digital Cultures, 17 giugno 2019, pp. 21-36, p. 28.
<https://doi.org/10.4399/97888255263183>.

⁸⁸ U. Pagano, «The Crisis of Intellectual Monopoly Capitalism», Cambridge Journal of Economics 38, fasc. 6, 1 novembre 2014, pp. 1409-1429.
<https://doi.org/10.1093/cje/beu025>.

⁸⁹ Ibidem, p. 1418.

⁹⁰ Ibidem, p. 1413.

⁹¹ Ibidem.

proprietà intellettuale esistenti li ostacolano.⁹² La privatizzazione della conoscenza, in ultima istanza, comporta l'impossibilità che da questa si formi ulteriore conoscenza.⁹³

Cecilia Rikap⁹⁴ sottolinea sapientemente che la tutela dei diritti di proprietà intellettuale – in particolare la tutela dei brevetti per invenzione - non è l'unico strumento con cui l'universo GAFAM non permette l'accesso di terzi alla conoscenza. Ogni azienda utilizza a suo vantaggio, a seconda delle diverse esigenze del settore, una serie di altri elementi, come la generale segretezza nella quale le operazioni vengono compiute, così come il vantaggio di velocità in termini di tempo di consegna (*lead-time*).

Per Rikap e Lundvall⁹⁵ è possibile classificare i monopoli intellettuali a seconda del grado di monopolizzazione della conoscenza:

- (i) i monopoli intellettuali di primo grado si basano solamente su diritti di proprietà intellettuale, e sono per tanto temporanei e specifici per una peculiare tecnologia;
- (ii) quelli di secondo grado combinano ai diritti di proprietà intellettuale meccanismi per mantenere il vantaggio con riferimento a quella specifica tecnologia;
- (iii) ci riferiamo invece ai monopoli intellettuali di terzo grado quando un operatore è in grado di sviluppare un dominio con riferimento alle tecnologie di portata generale («*general-purpose technology*»), che possono essere utilizzate in diversi sistemi di produzione;
- (iv) nel momento in cui uno o più operatori invece riescono a dominare l'implementazione e lo sviluppo di tecnologie a uso generale che permettono l'innovazione tecnologica stessa, si ha una vera e propria monopolizzazione dell'innovazione, descritta da Rikap monopolio intellettuale di quarto grado.

Un particolare esempio di tecnologia di portata generale che permette l'innovazione tecnologica stessa è il *machine learning*⁹⁶, già precedentemente descritto. Esso, infatti, viene considerato un vero e proprio metodo di invenzione.⁹⁷

Le aziende dell'universo GAFAM si prestano con facilità a diventare monopoli intellettuali di quarto grado, dal momento che sono ad oggi titolari tanto di enormi quantità di dati, quanto di sistemi di *machine learning* estremamente sofisticati. L'universo GAFAM è dunque considerato un «*data driven intellectual monopoly*», dal momento che le aziende sono state in grado di monopolizzare un nuovo metodo per le invenzioni, ovvero l'applicazione del *machine learning* per processare i *Big Data*. Le

⁹² U. Pagano, «Il capitalismo dei monopoli intellettuali», Menabò di Etica ed Economia (blog), 14 dicembre 2021.

<https://archivio.eticaeconomia.it/il-capitalismo-dei-monopoli-intellettuali/>.

⁹³ Ibidem.

⁹⁴ C. Rikap, B. Lundvall, «The Digital Innovation Race, conceptualizing the emerging New World Order», London, Palgrave Macmillan, 2021, p. 32 e ss.

<https://doi.org/10.1007/978-3-030-89443-6>

⁹⁵ Ibidem.

⁹⁶ Così C. Rikap, B. Lundvall, «The Digital Innovation Race, conceptualizing the emerging New World Order».

⁹⁷ Per un approfondimento, si v. I. M. Cockburn, R. Henderson, S. Stern «The impact of artificial intelligence on innovation», National Bureau of Economic Research, 2018.

piattaforme proprietarie di GAFAM sono la fonte principale da cui i dati vengono raccolti, anche se, come vedremo in seguito, il panorama di estrazione dei *Big Data* si è ormai ampliato.⁹⁸

Il meccanismo con cui si creano questi monopoli intellettuali è «*quasi invisibile eppure potente*»⁹⁹: i cittadini finanziano, principalmente con le imposte, la ricerca scientifica e tecnologica delle Università e degli istituti di ricerca, le conoscenze così prodotte finiscono però nelle imprese, dove vengono incorporate in decisioni di investimento e *venture capital*.¹⁰⁰ Ciò avviene anche grazie al fatto che ormai le cinque principali aziende tecnologiche riescono ad accaparrarsi i migliori talenti in materia di intelligenza artificiale grazie alle loro ampie disponibilità in termini di retribuzione.¹⁰¹ In questo modo, il capitale umano, creato a spese del settore pubblico nelle Università e nelle infrastrutture della ricerca, è messo al servizio di un'agenda di accumulazione del capitale.¹⁰² Le grandi aziende tecnologiche che distribuiscono i sistemi di intelligenza artificiale hanno dunque finanziato la ricerca universitaria e la divulgazione scientifica per diffondere nuovi sistemi di intelligenza artificiale che legittima un modello di business fondato sulla sorveglianza.¹⁰³ Infatti, maggiore è la conoscenza in materia di IA, migliori sono le performance di utilizzo del surplus comportamentale da parte degli algoritmi.¹⁰⁴ La conoscenza, pur non essendo un bene ben misurabile nei bilanci aziendali, è un bene decisivo per la sopravvivenza nel mercato: essa è «*causa del progresso economico*»¹⁰⁵, basti infatti pensare che «*il carbone e il petrolio non avrebbero alcun valore economico se non si sapesse come estrarre energia dalla combustione dei fossili*». ¹⁰⁶ Se queste informazioni fossero gestite da organizzazioni con missioni pubbliche, potrebbero essere una risorsa vitale per migliorare il benessere della società.¹⁰⁷

Per un certo periodo di tempo, in particolare tra gli anni '80 e '90, la normativa antitrust, in particolar modo quella di stampo brandesiano e ordoliberalista¹⁰⁸, è stata in

⁹⁸ C. Rikap, B. Lundvall, «The Digital Innovation Race, conceptualizing the emerging New World Order».

⁹⁹ M. Florio, «La privatizzazione della conoscenza», Bari, Editori Laterza, 2021, p. 12.

¹⁰⁰ Ibidem.

¹⁰¹ S. Zuboff, «Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri», p. 201.

¹⁰² M. Florio, «La privatizzazione della conoscenza», p. 61-62.

¹⁰³ D. Tafani, «Sistemi fuori controllo o prodotti fuorilegge? La cosiddetta "intelligenza artificiale" e il risveglio del diritto», bollettino telematico di filosofia politica, maggio 2023, p. 4.

<https://doi.org/10.5281/zenodo.7953605>.

¹⁰⁴ S. Zuboff, «Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri», p. 201.

¹⁰⁵ M. Florio, «La privatizzazione della conoscenza», p.7.

¹⁰⁶ Ibidem.

¹⁰⁷ Ibidem. Florio ipotizza inoltre una strategia, per l'industria farmaceutica, il cambiamento climatico e il governo pubblico dei dati, che restituisca ai cittadini i benefici di ciò che essi hanno contribuito a creare, nella forma di imprese pubbliche ad alta intensità di conoscenza quale evoluzione delle infrastrutture della ricerca. Per un approfondimento, si v. M. Florio, «La privatizzazione della conoscenza», Bari, Editori Laterza, 2021.

¹⁰⁸ Louis Brandeis connetteva la struttura economica con le condizioni proprie della democrazia, dunque un buon sistema economico avrebbe dovuto essere in grado di fornire a tutti un supporto adeguato a vivere vite dotate di un significato. La teoria ordoliberalista, invece, riteneva che il governo dell'economia fosse un problema di gestione del potere economico privato, auspicando la creazione di una «Costituzione economica» che connettesse la libertà umana con la politica economica. Lo Stato, che correva il rischio di essere soggiogato da potenti interessi privati, con il rischio di pesanti conseguenze anche per la

grado di erodere il monopolio intellettuale e tecnologico incentivando l'innovazione e la conoscenza.¹⁰⁹

Si pensi, ad esempio, al caso della International Business Machine (IBM) che, finita nel mirino della legislazione antitrust statunitense, onde evitare sanzioni, iniziò la produzione e la vendita separata di software e hardware, contribuendo all'ascesa di un'industria di software indipendente.¹¹⁰ La normativa antitrust fu dunque in grado di «sfidare i potenti e cambiare gli incentivi delle imprese e la struttura del mercato, in modo da creare nuove industrie e opportunità».¹¹¹

Sfortunatamente, la teoria antitrust di stampo ordoliberal e brandesiana è stata superata dalla Scuola di Chicago, che mette al centro della lente antitrust la teoria del prezzo.¹¹² In una frase, secondo la nuova scuola di Chicago la legge antitrust dovrebbe solamente preoccuparsi del monitoraggio dei prezzi e dunque del benessere del consumatore.¹¹³ Tale teoria è oggi diventata un presupposto fondamentale della legislazione antitrust,¹¹⁴ ma essa è inadatta ad affrontare il monopolio di Google, che presta i suoi servizi in maniera – apparentemente – gratuita.¹¹⁵ In generale, ad oggi raramente le preoccupazioni per l'innovazione o per gli effetti sul mercato non legati al prezzo animano le indagini antitrust, soprattutto al di fuori del contesto delle fusioni,¹¹⁶ che verrà analizzato al IV capitolo del presente lavoro.

1.3.3 Caratteristiche di monopoli e oligopoli: cenni

Più in generale, tutti gli operatori dell'universo GAFAM possono essere qualificati come operanti in mercati bilaterali, poiché svolgono funzioni di veri e propri intermediari tra domanda e offerta, tra utenti e inserzionisti pubblicitari. Questa realtà si caratterizza per una tendenza connaturata al monopolio, ovvero un'ipotesi limite di fallimento di mercato in cui si verifica un fenomeno di concentrazione in capo a un unico produttore di beni e servizi.¹¹⁷

democrazia, avrebbe dovuto rompere il potere privato, senza controllare le società. Per un approfondimento sull'evoluzione della dottrina antitrust, si v. T. Wu, «La maledizione dei giganti: un manifesto per la concorrenza e la democrazia», Bologna, Il Mulino, 2020 e l'addenda T. Wu, «The Curse of Bigness: New Deal Supplement», 2020, <http://dx.doi.org/10.2139/ssrn.3646258>; si v. anche L. Khan, «The End of Antitrust History Revisited», 133 Harvard Law Review 1655, 2020, pp. 1655-1672, <https://ssrn.com/abstract=3552132>.

¹⁰⁹ T. Wu, «La maledizione dei giganti: un manifesto per la concorrenza e la democrazia» p. 83 e ss.

¹¹⁰ Ibidem, p. 85.

¹¹¹ Ibidem, p. 89.

¹¹² Si v. R. A. Posner, «The Chicago School of Antitrust Analysis», 127, U. PA. Law. Review, 1979, pp. 925-948.

¹¹³ Per un approfondimento, si v. L. Khan, «Amazon's Antitrust Paradox», Yale Law Journal, Vol. 126, 31, 2017, pp. 710-805, <https://ssrn.com/abstract=2911742> e L. Khan, «The End of Antitrust History Revisited».

¹¹⁴ T. Wu, «La maledizione dei giganti: un manifesto per la concorrenza e la democrazia», p. 122.

¹¹⁵ Ibidem, p. 127. Allo stesso modo, la teoria antitrust della Scuola di Chicago fatica ad affrontare le peculiarità del dominio di Amazon, fondato su politiche di prezzi predatori, integrazione verticale con cui controlla diverse fasi della catena di produzione o distribuzione di beni o servizi e accumulazione di dati. Per un approfondimento, si v. L. Khan, «Amazon's Antitrust Paradox».

¹¹⁶ L. Khan, «Amazon's Antitrust Paradox», p. 722.

¹¹⁷ A. Quarta, G. Smorto, «Diritto privato dei mercati digitali», p.71.

Si guarderà con maggiore dettaglio la tutela della concorrenza e le soluzioni proposte in materia di antitrust nel quarto capitolo del presente lavoro, per ora giova invece spiegare cosa caratterizza un monopolio dal punto di vista della teoria economica.

In primis è fondamentale la presenza di esternalità di rete, ovvero un fenomeno per cui l'utilità del consumatore derivante dall'utilizzo di certi beni o servizi aumenta all'aumentare dell'utilizzo dei medesimi beni o servizi da parte di altri consumatori. Il caso paradigmatico è WhatsApp: se un consumatore è l'unico a disporre di tale servizio di messaggistica istantanea, la sua utilità non è molto alta, ma aumenterà nel momento in cui molti più consumatori lo utilizzeranno.¹¹⁸

Fondamentale poi è sottolineare l'impatto che hanno i costi di uscita: per quanto semplice possa sembrare smettere di usare una piattaforma per utilizzarne un'altra, in realtà le piattaforme GAFAM hanno individuato una serie di strategie che rendono alti i costi di uscita. Ad esempio, Apple crea un vero e proprio ecosistema in cui fornisce tutta una serie di beni e servizi tra loro dipendenti, scoraggiando l'utilizzo di beni e servizi alternativi.¹¹⁹

Importanti sono anche i rendimenti di scala, ovvero un fenomeno economico per cui un aumento nella scala della produzione provoca una diminuzione del costo medio unitario di produzione. Ciò avviene perché si ha una produzione caratterizzata da alti costi fissi, pertanto all'aumentare della stessa, diminuisce il costo medio unitario del prodotto, poiché i costi fissi si distribuiscono su una produzione più ampia.¹²⁰

Ancora una volta, però, la differenza è data dalla grande quantità di dati di cui queste aziende dispongono. I dati permettono, come già sottolineato, di conoscere la domanda del consumatore, e indirizzarlo verso ciò che davvero cerca. Ciò crea un vantaggio competitivo, che difficilmente le altre piattaforme emergenti possono colmare. Infatti, la combinazione tra *Big Data* e esternalità di rete genera benefici per un singolo operatore, così che questo possa creare barriere all'ingresso a danno della sua base di utilizzatori.¹²¹

Un altro modo di leggere l'universo GAFAM è quello di qualificarli come operatori oligopolistici. Infatti, se è vero che – ad esempio – Meta detiene un grande potere di mercato in materia di social network, Google per quanto riguarda i motori di ricerca e Amazon per in materia di e-commerce, qualificandosi quindi come operatori monopolistici ognuno nella propria fetta di mercato, è anche vero che l'imperativo dell'estrazione dei dati guida la loro attività economica, a prescindere dai servizi effettivamente offerti, come una sorta di minimo comune denominatore. La competizione tra i GAFAM si sposta dall'offerta di beni e servizi alla corsa all'estrazione dei dati: non sono dunque mancate letture che guardano al mercato dei dati come un mercato a sé stante, unico, dominato dagli oligopoli di GAFAM.¹²²

1.4. Fuori dalla Silicon Valley

¹¹⁸ Ibidem.

¹¹⁹ Ibidem.

¹²⁰ Ibidem.

¹²¹ Ibidem, p.72.

¹²² Ibidem, p.158.

1.4.1 Internet of Things

Secondo Shoshana Zuboff,¹²³ i capitalisti della sorveglianza hanno compreso fin da subito l'importanza di ricercare una diversificazione delle fonti da cui estrarre surplus comportamentale. *In primis*, hanno scelto di implementare delle economie di scopo, partendo dall'intuizione per cui il surplus comportamentale necessita di varietà. Questa varietà può essere raggiunta tramite un'estensione delle logiche di estrazione al mondo reale, fuori dal mondo online. Inoltre, risulta necessario indagare anche la profondità, ovvero la personalità e l'intimità degli utenti. Zuboff ritiene che siano state anche implementate delle scelte strategiche che chiama «*economie di azione*»¹²⁴: l'intelligenza artificiale inizia a guadagnare terreno anche nel mondo reale, tangibile, tra le cose e le persone, per rendere le tecniche di condizionamento già esistenti ancora più raffinate e specifiche. Tutto ciò ha portato allo sviluppo dell'*Internet of Things* (IoT), ovvero «Internet delle cose».¹²⁵

Fornire una definizione unica di IoT risulta particolarmente complesso, dal momento che non si registra ancora una definizione legislativa del fenomeno né a livello europeo¹²⁶, né a livello statunitense. Volendo cercare una definizione quanto più possibile chiara, si potrebbe porre l'accento sul fatto che le tecnologie appartenenti al mondo dell'IoT operano grazie ad una serie di sensori in grado di trasformare gli oggetti in *smart objects*. Questi sensori sono in grado di captare, come i capitalisti della sorveglianza desiderano, la realtà circostante, dalla quale si ricavano tutta una serie di dati, tra cui anche *Big Data*. Si formano così degli «*smart objects*» interconnessi tra loro e in grado di scambiarsi i dati raccolti.¹²⁷

Non è mancato chi ha voluto inquadrare il fenomeno diversamente, ribaltando il concetto in «*Things on the Internet*». Le tecnologie utilizzate, infatti, sono in grado di influenzare la realtà materiale spostando «*the bulk of internet communication from*

¹²³Per approfondire, si v. S. Zuboff, «Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri», p. 211 e ss.

¹²⁴ Ibidem, p. 313.

¹²⁵ Per un approfondimento in materia di Internet of Things, si v. G. Noto La Diega, «Internet of Things and the Law: Legal Strategies for Consumer-Centric Smart Technologies», Research in the Law of Emerging Technologies, London, Routledge, 2022.

¹²⁶ Come ad esempio esiste in materia di «dato personale» grazie all'articolo 4 del General Data Protection Regulation (GDPR).

¹²⁷ Gruppo di lavoro ex art. 29 Direttiva 95/46/CE, parere 8/2014 sui recenti sviluppi dell'internet degli oggetti: «*The concept of the Internet of Things (IoT) refers to an infrastructure in which billions of sensors embedded in common, everyday devices – “things” as such, or things linked to other objects or individuals – are designed to record, process, store and transfer data and, as they are associated with unique identifiers, interact with other devices or systems using networking capabilities. As the IoT relies on the principle of the extensive processing of data through these sensors that are designed to communicate unobtrusively and exchange data in a seamless way, it is closely linked to the notions of “pervasive” and “ubiquitous” computing.*

Il parere è consultabile al link:

https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_it.pdf.

*human-human communication mediated by computers*¹²⁸, *to computer-computer communication mediated by humans*».¹²⁹

L'esempio delle *smart home*¹³⁰ gioverà alla comprensione del fenomeno. In una *smart home* i dispositivi sono in grado di comunicare tra loro grazie alla connessione Internet ed è possibile la loro gestione tramite apposite applicazioni su smartphone e tablet o tramite gli assistenti vocali. Essa rappresenta l'evoluzione della domotica, in cui invece l'interconnessione avviene con modalità fisiche.¹³¹ All'interno di una *smart home*, dunque, devono coesistere tutta una serie di *smart objects*. A titolo esemplificativo, si pensi ad un'aspirapolvere in grado di funzionare da sola, creando una piantina degli ambienti entro i quali muoversi, oppure ad un materasso dotato di particolari sensori che monitorano respiro, battito cardiaco e qualità del sonno,¹³² o a termostati controllabili a distanza tramite apposite applicazioni, che adattano la temperatura dell'abitazione a seconda che vi sia o meno qualcuno all'interno. Ancora, alcuni *smart objects* possono aumentare il livello di sicurezza, controllando eventuali fughe di gas o rilevando la presenza di monossido di carbonio. Celeberrimi, poi, sono gli *smart objects* Alexa e Google Assistant, qualificabili come una tecnologia di *smart personal assistance*, tramite i quali è possibile impartire a distanza tutta una serie di comandi, come spegnere la luce o segnare la lista della spesa.

Secondo Zuboff, il passaggio dall'esperienza captata dai sensori ai dati può essere chiamato «*renderizzazione*».¹³³ La parola deriva da *render*, un termine dotato di un duplice significato: significa tanto il processo di trasformazione di una cosa in un'altra, quanto il modo in cui «*la cosa che cambia si sottopone a tale processo: tramite la resa*».¹³⁴

*«Il capitalismo della sorveglianza deve occuparsi di entrambi i termini dell'equazione. Da un lato, le sue tecnologie sono pensate per renderizzare la nostra esperienza e tradurla in dati, come dal grasso si ricava l'olio; (...) Dall'altro, ogni volta che incontriamo un'interfaccia digitale rendiamo la nostra esperienza disponibile alla "datificazione", per "renderizzare a beneficio del capitalismo della sorveglianza" il suo perenne tributo di materie prime».*¹³⁵

¹²⁸ Per un approfondimento circa il concetto di «*computer mediated transaction*» di Val Harian si veda il paragrafo successivo.

¹²⁹ R. Mortier, «Explainer: The Internet of Things», The Conversation, 2 August 2013.

¹³⁰ Per «*smart home*» si intende: «*home embedded with information and communication infrastructure that collaborates to the need of the home occupants*», per un approfondimento, si v. B. Abba, M. Sulaiman, N. Mustapha, T. Perumal, «HMM-Based Decision Model for Smart Home Environment», International Journal of Smart Home, Gennaio 2014, consultabile al seguente link: https://www.researchgate.net/publication/284351676_HMM-.

¹³¹ G. Salvadori, «Smart Home: significato, mercato, applicazioni della casa intelligente», 4 gennaio 2020, https://blog.osservatori.net/it_it/smart-home-italia-significato.

¹³² Particolari criticità si rilevano con riferimento a questo tipo di informazioni, che è possibile descrivere come «*categorie particolari di dati*» ex articolo 9 GDPR. Un'analisi più dettagliata con riferimento a questi ultimi sarà fatta al capitolo III del presente lavoro.

¹³³ S. Zuboff, «Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri» p. 247.

¹³⁴ Ibidem, p. 248.

¹³⁵ Ibidem.

Le aziende che producono e commercializzano questi *smart objects* sono in grado di estrarre e renderizzare un grandissimo quantitativo di surplus comportamentale dalle singole interazioni che l'utente ha con gli stessi.

Quando gli *smart objects* sono prodotti e commercializzati da operatori dell'universo GAFAM stesso, è chiaro che il capitalismo della sorveglianza operi indisturbato. Quando però tali prodotti vengono commercializzati da soggetti al di fuori della Silicon Valley, il punto di svolta è rappresentato dal fatto che questi non negano di vendere i dati ricavati agli operatori GAFAM. Le fitte privacy policy, infatti, descrivono (più o meno) chiaramente l'attività che viene svolta a partire dai dati personali raccolti dagli *smart objects*: condivisione con terzi, spesso aziende del capitalismo della sorveglianza, pubblicità mirate.¹³⁶

Dette privacy policy, inoltre, mettono gli utenti davanti ad una (non) scelta: possono acconsentire all'utilizzo dei dati prodotti dall'interazione con gli *smart objects* predeterminati, o possono non farlo, perdendo però gran parte delle funzionalità degli *smart objects* stessi.¹³⁷

Secondo Zuboff, l'utilizzo dell'aggettivo «*smart*» altro non sarebbe che un eufemismo per celare l'attività di renderizzazione che viene compiuta: ogni oggetto è «una sorta di marionetta, un povero pupazzo che balla seguendo gli imperativi economici del suo burattinaio».¹³⁸

1.4.2 Possibili applicazioni future: il mercato assicurativo

Per descrivere le nuove frontiere di estrazione di surplus comportamentale, Shoshana Zuboff muove dall'analisi di Hal Varian, già *chief economist* di Google, che si esprime sull'utilizzo attuale dei computer.

Secondo Varian¹³⁹, infatti, i computer sono nati come veri e propri calcolatori, finalizzati ad attività di contabilità, ma oggi vengono ampiamente utilizzati per altre operazioni, tant'è che esistono innumerevoli transazioni che sono mediate da un computer (*computer-mediated transactions*). Varian guarda con particolare entusiasmo questo fenomeno, dal momento che ritiene possibile osservare comportamenti in precedenza non osservabili e utilizzarli come base per stilare dei contratti.

Il mondo delle compagnie assicurative potrebbe ampiamente giovare da queste nuove logiche di economie di scopo e di azione implementate dai capitalisti della sorveglianza, in particolar modo dalla nuova possibilità - descritta da Varian - di implementare nuove forme contrattuali più convenienti.

Si pensi al fatto che, nella loro attività di calcolo dei premi, le compagnie assicurative sono costrette ad utilizzare parametri variabili tradizionali per il calcolo del rischio, senza che tuttavia questi parametri forniscano con certezza mezzi per la massimizzazione del profitto.

¹³⁶ Ibidem, p. 250.

¹³⁷ Ibidem, p. 252.

¹³⁸ Ibidem.

¹³⁹ Si v. H. R. Varian, «Beyond Big Data», *Business Economics* 49, fasc. 1, gennaio 2014, pp. 27-31, <https://doi.org/10.1057/be.2014.1>.

Questo orizzonte varia nel momento in cui vengono invece implementate delle *smart cars*: attraverso i sensori possono essere trasmesse alla compagnia assicurativa centinaia di migliaia di dati, come ad esempio l'uso della cintura di sicurezza, la velocità media, accelerazioni e frenate brusche, ma in generale conversazioni del conducente e, più in generale, il suo comportamento alla guida o la sua attitudine al rischio.¹⁴⁰

Grazie a questi dati, le compagnie assicurative potrebbero implementare polizze assicurative costruite su misura per il singolo cliente, riducendo l'incertezza fisiologica dell'attività assicurativa. Il rischio, dunque, potrebbe non essere più omogeneamente spalmato tra la pluralità degli assicurati, ma diventerebbe gestito in maniera individuale. L'incertezza della vita quotidiana, ad oggi inevitabile, verrebbe superata grazie ad un ingente quantitativo di dati che permette di calcolare in termini vicini alla certezza il rischio di un sinistro stradale, classificando il conducente in base ai dati prodotti mentre è alla guida. Ciò permetterebbe di ottimizzare il prezzo delle assicurazioni e garantire il successo commerciale, si spiega dunque in questi termini il motivo per cui i fornitori di beni e servizi lontani dalla Silicon Valley guardano con entusiasmo al capitalismo della sorveglianza.¹⁴¹

1.5 Alcune considerazioni critiche

1.5.1 *Data-driven economy* e mercificazione della persona

Si è visto come gli individui siano diventati un mezzo per uno scopo, la fonte di approvvigionamento della materia prima, il surplus comportamentale, da cui si ricavano prodotti predittivi, poi scambiati all'interno del mercato dei comportamenti futuri. Se in un primo momento l'imperativo del surplus dell'estrazione si fermava alle attività *online*, ben presto si è intuita l'enorme potenzialità di acquisire informazioni anche dalle attività *offline*. Il surplus comportamentale, scoperto in California e nella Silicon Valley, ha presto guidato le scelte imprenditoriali di operatori estranei alla Bay Area. La progressiva opera di digitalizzazione e datizzazione della realtà empirica ha permesso la registrazione di un enorme quantitativo di dati che ha inaugurato nuove prospettive.

Il sistema economico che ne è risultato viene descritto come *data-driven economy*, vale a dire economia basata sui dati. Per comprendere il valore che i *Big Data* ricoprono nell'attuale economia, basti pensare che è stato stimato che il loro potenziale economico è di circa un dollaro per persona al giorno.¹⁴² Ma al di là di questa suggestiva immagine, il vero valore dei dati è insito nella loro possibilità di essere utilizzati come una fonte di produzione di conoscenza e, in ultima istanza, come fonte di nuovo profitto.

Una delle idee più promettenti di questa epoca è l'idea di poter utilizzare i dati in maniera *smart*, ovvero utilizzare i dati come motore per l'innovazione stessa, in ottica

¹⁴⁰ Ibidem.

¹⁴¹ Per approfondire, si v. S. Zuboff, «Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri», capitolo VIII, IX.

¹⁴² G. Resta, Z. Zencovich, «Volontà e consenso nella fruizione dei servizi di Rete», in Riv. trim. dir. e proc. civ., 2018, 2, pp. 411-440, p. 416, che richiamano la stima di G. Malgieri e B. Custers, «Pricing Privacy: The Right to Know the Value of Your Personal Data», Computer Law & Security Review, 2018, <https://ssrn.com/abstract=3047257>.

di favorire lo sviluppo economico e sociale.¹⁴³ L'idea di fondo è quella di adottare «*un approccio sistematico e metodologico capace di garantire la trasformazione di dati in innovazione*». ¹⁴⁴ Il fenomeno prende il nome di Data-Driven Innovation e incontra il favore anche dell'Organizzazione per la Cooperazione e lo Sviluppo Economico che, nel rapporto finale «*Data Driven Innovation: Big Data for Growth and Well-Being*» dell'ottobre del 2015 lo definisce come «*the use of data and analytics to improve or foster new product, processes organizational, methods and market*». ¹⁴⁵

Se è vero che i *Big Data* sono il nuovo petrolio¹⁴⁶, è anche vero che, così come il petrolio, producono effetti inquinanti che si declinano non solo nell'intrusione nella vita privata, ma anche in una vera e propria mercificazione della persona.¹⁴⁷ In questo procedimento, le persone sono materia prima, ma sono anche oggetto del processo di datizzazione, e sono in ultima istanza poi oggetto di mercificazione quando datificate.¹⁴⁸

«*La mercificazione è un processo di riduzione di un'entità – lavoro, terra, moneta, conoscenza, persona – al concetto di merce*». ¹⁴⁹ Già nel 1974 lo storico, antropologo ed economista unghese Karl Polanyi¹⁵⁰ aveva ricostruito il fenomeno in prospettiva critica:

«Un'economia di mercato deve comprendere tutti gli elementi dell'industria compreso il lavoro, la terra e la moneta. (In un'economia di mercato anche quest'ultima è un elemento essenziale della vita industriale e la sua inclusione nel meccanismo di mercato ha [...] conseguenze istituzionali di lunga portata). Lavoro e terra tuttavia non sono altro che gli esseri umani stessi dai quali è costituita ogni società e l'ambiente naturale nel quale essa esiste. Includerli nel meccanismo di mercato significa subordinare la sostanza della società stessa alle leggi di mercato [...]».

Secondo Polanyi, lavoro, terra e moneta sono organizzati in mercati, quindi vengono equiparati alla merce, pur non essendolo, infatti:

«Il lavoro è soltanto un altro nome per un'attività umana che si accompagna alla vita stessa la quale a sua volta non è prodotta per essere venduta ma per ragioni del tutto diverse, né questo tipo di attività può essere distaccato dal resto della vita, essere accumulato o mobilitato. La terra è soltanto un altro nome per la natura che non è prodotta dall'uomo, la moneta infine è soltanto un simbolo del potere d'acquisto che di regola non è affatto prodotto ma si sviluppa attraverso il meccanismo della banca o della finanza di stato. La descrizione, quindi, del lavoro, della terra e della moneta come merce è

¹⁴³ A. Stazi, F. Corrado «Datificazione dei rapporti socio-economici e questioni giudicizie: profili evolutivi in prospettiva comparatistica», 2019.

¹⁴⁴ Ibidem, p. 448.

¹⁴⁵ Si v. OECD, Data Driven Innovation, big data for growth and well-being, OECD publishing, Paris 2015, consultabile al link:

<https://www.oecd.org/sti/data-driven-innovation-9789264229358-en.htm>.

¹⁴⁶ The Economist, «The world's most valuable resource is no longer oil, but data».

¹⁴⁷ I. Speziale, «L'ingresso dei dati nella prospettiva causale dello scambio: i modelli contrattuali di circolazione», Contratto e impresa, febbraio 2021, pp. 602-629.

¹⁴⁸ R. Caso, «La società della mercificazione e della sorveglianza: dalla persona ai dati», p.337.

¹⁴⁹ Ibidem, p. 337.

¹⁵⁰ K. Polanyi, «La grande trasformazione. Le origini economiche e politiche della nostra epoca», Torino, Einaudi, 1974, p.92-94.

*interamente fittizia. [...]Permettere al meccanismo di mercato di essere l'unico elemento direttivo del destino degli esseri umani e del loro ambiente naturale e perfino della quantità e dell'impiego del potere di acquisto porterebbe alla demolizione della società».*¹⁵¹

Si tratta di concetti in qualche modo condivisi anche da Shoshana Zuboff quando specifica che:

*«Il capitalismo della sorveglianza non ha confini e ignora le vecchie distinzioni tra mercato e società, tra mercato e mondo, tra mercato e persona. Agisce a scopo di lucro subordinando la produzione all'estrazione [dei dati relativi all'esperienza umana], rivendicando il controllo esclusivo di umanità, società e politica, andando ben oltre l'ambito convenzionale di un'azienda o del mercato. Rifacendoci a Karl Polanyi, possiamo vedere che il capitalismo della sorveglianza annette l'esperienza umana alle dinamiche di mercato per farle rinascere come comportamento: il quarto «bene fittizio». I primi tre beni fittizi di Polanyi – terra, lavoro e denaro – erano soggetti alla legge. Anche se imperfette, le leggi sul lavoro, sull'ambiente e sulle banche costituiscono delle cornici di regole per difendere la società (così come la natura, la vita e la finanza) dagli eccessi peggiori del capitalismo. L'esproprio dell'esperienza umana da parte del capitalismo della sorveglianza non ha incontrato ostacoli simili».*¹⁵²

La tendenza di mettere al centro i dati è stata brillantemente descritta dallo storico israeliano Yuval Noah Harari come la religione del «datismo»:

*«La religione dei dati ora dice che ogni parola e ogni azione è parte del grandioso flusso dei dati, che gli algoritmi vi stanno guardando costantemente e che essi si preoccupano di qualsiasi cosa facciate e di qualsiasi sentimento proviate. Alla maggior parte delle persone questo piace parecchio. Per i veri credenti, essere disconnessi dal flusso dei dati comporta il rischio di perdere il vero significato della vita. Che senso ha fare o sperimentare qualsiasi cosa se nessuno ne è al corrente, e se ciò non contribuisce in qualche maniera allo scambio globale di informazioni?».*¹⁵³

Secondo Harari, il datismo si origina dall'informatica e la biologia, ma è l'incontro con quest'ultima ad aver segnato la creazione di un nuovo dogma scientifico per cui tutti gli esseri viventi possono essere visti come algoritmi, e la differenza tra specie altro non è che il frutto di diversi metodi per elaborare i dati¹⁵⁴:

«L'umanesimo ritiene che le esperienze accadano dentro di noi, e che proprio lì dovremmo trovare il significato di tutto quello che accade, permeando in tal modo l'universo di significato. I datisti credono che le esperienze siano senza valore se non sono condivise, e che non abbiamo bisogno di – in effetti non possiamo – trovare il significato in noi stessi. Abbiamo soltanto bisogno

¹⁵¹ Ibidem.

¹⁵² S. Zuboff, «Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri», p. 529.

¹⁵³ Y.N. Harari, «Homo deus. Breve storia del futuro», Firenze-Milano, Giunti- Bompiani, 2017, p. 587.

¹⁵⁴ Ibidem.

*di registrare e connettere le nostre esperienze al grande flusso dei dati, e gli algoritmi scopriranno il loro significato e ci diranno come agire».*¹⁵⁵

La riduzione della persona in un insieme di dati, inoltre, comporta una trasformazione da una *natural person* ad una *digital person*. All'interno della digital person, si crea però una *transaction identity* che riflette le abitudini economiche delle sue attività online e che pone nuove criticità e nuovi interrogativi con riferimento alla tutela dell'identità personale.¹⁵⁶

Secondo Rodotà, «è nata una nuova concezione integrale della persona, alla cui proiezione nel mondo corrisponde il diritto al pieno rispetto di un corpo che ormai è, al tempo stesso, "fisico" ed "elettronico"» e, così come l'integrità fisica è protetta dall'*habeas corpus*, la persona digitale, secondo Rodotà, deve essere protetta tramite l'*habeas data*, che deve proteggere l'immagine in cui il soggetto si riconosce e con cui si proietta all'esterno, in ossequio al diritto alla dignità e all'autodeterminazione.¹⁵⁷

1.5.2 Rischi per gli utenti come consumatori: cenni

Come illustrato da Karen Yeung,¹⁵⁸ gli utenti delle piattaforme, dell'IoT e di ogni nuova economia di azione implementata dal capitalismo della sorveglianza possono essere qualificati anche come consumatori.

Grazie alla capacità di personalizzazione di massa sembrerebbe possibile il raggiungimento di un obiettivo a lungo desiderato: dividere i consumatori in veri e propri gruppi affinché si conosca effettivamente chi è interessato a un determinato prodotto e chi non lo è. L'obiettivo ultimo, secondo Yeung, è quello immaginare ogni singolo utente come un mercato a sé in base al quale implementare offerta, prezzi e strategie di mercato. Questa possibilità gioverebbe anche al consumatore stesso, che sarebbe finalmente libero da eventuali offerte o iniziative pubblicitarie indesiderate.

Tuttavia, segnala sapientemente Yeung, dietro questa parvenza di efficienza tanto per i produttori di beni e servizi quanto per i consumatori, si celano delle criticità per questi ultimi.

In primo luogo, le tecniche di personalizzazione si basano sulla possibilità di conoscere preferenze, abitudini e vulnerabilità degli utenti, esacerbando il problema dell'asimmetria di potere esistente tra produttori e consumatori: i capitalisti della sorveglianza raccolgono un numero sempre maggiore di informazioni sui consumatori, senza che questi abbiano accesso alle informazioni raccolte o alle pratiche implementate. Dal punto di vista dei diritti del consumatore, questa asimmetria si declina nell'implementazione, da parte dei capitalisti della sorveglianza, di una strategia

¹⁵⁵ Ibidem, p. 588.

¹⁵⁶ Si v. P.G. Alpa «L'identità digitale e la tutela della persona. Spunti di riflessione», *Contratto e impresa*, 3/2017, p. 723-727.

¹⁵⁷ S. Rodotà, Discorso conclusivo della 26esima Conferenza internazionale sulla protezione dei dati, settembre 2004, consultabile al link: <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1049293>.

¹⁵⁸ Si v. K. Yeung, «Five Fears about Mass Predictive Personalization in an Age of Surveillance Capitalism», *International Data Privacy Law*, 2018. <http://dx.doi.org/10.2139/ssrn.3266800>.

di «*divide et impera*». ¹⁵⁹ La personalizzazione, infatti, riesce a isolare il singolo consumatore, ledendo in concreto le possibilità che i consumatori agiscano come gruppo per ribellarsi alle attività di monitoraggio e condizionamento implementate. ¹⁶⁰

La tecnica della personalizzazione, inoltre, è utile anche per attuare una politica di personalizzazione dei prezzi. Attraverso l'analisi dei dati raccolti è possibile conoscere il prezzo che il singolo consumatore è disposto a pagare, pertanto si realizza la possibilità di differenziare la somma per ogni consumatore, portando a una massimizzazione del profitto per il produttore di un bene o un servizio. Questo tipo di discriminazione di prezzo individuale, sottolinea Yeung, potrebbe comportare uno svantaggio sistematico per quel particolare gruppo di consumatori caratterizzato da una scarsa alfabetizzazione digitale. I soggetti appartenenti a questo gruppo, spesso, non riescono ad informarsi circa la diversificazione dell'offerta e si caratterizzano per una domanda inelastica, ovvero poco influenzata da eventuali aumenti di prezzo. Per questi motivi, questo gruppo di consumatori rischia di essere a lungo svantaggiato poiché destinatario di prezzi sistematicamente più alti rispetto a quelli praticati nei confronti di soggetti con un grado di alfabetizzazione digitale maggiore, in grado di valutare meglio le diverse offerte sul web. ¹⁶¹

La scienza economica ha conosciuto un periodo di difficoltà legato al venir meno di stabilità delle categorie tradizionali sulla base delle quali differenziare l'offerta (come, ad esempio, la differenziazione in base di sesso, età, religione), ma l'utilizzo dei dati personali e dei sistemi tipici del capitalismo della sorveglianza sembrano aver risolto questo problema. Lo sviluppo di tecnologie innovative di intelligenza artificiale e di *machine learning* sulla base dei dati raccolti ha permesso ai produttori di beni e servizi di sviluppare strategie molto efficaci di segmentazione dei clienti in gruppi, permettendo una sempre più accurata scelta di presentazione e offerta di beni e servizi, evitando invece la proposta di elementi indesiderati. Tramite queste tecnologie, i consumatori sono accuratamente selezionati, messi in ordine in base a criteri specifici, e valutati in base alla loro compatibilità con gli algoritmi di intelligenza artificiale. ¹⁶²

Questo sistema giova a quel gruppo di consumatori che risponde alla logica dell'algoritmo sottostante ai modelli di previsione. Tutti gli altri consumatori che, invece, vengono considerati come «*low volume*», perché non rispondono alle logiche dell'algoritmo, rischiando così di essere vittima di un sistema che li esclude da tutta una serie di particolari offerte o proposte che potrebbero implementare il loro benessere generale. ¹⁶³

Vi è il rischio che i consumatori «*low volume*» siano sistematicamente ignorati, esacerbando le disparità sociali già esistenti. Nello specifico, sarebbe addirittura possibile escludere in maniera irreversibile tutta una serie di consumatori dall'offerta di beni e servizi, senza che questi ne siano a conoscenza. Per illustrare il fenomeno, Yeung

¹⁵⁹ Ibidem, p.261.

¹⁶⁰ Ibidem.

¹⁶¹ Ibidem.

¹⁶² Si v. N. Draper and J. Turow, «Audience Constructions, Reputations and Emerging Media Technologies: New Issues of Legal and Social Policy» in R. Brownsword, E. Scotford, K. Yeung (eds), *The Oxford Handbook of Law, Regulation and Technology*, Oxford University Press 2017, pp. 1143–67.

¹⁶³ K. Yeung, «Five Fears about Mass Predictive Personalization in an Age of Surveillance Capitalism», p. 264.

riporta l'esempio di celeberrime catene di supermercati alimentari che applicano la segmentazione della clientela. Se è vero che esistono supermercati rivolti ad una clientela abbiente ed altri rivolti a una clientela con un reddito inferiore, nulla si oppone alla possibilità che un cliente con minori disponibilità economiche acquisti occasionalmente prodotti dal supermercato pensato per una clientela benestante e viceversa. Nel mondo digitale, invece, il consumatore è in grado di vedere e conoscere solamente il prezzo che viene praticato nei suoi confronti, senza avere la possibilità di conoscere i prezzi praticati con gli altri consumatori.¹⁶⁴

1.5.3 La manipolazione degli utenti

Secondo Zuboff,¹⁶⁵ le nuove economie di azione non si limitano solamente a collezionare *Big Data* tramite i sensori e processarli tramite IA per fini pubblicitari. La nuova frontiera del capitalismo della sorveglianza, avverte Zuboff, è quella di «*modificare le azioni in tempo reale nel mondo reale*».¹⁶⁶

Questo processo avviene tramite tre approcci: *tuning*, *herding*, e *condizionamento*.

Per quanto riguarda il *tuning*, esso opera su quella che viene chiamata «*architettura della scelta*».¹⁶⁷ Nello specifico, queste architetture sono progettate in un certo modo proprio per ottenere un comportamento specifico; l'esempio tradizionale quello delle sedie di un'aula scolastica rivolte verso la cattedra per condizionare l'attenzione, ma si tratta comunque di *tuning* tutte quelle volte in cui un sito non permette di disattivare i *cookies* senza cliccare su tante pagine redatte in modo poco chiaro.¹⁶⁸ Il *tuning* è ricondotto anche a tutta quella serie di «*nudging techniques*»¹⁶⁹, ovvero «tecniche di spintarella gentile» che, tramite la profilazione sulla base dei dati, permettono la riconfigurazione in tempo reale dell'architettura della scelta.

Se da un lato il marketing ha iniziato a perseguire gli stessi obiettivi ancor prima della rivoluzione digitale, va sottolineato che le attività di manipolazione degli utenti perseguita dai capitalisti della sorveglianza si presenta come particolarmente pervasiva, dal momento che non è più basata su assunzioni prettamente convenzionali di preferenze, ma utilizza dati, algoritmi e intelligenza artificiale con cui è possibile dedurre con certezza le preferenze e le inclinazioni degli utenti per modificare l'architettura della scelta.¹⁷⁰

L'*herding*, invece, permette il controllo sugli elementi chiave di un determinato contesto. Con l'*herding* è possibile eliminare determinate azioni alternative per spostare il comportamento verso un diverso percorso. Un esempio – estremizzato – di *herding*, potrebbe essere quello di decidere di chiudere un frigorifero poiché, tramite l'analisi dei

¹⁶⁴ Ibidem, p. 265.

¹⁶⁵ S. Zuboff, «Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri», capitolo X, p. 309 e ss.

¹⁶⁶ Ibidem, p. 309.

¹⁶⁷ R.H. Thaler, C. R. Sustain, «Nudge: Improving Decision About Health, Wealth and Happiness», Penugin, New York 2009.

¹⁶⁸ S. Zuboff, «Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri», p. 309.

¹⁶⁹ K. Yeung, «Five Fears about Mass Predictive Personalization in an Age of Surveillance Capitalism», p. 263.

¹⁷⁰ Ibidem.

dati, si ritiene che quel soggetto non abbia bisogno in quel determinato momento di mangiare.¹⁷¹

Il *condizionamento*, invece, si basa sul concetto di «rinforzo», ovvero premi, ricompense, riconoscimenti o complimenti, tramite i quali è possibile influenzare un soggetto a ripetere quel determinato comportamento elogiato.¹⁷² Si pensi ad un'applicazione per smartphone che fornisce premi in denaro di pochi centesimi per ogni kilometro camminato: il soggetto, vittima del meccanismo premiale, sarà condizionato a camminare più a lungo.

Non bisogna credere che questo meccanismo sia tutto a vantaggio del consumatore, il modello di reinvestimento del surplus comportamentale è passato, i capitalisti sono diventati capitalisti della sorveglianza. Questi hanno ormai il potere di modificare il comportamento altrui con mezzi che mettono seriamente in discussione l'autonomia umana e il diritto all'autodeterminazione.¹⁷³

I capitalisti della sorveglianza mettono in atto una sorta di profilazione predittiva: tramite le informazioni raccolte, il servizio offerto è configurato automaticamente, senza che l'utente lo abbia mai richiesto. La necessità di quel determinato servizio viene dedotta con una probabilità vicina alla certezza grazie all'IA e il comportamento dell'utente viene manipolato affinché ne usufruisca. Gli algoritmi che permettono questa manipolazione non rispondono agli interessi dell'utente, ma a quelli di massimizzazione del profitto dei capitalisti della sorveglianza.¹⁷⁴

1.5.4 I rischi per la democrazia: il caso *Cambridge Analytica*

Nella prospettiva della manipolazione del comportamento umano, il controllo del tipo di informazioni che vengono condivise e mostrate agli utenti gioca un ruolo fondamentale.¹⁷⁵ Tramite le tecniche di profilazione già descritte, i capitalisti della sorveglianza sono in grado di mostrare agli utenti solo il tipo di informazioni che si rivelano come compatibili con i loro interessi, ma anche con i loro pregiudizi. L'utente, dunque, si trova in una vera e propria «*filter bubble*»¹⁷⁶ dalla quale sfugge ogni possibilità di confronto tra opinioni e conoscenza. All'interno di questa bolla si crea una sorta di «*identità esterna*», la cui costruzione non è più esclusivo appannaggio del soggetto ma frutto di una subdola manipolazione da parte di soggetti terzi.¹⁷⁷ Il venir meno della possibilità di confronto e dialogo in forza di un'accurata canalizzazione di informazioni mostrate rappresenta, in ultima istanza, un rischio per la democrazia

¹⁷¹ S. Zuboff, «Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri», p.311.

¹⁷² Ibidem, p. 312.

¹⁷³ Ibidem, p.135.

¹⁷⁴ Si v. K.Yeung, «Five Fears about Mass Predictive Personalization in an Age of Surveillance Capitalism».

¹⁷⁵ Si v. A. Astone, «Capitalism of Digital Surveillance and Digital Disintermediation in the Era of the Pandemic», *European Journal of Privacy Law & Technologies* 2020, fasc. 2,2020, pp. 163-171, <https://universitypress.unisob.na.it/ojs/index.php/ejplt/article/view/1215>.

¹⁷⁶ Si v. M. Bianca, «La filter bubble e il problema dell'identità digitale», *MediaLaws. Riv. dir. media*, 2, 2019, pp. 39-53.

¹⁷⁷ A. Astone, «Capitalism of Digital Surveillance and Digital Disintermediation in the Era of the Pandemic», p.168.

stessa.¹⁷⁸ La democrazia, infatti, funziona solo se è possibile un dibattito tra diverse opinioni minoritarie.¹⁷⁹

Tra i rischi legati al capitalismo della sorveglianza, quello che riguarda la tutela della democrazia è divenuto celebre alla luce dello scandalo che ha colpito le elezioni presidenziali statunitensi del 2016 e il referendum sull'uscita dall'Unione europea del Regno Unito.

Al centro dello scandalo, emerso nel 2018, vi è la società di consulenza inglese *Cambridge Analytica*, particolarmente vicina al partito repubblicano statunitense, che è riuscita ad acquisire i dati di approssimativamente 87 milioni di utenti Facebook tramite un'applicazione chiamata «*This is Your Digital Life*», in grado di costruire dei veri e propri profili psicologici degli utenti. L'app funzionava come un vero e proprio questionario di psicologia, a cui era possibile rispondere solamente dopo aver concesso l'accesso al proprio profilo Facebook, da cui venivano poi raccolti i dati non solo dell'utente, ma anche di tutti i collegamenti, noti come «amici», di chi effettuava il test.¹⁸⁰

I dati così raccolti venivano poi utilizzati per implementare una campagna elettorale efficace: in particolar modo, una volta conosciute le convinzioni politiche e preferenze, era possibile mostrare a ogni utente informazioni capaci di influenzare le scelte elettorali. L'utilità di questa tecnica di manipolazione si coglie in tutta la sua pervasività con riferimento agli *swing voters*, ovvero quegli elettori non legati a nessun tipo di partito, che possono essere persuasi a votare in diversi sensi.¹⁸¹ Tramite i dati personali è possibile conoscere le inclinazioni degli elettori, e successivamente trasmettere loro informazioni in grado di stimolare un'introspezione che li guidi verso un voto preciso, che all'esito risulterà non pienamente libero.

Nonostante le criticità sottolineate, Facebook – ora parte dell'universo Meta – non sembra essere stato troppo impattato dallo scandalo di *Cambridge Analytica*. È stato infatti osservato¹⁸² che il prezzo delle azioni ha subito una diminuzione solamente nel breve periodo, mentre nel lungo periodo, complice anche la pandemia da Covid-19, il prezzo delle azioni di Facebook è ritornato al valore iniziale.¹⁸³

I rischi per l'autodeterminazione e la democrazia non hanno spaventato gli utenti, che, seppur insoddisfatti dell'uso che veniva fatto dei loro dati, hanno ritenuto che i benefici dell'utilizzo di Facebook superassero i costi legati alla loro libertà di scelta.

¹⁷⁸ Ibidem.

¹⁷⁹ V. Boehme-Neßler, «Privacy: A Matter of Democracy. Why Democracy Needs Privacy and Data Protection», *International Data Privacy Law* 6, fasc. 3, agosto 2016, pp. 222-229, p.266 <https://doi.org/10.1093/idpl/ipw007>.

¹⁸⁰ Per un approfondimento sugli eventi, si v. N. Confessore, «Cambridge Analytica and Facebook: The Scandal and the Fallout So Far (Published 2018)», *The New York Times*, 4 aprile 2018, <https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html>.

¹⁸¹ C. Cadwalladr, E. Graham-Harrison, «Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach», *The Guardian*, 17 marzo 2018, sez. News, <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>.

¹⁸² Si v. Conyon, M.J. «Big Technology and Data Privacy», *Cambridge Journal of Economics* 46, 2022, pp. 1369–1385.

<https://doi.org/10.1093/cje/beac052>.

¹⁸³ Si v. sempre Conyon per un'analisi più approfondita sul valore delle azioni e su come altri *data breach* non abbiano mai impattato il valore di queste ultime.

Infatti, se nel 2017 vi erano circa due miliardi di utenti attivi su Facebook, nel 2022 questi sono diventati quasi tre miliardi.¹⁸⁴

Secondo Zuboff, il caso di Cambridge Analytica

*«racchiude tutto il progetto del capitalismo della sorveglianza e spiega la sua determinazione a renderizzare gli aspetti più profondi delle persone. [...] Cambridge Analytica ha semplicemente spostato la macchina dei soldi garantiti dalla macchina dei comportamenti futuri alla sfera politica. [...] Oltre a utilizzare i meccanismi di base del capitalismo della sorveglianza – renderizzazione, surplus comportamentale, intelligenza delle macchine, prodotti predittivi, economie di scala, di scopo e di azione – la tetra avventura di Cambridge Analytica ci mostra quali sono le esigenze tattiche di tale capitalismo. Le sue operazioni erano pensate per produrre ignoranza per mezzo della segretezza, eludendo attentamente la consapevolezza dell'individuo. [...] Indipendentemente dal reale impatto politico di Cambridge Analytica, i piani alla base delle sue ambizioni testimoniano il ruolo centrale della renderizzazione più profonda nella previsione e nella modifica del comportamento».*¹⁸⁵

1.6 La tutela dei dati personali

L'enorme quantitativo di dati estratto, analizzato e utilizzato per le finalità sopra illustrate da parte degli operatori del capitalismo della sorveglianza solleva numerose criticità in materia di tutela della privacy e, più nello specifico, dei dati personali. Nel presente paragrafo si ricostruirà brevemente la storia della tutela della privacy, partendo dall'esperienza statunitense e italiana fino a descrivere l'attuale atto normativo europeo in materia di protezione dei dati personali, ovvero il General Data Protection Regulation 2016/679 (d'ora in poi: GDPR).¹⁸⁶ Come si delinea nei paragrafi che seguono, la privacy, riservatezza nel diritto italiano, e il diritto alla protezione dei dati personali sono concetti tradizionalmente differenti. Tuttavia, non mancano voci in dottrina che tendono a utilizzare tali termini in maniera intercambiabile.

Nel presente lavoro si analizzeranno, nei capitoli successivi, i problemi relativi alla tutela dei dati personali con riferimento al capitalismo della sorveglianza, con particolare attenzione all'esperienza della didattica a distanza. Come verrà illustrato nei prossimi capitoli, infatti, il trattamento dei dati personali posto in essere dai grandi operatori del capitalismo della sorveglianza desta particolari criticità con riferimento alla compatibilità con la disciplina europea in materia.

Occorre sin da subito specificare che non tutti i dati raccolti dai capitalisti della sorveglianza sono dati personali, ovvero, ai sensi dell'articolo 4, n.1 del GDPR:

«qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che

¹⁸⁴ Ibidem, p. 1378.

¹⁸⁵ S. Zuboff, «Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri», p. 295-96.

¹⁸⁶ Regolamento (UE) del Parlamento europeo e del Consiglio, 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 (regolamento generale sulla protezione dei dati), consultabile al link: <https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32016R0679>.

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».

1.6.1 Excursus storico: la privacy negli USA e la riservatezza in Italia

L'innovazione tecnologica, in particolare la diffusione della stampa e l'invenzione della macchina fotografica portatile, portò alla diffusione di una peculiare cronaca giornalistica interessata alla vita privata dei membri della classe borghese, chiamata «*yellow journalism*», dal colore della carta dei giornali che si occupavano principalmente di gossip. Tale nuova tipologia di giornalismo, basata sul sensazionalismo, rispondeva alla curiosità di cittadini privati desiderosi di conoscere gli intimi dettagli della vita dei personaggi di spicco della borghesia¹⁸⁷.

Convenzionalmente, la creazione del concetto di tutela della privacy in ambito statunitense è attribuita al celeberrimo articolo «*The Right to Privacy*» redatto da Warren e Brandeis e pubblicato nel 1890 nella rivista giuridica *Harvard Law Review*. In questo articolo, la privacy viene descritta come «*the right to be let alone*».¹⁸⁸ Probabilmente, fu il fatto di essere in prima persona vittima di tali articoli scandalistici che spinse Samuel Warren alla riflessione sul diritto a essere lasciati soli. Warren, importante avvocato, aveva infatti sposato la figlia di un senatore del Delaware, guadagnandosi così l'attenzione non gradita della stampa.¹⁸⁹

Mancando una tutela costituzionale, i due autori cercarono all'interno delle norme già esistenti un fondamento per il nuovo diritto a essere lasciati soli. Particolarmente utile si rivelò la disciplina in materia di diritto d'autore prevista dal common law, più nello specifico il diritto di inedito. Il ragionamento di Warren e Brandeis è di tipo analogico: così come il diritto di inedito permette di scegliere se, e in che termini, pubblicare una propria opera dell'ingegno, allo stesso modo l'individuo dovrebbe essere libero di scegliere se condividere o meno informazioni sulla propria sfera privata.¹⁹⁰ I rimedi del common law, però, non erano idonei a prevenire la pubblicazione o la descrizione di un fatto privato e a dare ristoro al «*mental pain and distress*» provocati dalla pubblicazione di un fatto privato. Era pertanto necessario individuare un diverso principio, si legge infatti:

«These considerations lead to the conclusion that the protection afforded to thoughts, sentiments, and emotions, expressed through the medium of

¹⁸⁷ P. Guarda, G. Bincoletto, «Diritto comparato della privacy e della protezione dei dati personali», Zenodo, 2023, p.19.

<https://doi.org/10.5281/zenodo.7805085>.

¹⁸⁸ S. D. Warren, L. D. Brandeis, «The Right to Privacy», 4 *Harvard Law Review*, 1890, pp. 193-220.

¹⁸⁹ D. Solove, P.M. Schwartz, «Information Privacy Law», New York, 2021 Wolters Kluwer Law & Business, p. 12.

¹⁹⁰ «*Right to be let alone: (...) The common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others*» in S.D. Warren, L. D. Brandeis, «The Right to Privacy», p.198.

*writing or of the arts, so far as it consists in preventing publication, is merely an instance of the enforcement of the more general right of the individual to be let alone. It is like the right not to be assaulted or beaten, the right not to be imprisoned, the right not to be maliciously prosecuted, the right not to be defamed. In each of these rights, as indeed in all other rights recognized by the law, there inheres the quality of being owned or possessed – and (as that is the distinguishing attribute of property) there may be some propriety in speaking of those rights as property. But, obviously, they bear little resemblance to what is ordinarily comprehended under that term. The principle which protects personal writings and all other personal productions, not against theft and physical appropriation, but against publication in any form, is in reality not the principle of private property, but that of an inviolate personality».*¹⁹¹

Il fondamento del nuovo right to privacy veniva pertanto individuato nel principio di common law alla tutela di «*un'inviolata personalità*»¹⁹².

Tale diritto non era visto dagli autori come un diritto assoluto. In primo luogo, era comunque possibile la pubblicazione di fatti che, benché privati, fossero di interesse pubblico. Analogamente, se la pubblicazione di circostanze private fosse avvenuta nel rispetto delle norme in materia di calunnia e diffamazione, il diritto alla privacy non veniva violato. Il diritto alla privacy non era violato ogni qualvolta ci fosse stata la diffusione di una notizia previo consenso dell'individuo, oppure nel caso di divulgazione avvenuta a opera dello stesso protagonista dei fatti. I rimedi in caso di pubblicazione di notizie private che i due autori immaginavano erano un ristoro monetario, possibile solamente laddove si fosse patito uno «*special damage*», oppure una «*injunction*» finalizzata a impedire nuove offese.¹⁹³

L'evoluzione del diritto alla privacy e una sua più approfondita analisi si deve poi alla giurisprudenza della Corte Suprema, che individuò il diritto alla privacy come una protezione nei confronti di eventuali intrusioni governative non autorizzate. In particolare, la lettura congiunta del Primo¹⁹⁴ e del Quarto¹⁹⁵ Emendamento della Costituzione americana permise di riconoscere a questo diritto il rango di diritto costituzionalmente garantito.¹⁹⁶

Negli Stati Uniti, il diritto alla privacy assume una connotazione particolarmente pervasiva: viene infatti interpretato dalla Corte Suprema come diritto costituzionale

¹⁹¹ Ibidem, p.205.

¹⁹² P. Guarda, G. Bincoletto, «Diritto comparato della privacy e della protezione dei dati personali», p. 23.

¹⁹³ Ibidem, p. 22.

¹⁹⁴ «*Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances*».

¹⁹⁵ «*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*».

¹⁹⁶ Per un approfondimento, si v. P. Guarda, G. Bincoletto, «Diritto comparato della privacy e della protezione dei dati personali».

all'interno del quale far rientrare tutta una serie di diritti che, nell'orizzonte italiano ed europeo, definiremmo come diritti della personalità.¹⁹⁷

Nel 1977, anno della decisione *Whalen v. Roe* fu coniata l'espressione di «*informational privacy*»¹⁹⁸, che rende la privacy non solo un diritto al controllo sulle informazioni divulgate all'esterno, ma anche un diritto a compiere delle scelte personali sulle proprie informazioni.¹⁹⁹ Tuttavia, nel 2011, la Corte Suprema, ribadendo l'esistenza di una tutela costituzionale per il diritto alla privacy, negò l'esistenza dell'*informational privacy* quale entità separata e autonoma. Ad oggi, dunque, nel panorama tanto legislativo quanto giurisprudenziale statunitense, manca una tutela di qualsiasi informazione riguardante una persona fisica identificata o identificabile, analoga quindi a quella prevista a livello europeo dalla nozione di «dato personale» prevista dal GDPR. L'ordinamento, infatti, si limita a tutelare la *personal information* intesa quale informazione relativa alla sola persona identificata, ma non anche *identificabile*.²⁰⁰

Dal punto di vista legislativo, invece, la disciplina è regolata a livello federale da numerosi statuti che rendono la disciplina settoriale e frammentaria.²⁰¹ A titolo esemplificativo, si ricorda il Family Educational Rights and Privacy Act del 1978 per la protezione dei registri scolastici, il Foreign Intelligence Surveillance Act, emanato nel 1978 e modificato nel 2008 e nel 2012, che governa l'accesso alle informazioni da parte delle agenzie di intelligence, l'Electronic Communications Privacy Act del 1986, che contiene meccanismi di tutela nei confronti della sorveglianza tramite sistemi tecnologici delle comunicazioni, il Children's Online Privacy Protection Act del 1998, che tutela i dati online dei minori di tredici anni, l'USA Patriot Act del 2001, che consente la sorveglianza per esigenze di sicurezza nazionale, il Telephone Consumer Protection Act del 1994 che fornisce rimedi in caso di Telemarketing, e così via.²⁰²

Peraltro, permane in capo ai singoli stati la possibilità di disciplinare la materia in maniera autonoma²⁰³. Ne deriva un quadro certamente frammentato e settorializzato.²⁰⁴

¹⁹⁷ Basti pensare che nel celeberrimo caso *Griswold v. Connecticut* (1965), la Corte Suprema statunitense riconosce come contraria al diritto alla privacy, in particolar modo alla privacy coniugale, una legge del Connecticut che vietava la prescrizione e l'utilizzo di metodi anticoncezionali. Analogamente, nel caso *Roe v. Wade* (1973), il diritto alla privacy fu interpretato come un diritto talmente ampio da includere il diritto della donna a far ricorso all'interruzione volontaria di gravidanza.

¹⁹⁸ «*The individual interest in avoiding disclosure of personal matters*», ma anche «*the interest in independence in making certain kinds of important decisions*».

¹⁹⁹ P. Guarda, G. Bincoletto, «Diritto comparato della privacy e della protezione dei dati personali», p. 31.

²⁰⁰ *Ibidem*, p. 32.

²⁰¹ Si v. F. Giovanella, «Copyright and Information Privacy. Conflicting Rights in Balance», Cheltenham, Edward Elgar, 2017.

²⁰² Per un elenco complete, si v. P. Guarda, G. Bincoletto, «Diritto comparato della privacy e della protezione dei dati personali», pp. 32-34.

²⁰³ Si v., ad esempio, il Privacy Act della California, che recita all'art. 1 § 1: «*All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy*».

²⁰⁴ G. Bincoletto «La privacy by design: un'analisi comparata nell'era digitale», Ariccia, Aracne editrice, 2019, p. 42.

A livello statale, merita sicuramente particolare attenzione il California Consumer Privacy Act (CCPA),²⁰⁵ approvato nel 2018 ma divenuto vincolante nel 2020. Tale insieme di norme si caratterizza per essere «*one of the strongest state privacy laws in the United States*»²⁰⁶ e si applica a tutte le società che raccolgono e conservino informazioni di cittadini californiani per finalità commerciali e che conseguano annualmente utili superiori a 25 milioni di dollari, trattino informazioni di più di cinquantamila californiani all'anno, e che ottengano almeno il 50% degli utili annuali dalla vendita di informazioni di californiani.

In Italia, invece, il riconoscimento dell'esistenza del diritto alla riservatezza ha origine giurisprudenziale. Tale diritto, secondo l'analisi condotta da Stefano Rodotà²⁰⁷, nacque come un diritto di stampo borghese.

Il riconoscimento di un generale diritto alla riservatezza non fu però immediato. La Corte di Cassazione, infatti, lo negò per ben due volte: la prima volta, nella sentenza n. 4487 del 1956²⁰⁸, nel celebre caso Caruso, e poi nuovamente nel 1963 con la sentenza n. 990, in cui, pur riconoscendo una generale violazione del diritto alla personalità, in particolar modo all'autodeterminazione del singolo, ogni qualvolta ci fosse stata una divulgazione della vita privata in assenza di consenso o di interesse pubblico verso la vicenda, non si spinse fino al punto di elaborare un autonomo diritto alla riservatezza.

Fu solo nel 1975, infatti, che la Corte di Cassazione, con la sentenza pronunciata il 25 maggio n. 2129, riconobbe l'esistenza di un autonomo diritto alla riservatezza. Il caso riguardava la principessa Soraya, celebrità del tempo, che fu raggiunta da un tele-obbiettivo di un giornalista dentro la sua abitazione.

Il diritto alla riservatezza venne in questa sede delineato come quel diritto che

«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 o il decoro, non sono giustificati da interessi pubblici preminenti».

Anche in Italia, grazie alla celeberrima sentenza del 1975, il diritto alla riservatezza conosce un fondamento costituzionale, in particolar modo la Corte di Cassazione pone l'accento sugli articoli 2, 3 e 13 della Costituzione:

²⁰⁵ Consultabile al link:

https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5

²⁰⁶ D. Solove, P.M. Schwartz, «Information Privacy Law», p.970-973.

²⁰⁷ S. Rodotà, «Riservatezza», Enciclopedia Treccani, VI appendice, 2000, consultabile al link:

https://www.treccani.it/enciclopedia/riservatezza_%28Enciclopedia-Italiana%29/.

²⁰⁸ Nella sentenza citata si legge che «nessuna disposizione di legge autorizza a ritenere che sia stato sancito, come principio generale, il rispetto assoluto alla 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.» [...] «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».

«[L'articolo 2] riconosce e garantisce i diritti inviolabili dell'uomo, sia come singolo, sia nelle formazioni sociali ove si svolge la sua personalità» [...]

«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. E, sotto questo profilo, va ricordata anche la inviolabilità della libertà personale, intesa questa in un senso più ampio della libertà meramente fisica».

Grazie a questa pronuncia, il diritto alla riservatezza ad oggi rientra all'interno dei diritti della personalità, costituzionalmente tutelati dall'articolo 2 della Carta Costituzionale:

*«nella sua più ampia dimensione di clausola generale, «aperta» all'evoluzione dell'ordinamento e suscettibile, per ciò appunto, di apprestare copertura costituzionale ai nuovi valori emergenti della personalità in correlazione anche all'obiettivo primario di tutela del "pieno sviluppo della persona umana", di cui al successivo art. 3, cpv».*²⁰⁹

Il diritto al rispetto della vita privata e familiare, del domicilio e delle comunicazioni trova espresso riconoscimento anche all'articolo 7 della Carta dei Diritti fondamentali dell'Unione europea, accanto ad esso, l'articolo 8 prevede espressamente il riconoscimento della tutela del diritto alla protezione dei dati personali.

Si ricordi inoltre la Convenzione europea sui diritti dell'uomo (CEDU), per cui ogni persona ha diritto al rispetto della sua vita privata e familiare, del suo domicilio e della sua corrispondenza (articolo 8).²¹⁰

In questa sede si preme sottolineare come la tutela della riservatezza sia strumentale alla tutela della dignità umana. Senza la possibilità di mantenere un certo controllo sulla propria sfera privata, si perpetua uno stato di incertezza circa le informazioni personali accessibili a terzi. Ciò comporta il rischio che l'individuo non sia in grado di sviluppare la propria personalità liberamente. L'individuo, infatti, per poter liberamente sviluppare la propria personalità e la propria autonomia, necessita di scegliere cosa mostrare di sé agli altri, e in che termini.²¹¹

La personalità di ognuno è, infatti, il frutto di un complesso insieme di fattori biologici, culturali e sociali, che interagiscono tra di loro nella formazione dell'identità personale in un percorso che comincia sin dalla nascita.²¹² Ogni individuo deve mantenere inalterata la possibilità di mostrare parte della propria personalità e nasconderne, invece, altre. Senza la libertà di mantenere una sfera privata all'interno

²⁰⁹ Corte di Cassazione, 7 febbraio 1996, n. 978.

²¹⁰ Si ricordi in questa sede che in forza dell'articolo 6 del Trattato di Lisbona, i diritti contenuti nella CEDU sono riconosciuti quali principi fondamentali dell'Unione europea.

²¹¹ V. Boehme-Neßler, «Privacy: A Matter of Democracy. Why Democracy Needs Privacy and Data Protection», p. 223.

²¹² Ibidem, p. 227.

della quale interrogarsi e sviluppare le proprie idee e voci fuori dal coro, la dignità dell'individuo è seriamente messa in pericolo.²¹³

La correlazione tra libertà, dignità e privacy è ribadita anche da Stefano Rodotà nel discorso conclusivo della 26esima Conferenza internazionale sulla protezione dei dati²¹⁴:

«Senza una forte tutela delle informazioni che le riguardano, le persone rischiano sempre di più d'essere discriminate per le loro opinioni, credenze religiose, condizioni di salute: la privacy si presenta così come un elemento fondamentale dalla società dell'eguaglianza. Senza una forte tutela dei dati riguardanti le convinzioni politiche o l'appartenenza a partiti, sindacati, associazioni, i cittadini rischiano d'essere esclusi dai processi democratici: così la privacy diventa una condizione essenziale per essere inclusi nella società della partecipazione. Senza una forte tutela del "corpo elettronico", dell'insieme delle informazioni raccolte sul nostro conto, la stessa libertà personale è in pericolo diventa così evidente che: la privacy è uno strumento necessario per difendere la società della libertà, e per opporsi alle spinte verso la costruzione di una società della sorveglianza, della classificazione, della selezione sociale...».

«Nel quadro della privacy, la dignità si precisa come un concetto riassuntivo dei principi di riconoscimento della personalità e di non riduzione a merce della persona, di eguaglianza, di rispetto degli altri, di eguaglianza, di solidarietà, di non interferenza nelle scelte di vita, di possibilità di agire liberamente nella sfera pubblica».

Il fatto che il diritto alla privacy sia collocato, nella Carta dei diritti fondamentali dell'Unione europea, nel capo dedicato alla libertà, rappresenta secondo Rodotà il sintomo di un importante mutamento culturale, che vede il diritto alla privacy quale un diritto strumentale all'esercizio di altri diritti e libertà fondamentali, avvicinando il sistema europeo, tradizionalmente basato sulla dignità, a quello statunitense, improntato, invece alla tutela della libertà:

*«La forte tutela dei dati sensibili è divenuta una componente essenziale dell'eguaglianza, per evitare che la raccolta di queste particolari informazioni possa trasformarsi in uno strumento di discriminazione delle persone. Ma la tutela dei dati sanitari o genetici è anche la condizione per realizzare il diritto alla salute, così come la tutela dei dati sulle opinioni diventa una premessa per esercitare la libertà di espressione, comunicazione, associazione, culto. E la condizione di lavoratore, l'accesso al credito e alle assicurazioni dipendono sempre di più dall'intensità di tutela delle informazioni personali. Nel modello europeo l'associazione tra privacy e libertà diviene sempre più stretta».*²¹⁵

1.6.2 La tutela dei dati personali: la disciplina europea

²¹³ Ibidem, p. 228.

²¹⁴ S. Rodotà, discorso conclusivo della 26esima Conferenza internazionale sulla protezione dei dati, settembre 2004. Il discorso è riportato al link:
<https://www.garantepriacy.it/home/docweb/-/docweb-display/docweb/1049293>.

²¹⁵ Ibidem.

Si è visto come nel contesto italiano la privacy sia nata come un diritto legato alla protezione della vita privata dei personaggi pubblici dalle ingerenze dei privati, mentre negli Stati Uniti, dopo una simile vicenda di Warren e Brandeis, tale diritto ha fin da subito assunto una forte connotazione di tutela dalle invasioni operate dal potere pubblico. Il diritto alla privacy ha subito inevitabilmente gli effetti dell'innovazione tecnologica. Infatti, con la diffusione pervasiva delle tecnologie dell'informazione e della comunicazione, la raccolta e la gestione di informazioni è diventata sempre più diffusa.²¹⁶

L'asse del problema si è dunque spostato dalla tutela del soggetto dalle incursioni nella sua vita privata alla necessità di evitare utilizzi impropri dell'ingente mole di informazioni che si rendono disponibili.²¹⁷

In generale, dunque, *«la privacy si presenta ormai come nozione fortemente dinamica e che si è stabilita una stretta e costante interrelazione tra mutamenti determinati dalle tecnologie dell'informazione»*²¹⁸. Essa non è più configurabile come diritto a essere lasciati soli, ma come diritto al controllo sul modo in cui le informazioni personali vengono utilizzate,²¹⁹ riporta infatti Pascuzzi:²²⁰

«L'introduzione delle tecnologie informatiche ha comportato un cambiamento importante del campo della tutela dei diritti della personalità. L'avvento dei calcolatori ha richiesto l'adozione di specifici meccanismi di tutela perché il problema non era più (solo) quello di salvaguardare la vita privata di persone famose dall'aggressione portata dai mass media, bensì quello di scongiurare i pericoli più o meno palesi e avvertibili (discriminazioni in testa) derivanti a ciascun cittadino dalla facilità con la quale possono essere trattate e incrociate le informazioni che lo riguardano. La rivoluzione digitale comporta addirittura il cambiamento della nozione e del contenuto del diritto alla riservatezza: non più diritto a essere lasciati soli, ma diritto al controllo sui propri dati».

I problemi della società della sorveglianza hanno spinto l'Unione europea verso la ricerca di una soluzione, ridefinendo il concetto di privacy nella dimensione del diritto a protezione dei dati personali.²²¹

Un primo intervento si è avuto con la Direttiva 95/46/CE («direttiva madre») del Parlamento europeo e del Consiglio relativa alla *«tutela delle persone fisiche con*

²¹⁶ S. Rodotà, «Riservatezza».

²¹⁷ In questo senso anche R. Caso, «La società della mercificazione e della sorveglianza: dalla persona ai dati», p. 231 e ss.

²¹⁸ S. Rodotà, «Riservatezza».

²¹⁹ Si v. F. Giovanella, «Copyright and Information Privacy», in cui la privacy è definita come *«la possibilità per un individuo di esercitare un controllo su come le sue informazioni personali sono raccolte, usate o divulgate da terzi».*

²²⁰ G. Pascuzzi, «Il diritto dell'era digitale», p. 81-82.

²²¹ P. Guarda, G. Bincoletto, «Diritto comparato della privacy e della protezione dei dati personali», p. 51.

*riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati».*²²² Il recepimento della direttiva in Italia è avvenuto con la legge 31 dicembre 1996 n. 675.

Inoltre, una tappa fondamentale nella tutela della privacy a livello europeo si ha già nel 2000, quando l'Unione europea adotta la Carta dei diritti fondamentali dell'Unione europea,²²³ all'interno della quale la privacy, intesa nel senso di tutela dei dati personali, assume il rango di diritto fondamentale a livello europeo grazie alla formulazione dell'articolo 8:

«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. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente».

Successivamente, il Parlamento europeo e il Consiglio hanno emanato la direttiva 2002/57/CE, in materia di *«trattamento dei dati personali e sulla tutela della vita privata nel settore delle comunicazioni elettroniche»*.

Il recepimento di quest'ultima direttiva ha poi portato il nostro legislatore all'emanazione di una disciplina settoriale in materia di privacy tramite l'approvazione del decreto legislativo del 30 giugno 2003 n. 196, rubricato *«Codice in materia di protezione dei dati personali»*.²²⁴

Grazie all'articolo 16 del Trattato sul Funzionamento dell'Unione, che al primo paragrafo attua un riconoscimento *expressis verbis* del diritto alla protezione dei dati di carattere personale, la competenza dell'UE è stata ampliata, permettendo l'adozione di norme di diritto derivato in materia di protezione dei dati personali, sulla base del quale è stato poi introdotto il GDPR²²⁵ nel 2016.

L'iter di approvazione del GDPR è stato particolarmente lungo: sono stati infatti necessari quasi sei anni. Il punto d'inizio del percorso è stata la pubblicazione del Programma di Stoccolma²²⁶, in cui si delineavano le priorità dell'UE per lo spazio di libertà, sicurezza e giustizia per il periodo tra il 2010 e il 2014. Si legge infatti:

«ove si tratti di valutare il rispetto della vita privata delle persone nello spazio di libertà, sicurezza e giustizia, il diritto alla libertà risulta preponderante. Il diritto al rispetto della vita privata e alla protezione dei dati personali è sancito dalla Carta dei diritti fondamentali. L'Unione deve pertanto far fronte

²²² Direttiva 95/46/CE del Parlamento europeo e del Consiglio, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, 24 ottobre 1995, consultabile al link:

<https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX%3A31995L0046>.

²²³ Divenuta vincolante poi solo nel 2009.

²²⁴ Il Codice in materia di protezione dei dati personali, detto anche Codice Privacy, è norma tutt'ora cogente nel nostro ordinamento. L'implementazione del GDPR ha tuttavia reso necessaria una serie di interpolazioni nel testo normativo, rendendolo non particolarmente chiaro, poiché colmo di riferimenti al GDPR stesso.

²²⁵ G. Bincoletto, «La privacy by design: un'analisi comparata nell'era digitale».

²²⁶ Consiglio Europeo, Programma di Stoccolma – Un'Europa aperta e sicura al servizio e a tutela dei cittadini, 2010/C115/01, 4 maggio 2010, consultabile al link:

<https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX%3A52010XG0504%2801%29>.

alle sfide insite nello scambio crescente di dati personali, e all'esigenza di garantire la protezione della vita privata.»

L'invito è rivolto all'implementazione di una strategia globale in materia di protezione dei dati personali, che disciplini tanto la tutela all'interno dell'UE quanto nell'ambito delle relazioni con paesi terzi.²²⁷ Viene riconosciuta l'esigenza di uno scambio più intenso dei dati personali, pur ribadendo la necessità che ciò non comprometta la tutela della vita privata. Inoltre, il Consiglio non condanna l'innovazione tecnologica: se da un lato è vero che questa comporta la nascita di nuove criticità, al contempo offre nuove possibilità per la tutela dei dati personali.²²⁸

La prima proposta di regolamento da parte della Commissione europea è datata al 25 gennaio 2012, ma l'approvazione definitiva del GDPR si è avuta solamente, come già noto, il 14 aprile del 2016. Il GDPR è entrato in vigore il 24 maggio 2016, ma la sua applicazione è avvenuta solamente, dopo un periodo di transizione di due anni, il 25 maggio 2018.

1.6.3 I concetti chiave del GDPR

Prima di introdurre il ruolo del capitalismo della sorveglianza nel mondo accademico e dell'istruzione e presentare i rilievi critici in materia di didattica a distanza rispetto al GDPR, si preme in questa sede sintetizzare alcuni dei concetti chiave del Regolamento.

In primis, è necessario sottolineare la differenza tra il valore normativo di una direttiva e di un regolamento. Infatti, le direttive vincolano gli Stati membri con riferimento al risultato da raggiungere, lasciando alle singole autorità nazionali la possibilità di scegliere i mezzi considerati più idonei tramite apposite leggi di attuazione. I regolamenti, invece, hanno portata generale e sono direttamente applicabili negli Stati membri, senza necessità di recepimento da parte del diritto interno.²²⁹ Questa

²²⁷ Più nello specifico, Il Consiglio europeo invita la Commissione a: «*valutare il funzionamento dei vari strumenti concernenti la protezione dei dati e presentare, se del caso, iniziative complementari, legislative o meno, atte a preservare l'efficace applicazione dei succitati principi, — proporre una raccomandazione per la negoziazione di accordi in materia di protezione e, se necessario, condivisione dei dati a fini di contrasto con gli Stati Uniti d'America, sulla scorta dei lavori svolti dal Gruppo di contatto ad alto livello UE-Stati Uniti sulla condivisione delle informazioni e sulla tutela della vita privata e la protezione dei dati di carattere personale, — prendere in esame elementi essenziali per accordi sulla protezione dei dati con paesi terzi a fini di contrasto, che potrebbero contemplare, se necessario, i dati detenuti a titolo privato, fondati su un elevato livello di protezione dei dati, — migliorare il rispetto dei principi in materia di protezione dei dati grazie allo sviluppo di nuove tecnologie adeguate, migliorando la cooperazione tra il settore pubblico e privato specie nelle attività di ricerca, — valutare l'opportunità di introdurre un regime di certificazione europea per le tecnologie, i prodotti e i servizi «rispettosi della vita privata»; — svolgere campagne d'informazione e, in particolare, di sensibilizzazione presso i cittadini».*

²²⁸ Consiglio Europeo, Programma di Stoccolma, par. 2.5.

²²⁹ Si v. art. 288 TFUE.

differenza è colta in tutta la sua rilevanza dai Considerando numero 9²³⁰ e 10²³¹ del GDPR, in cui si riconosce che l'utilizzo dello strumento della direttiva per regolare la protezione dei dati personali ha creato frammentazione legislativa e non ha raggiunto l'obiettivo di eliminare l'incertezza giuridica in materia di rischi correlati alle attività online. Al fine di ottenere un livello coerente ed elevato di protezione dei dati personali, il Parlamento e il Consiglio dell'Unione europea sottolineano infatti la necessità di ottenere un livello di protezione dei diritti delle persone fisiche equivalente in tutto il territorio dell'Unione.

Il Considerando n. 15²³², inoltre, è di particolare importanza, dal momento che sancisce espressamente la necessità che la normativa si ponga come neutra rispetto alla tecnologia e indipendente rispetto alle tecnologie impiegate, così da evitare l'insorgenza di rischi di elusione.

Per comprendere il funzionamento del GDPR, occorre spiegare cosa si intenda per «trattamento». Ai sensi dell'articolo 4, rubricato «definizioni», numero 2, il trattamento di dati personali è:

²³⁰ «Sebbene i suoi obiettivi e principi rimangano tuttora validi, la direttiva 95/46/CE non ha impedito la frammentazione dell'applicazione della protezione dei dati personali nel territorio dell'Unione, né ha eliminato l'incertezza giuridica o la percezione, largamente diffusa nel pubblico, che in particolare le operazioni online comportino rischi per la protezione delle persone fisiche. La compresenza di diversi livelli di protezione dei diritti e delle libertà delle persone fisiche, in particolare del diritto alla protezione dei dati personali, con riguardo al trattamento di tali dati negli Stati membri può ostacolare la libera circolazione dei dati personali all'interno dell'Unione. Tali differenze possono pertanto costituire un freno all'esercizio delle attività economiche su scala dell'Unione, falsare la concorrenza e impedire alle autorità nazionali di adempiere agli obblighi loro derivanti dal diritto dell'Unione. Tale divario creatosi nei livelli di protezione è dovuto alle divergenze nell'attuare e applicare la direttiva 95/46/CE».

²³¹ «Al fine di assicurare un livello coerente ed elevato di protezione delle persone fisiche e rimuovere gli ostacoli alla circolazione dei dati personali all'interno dell'Unione, il livello di protezione dei diritti e delle libertà delle persone fisiche con riguardo al trattamento di tali dati dovrebbe essere equivalente in tutti gli Stati membri. È opportuno assicurare un'applicazione coerente e omogenea delle norme a protezione dei diritti e delle libertà fondamentali delle persone fisiche con riguardo al trattamento dei dati personali in tutta l'Unione. Per quanto riguarda il trattamento dei dati personali per l'adempimento di un obbligo legale, per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento, gli Stati membri dovrebbero rimanere liberi di mantenere o introdurre norme nazionali al fine di specificare ulteriormente l'applicazione delle norme del presente regolamento. In combinato disposto con la legislazione generale e orizzontale in materia di protezione dei dati che attua la direttiva 95/46/CE gli Stati membri dispongono di varie leggi settoriali in settori che richiedono disposizioni più specifiche. Il presente regolamento prevede anche un margine di manovra degli Stati membri per precisarne le norme, anche con riguardo al trattamento di categorie particolari di dati personali («dati sensibili»). In tal senso, il presente regolamento non esclude che il diritto degli Stati membri stabilisca le condizioni per specifiche situazioni di trattamento, anche determinando con maggiore precisione le condizioni alle quali il trattamento di dati personali è lecito».

²³² «Al fine di evitare l'insorgere di gravi rischi di elusione, la protezione delle persone fisiche dovrebbe essere neutrale sotto il profilo tecnologico e non dovrebbe dipendere dalle tecniche impiegate. La protezione delle persone fisiche dovrebbe applicarsi sia al trattamento automatizzato che al trattamento manuale dei dati personali, se i dati personali sono contenuti o destinati a essere contenuti in un archivio. Non dovrebbero rientrare nell'ambito di applicazione del presente regolamento i fascicoli o le serie di fascicoli non strutturati secondo criteri specifici, così come le rispettive copertine».

«qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e 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».

Si ritiene inoltre fondamentale riportare la definizione di «titolare del trattamento» (articolo 4, numero 7, GDPR) e «responsabile del trattamento» (articolo 4, numero 8, GDPR):

«titolare del trattamento: 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»;

«responsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento».

Per comprendere la differenza tra titolare e responsabile del trattamento, gioverà l'esempio - ricorrente nei prossimi due capitoli - dei sistemi di posta elettronica universitaria affidati a Google. Studenti, docenti, ricercatori, e in generale di tutto il personale universitario, sono gli interessati al trattamento, ovvero le persone fisiche cui si riferiscono i dati personali, mentre il titolare del trattamento è l'Università stessa, nella persona del Rettore. Google, invece, gestendo il sistema di posta elettronica, è il responsabile del trattamento. Inoltre, ai sensi del Considerando 14, gli interessati al trattamento possono essere solo persone fisiche e non persone giuridiche.

L'articolo 2 del GDPR delinea con chiarezza i confini dell'ambito di applicazione materiale: la normativa generale si applica infatti al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi. Fanno eccezione all'applicabilità del GDPR i trattamenti dei dati personali effettuati per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione, effettuati dagli Stati membri nell'esercizio di attività che rientrano nell'ambito di applicazione del secondo capo del titolo V del Trattato sull'Unione europea, oppure quelli effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico, nonché quelli compiuti dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzioni di sanzioni penali. In quest'ultimo caso, peraltro, si applica la Direttiva 2016/680 approvata contestualmente al GDPR e recante disposizioni circa la «*protezione delle persone fisiche con riguardo al trattamento dei*

*dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali».*²³³

Rappresenta un'importante novità anche l'ambito di applicazione territoriale, descritta dall'articolo 3. Il primo paragrafo stabilisce che il GDPR si applica al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione. A mente del paragrafo 2, inoltre, l'applicazione del GDPR si estende anche al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività riguardano: a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione.

In altre parole, il primo paragrafo dell'articolo 3 riprende il criterio dello stabilimento, già noto alla direttiva 95/46/CE. La definizione di stabilimento è ribadita al Considerando 22, in cui viene specificato che lo stabilimento implica l'effettivo e reale svolgimento di attività nel quadro di un'organizzazione stabile, indipendentemente dalla forma giuridica assunta, sia essa una succursale o una filiale dotata di personalità giuridica. Nella sentenza *Google v. Spain* del 2014, la Corte di Giustizia dell'Unione europea ha specificato che ogni attività effettiva e stabile, seppur di minima entità, assume rilevanza ai fini della determinazione della presenza di uno stabilimento.²³⁴

Il vero elemento di novità è rappresentato dal paragrafo 2, detto anche «*criterio del target*», che sancisce che il GDPR non si applica solamente per le entità stabilite all'interno del territorio dell'Unione europea, ma anche per quelle non stabilite all'interno del territorio che però trattano i dati personali all'interno dell'Unione, offrendo beni, prestando servizi o monitorando il comportamento di persone fisiche all'interno dell'UE. Ciò implica che l'eventuale assenza di un'attività stabile all'interno dell'Unione non determina una necessaria non applicabilità del GDPR, ma, al contrario, occorre porre l'accento sulle attività svolte durante il trattamento e dai destinatari delle stesse. Il Considerando 23 rappresenta un ausilio alla lettura del secondo paragrafo:

«Per determinare se tale titolare o responsabile del trattamento stia offrendo beni o servizi agli interessati che si trovano nell'Unione, è opportuno verificare se risulta che il titolare o il responsabile del trattamento intenda fornire servizi agli interessati in uno o più Stati membri dell'Unione. Mentre la semplice accessibilità del sito web del titolare del trattamento, del

²³³ Direttiva (UE) 2016/680, del Parlamento europeo e del Consiglio, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio, 27 aprile 2016, consultabile al link:

<https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32016L0680&from=RO>.

²³⁴ Corte di Giustizia dell'Unione europea, sentenza della Corte (Grande Sezione), 13 maggio 2014, *Google Spain SL e Google Inc. Contro Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*, Causa C-131/12. Consultabile al link:

<https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A62012CJ0131>.

responsabile del trattamento o di un intermediario nell'Unione, di un indirizzo di posta elettronica o di altre coordinate di contatto o l'impiego di una lingua abitualmente utilizzata nel paese terzo in cui il titolare del trattamento è stabilito sono insufficienti per accertare tale intenzione, fattori quali l'utilizzo di una lingua o di una moneta abitualmente utilizzata in uno o più Stati membri, con la possibilità di ordinare beni e servizi in tale altra lingua, o la menzione di clienti o utenti che si trovano nell'Unione possono evidenziare l'intenzione del titolare o del responsabile del trattamento di offrire beni o servizi agli interessati nell'Unione».

A mente del GDPR, il trattamento dei dati personali può avvenire solamente in presenza di una base giuridica, così da rispettare il principio di liceità sancito dall'articolo 5, paragrafo 1, lettera a), del Regolamento.

Ai fini del presente lavoro, assume un carattere fondamentale la distinzione tra «dati personali» e «categorie particolari di dati», alla luce della diversa base giuridica del trattamento necessaria per il trattamento di questi ultimi.

All'interno delle categorie particolari di dati rientrano i dati genetici, biometrici, relativi alla salute²³⁵, alla vita sessuale o all'orientamento sessuale, nonché i dati che rivelino originale razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, per come specificato espressamente dall'articolo 9, paragrafo 1.

Infatti, il trattamento dei dati personali è lecito quando avviene, ai sensi dell'articolo 6, alternativamente: con il consenso dell'interessato, per finalità di adempimento di obblighi contrattuali e misure precontrattuali, obblighi di legge a cui è soggetto il titolare del trattamento, per la tutela di interessi vitali dell'interessato o di altra persona fisica, per legittimo interesse prevalente del titolare o di terzi a cui i dati vengono comunicati o nel caso in cui 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.

Differentemente, l'articolo 9 del GDPR, nel descrivere il trattamento di categorie particolari di dati, detta un divieto di trattare categorie particolari di dati. Tale divieto, però, non è assoluto, conosce infatti le eccezioni di cui al secondo paragrafo dello stesso articolo. Più nello specifico, è possibile effettuare il trattamento dei dati personali rientranti nelle categorie particolari di dati se l'interessato ha prestato il consenso esplicito, oppure per assolvere obblighi di diritto del lavoro, sicurezza sociale e protezione sociale. Le altre basi giuridiche ammesse dal secondo paragrafo dell'articolo 9 prevedono: finalità di tutela di un interesse vitale dell'interessato, il caso di un'attività di un'associazione che persegue finalità politiche, religiose, filosofiche o di sindacati, o quello in cui i dati siano resi manifestamente pubblici dall'interessato. Il trattamento è inoltre possibile per accertare, esercitare o difendere un diritto in sede giudiziaria, per motivi di interesse pubblico rilevante, per finalità di medicina o sanità pubblica e per finalità di archiviazione nel pubblico interesse, di ricerca scientifica o per fini statistici.

²³⁵ Per una definizione di dati genetici, biometrici o relativi alla salute, si v. articolo 4 GDPR, rispettivamente n. 13, 14, 15.

Ex multis, si noti che tanto il trattamento dei dati personali, quanto il trattamento di categorie particolari di dati, può avvenire sulla base del consenso dell'interessato. Ai sensi dell'articolo 4, numero 11 del GDPR, il consenso può identificarsi come

«qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento».

In particolare, il Considerando numero 32 specifica che il consenso dovrebbe essere prestato mediante un atto positivo inequivocabile, che manifesti l'intenzione dell'interessato *«libera, specifica, informata e inequivocabile»* di accettare il trattamento dei dati personali. Il consenso, dunque, non si dovrebbe considerare come prestato ogni qualvolta il titolare si limiti a registrare l'eventuale silenzio, inattività o preselezione di caselle. Inoltre, quando il trattamento abbia più finalità, occorre che l'interessato presti il consenso per ognuna di queste. Per il trattamento di categorie particolari di dati personali, il consenso deve essere, ai sensi dell'articolo 9, esplicito.

Oltre il principio di liceità, il trattamento deve rispettare gli altri principi sanciti dall'articolo 5. Si chiede, in primo luogo, che il trattamento sia condotto con correttezza e trasparenza nei confronti dell'interessato. Le finalità del trattamento, poi, devono essere limitate: in altre parole, i dati devono essere raccolti per finalità determinate, esplicite e legittime, e poi trattati in modo non incompatibile con dette finalità. In questa cornice, si colloca anche il principio di minimizzazione dei dati raccolti: è infatti fondamentale che si raccolgano solo i dati adeguati, pertinenti e limitati alle finalità per le quali sono stati raccolti. È poi enunciato il principio di esattezza, che implica che i dati raccolti devono essere esatti, e, quando necessario, aggiornati, insistendo sulla necessità che siano adottate le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per cui sono stati raccolti. La conservazione dei dati non deve inoltre avvenire per un arco di tempo superiore al conseguimento delle finalità del trattamento. Ulteriori principi sono poi integrità e riservatezza, che postulano la necessità che i dati siano trattati in maniera da garantire un'adeguata sicurezza, e, infine, la responsabilizzazione o *accountability* del titolare del trattamento. Questo ultimo principio è un'importante novità introdotta dal GDPR, che abbandona il vecchio sistema cosiddetto *«check-list»*, prevedendo un maggior grado di responsabilizzazione del titolare del trattamento.²³⁶

1.7. Considerazioni di sintesi

Nel presente capitolo, grazie alla sapiente analisi di Zuboff, Pagano, Rikiap, Wu, Khan e Florio si è descritta la nascita del fenomeno del capitalismo della sorveglianza, e come questo abbia contribuito alla nascita di monopoli intellettuali e *data-driven intellectual monopoly*.

²³⁶ Per un approfondimento si v. G.M. Riccio, G. Scorza, E. Bellisario, «GDPR e normativa privacy, commentario», Milano, Wolters Kluwer, 2018.

La scelta dei grandi operatori oligopolistici e monopolistici di implementare il ciclo di reinvestimento del surplus comportamentale in mercati estranei alle logiche tradizionali della Silicon Valley inasprisce le conseguenze critiche descritte.

L'individuo, divenuto mezzo per uno scopo, si presta a diventare una digital person al centro di un processo di mercificazione della persona, e consumatori e utenti perdono progressivamente la capacità di acquisto consapevole e di autodeterminazione, come dimostrato dal celeberrimo caso Cambridge Analytica.

Nel prossimo capitolo, si indagherà il fenomeno dell'intrusione del capitalismo della sorveglianza nel mondo della ricerca e si getterà luce su un nuovo «passo fuori dalla Silicon Valley» dei grandi operatori oligopolistici. Nello specifico, si descriverà la didattica del capitalismo della sorveglianza e come questa abbia guadagnato terreno soprattutto durante il periodo di svolgimento delle attività di didattica a distanza, resosi necessario per finalità di contenimento del virus SARS-CoV-2.

Merita inoltre particolare attenzione il fatto che molti dei *Big Data* estratti, analizzati e reinvestiti nel mercato dei comportamenti futuri sono spesso dati personali, pertanto, nel III capitolo, si guarderà con particolare attenzione alle norme del GDPR e alla compatibilità con le stesse della didattica del capitalismo della sorveglianza.

II CAPITOLO

GLI OLIGOPOLI NELLA DIDATTICA DEL CAPITALISMO DELLA SORVEGLIANZA

2.1 Operatori oligopolistici nel mondo dell'istruzione

Nel capitolo precedente è stato illustrato il ciclo di reinvestimento del surplus comportamentale nel mercato dei comportamenti futuri, descrivendo come numerose aziende della Silicon Valley si siano imposte come operatori monopolistici o oligopolistici in un nuovo ordine economico chiamato capitalismo della sorveglianza.

Nel presente capitolo, invece, si intende analizzare come questi monopoli e oligopoli abbiano ormai esteso il loro dominio anche in ambienti che dovrebbero essere estranei al mercato stesso, ma che adesso si prestano ad essere piegati alle logiche del capitalismo della sorveglianza.

Si intende osservare il fenomeno illustrando come gli operatori oligopolistici abbiano ormai non solo inglobato *in toto* il mondo dell'editoria scientifica, ma anche come questo fenomeno sia in realtà ricollegabile ad attività di vero e proprio monitoraggio.²³⁷

Il presente scritto guarderà poi con maggiore attenzione il ruolo che questi hanno ricoperto nel mondo dell'istruzione durante il fenomeno dell'*emergency remote teaching* (ERT), resosi necessario a causa della pandemia da Covid-19 a marzo 2020. Nello specifico, si guarderà al fenomeno della «*platformised education*»²³⁸, ovvero all'istruzione delle piattaforme.

Il fenomeno dell'ERT, rappresentando un cambio temporaneo e repentino verso modalità alternative di erogazione della didattica per far fronte ad una situazione emergenziale, si differenzia dall'*online learning*, in cui la didattica è pensata e progettata sin dall'inizio per essere svolta online.²³⁹

Tanto nell'istruzione delle piattaforme, quanto nell'ingerenza del capitalismo della sorveglianza nel mondo della ricerca scientifica, ai rischi – precedentemente illustrati - di mercificazione della persona, di manipolazione degli utenti e consumatori e condizionamento delle attività democratiche, si aggiungono nuove difficili sfide.

²³⁷ Per un approfondimento sul capitalismo della sorveglianza e dei monopoli intellettuali nel contesto della ricerca scientifica e sulle misure adottate per contrastare gli oligopoli commerciali nel mercato dell'editoria accademica a livello nazionale, internazionale e europeo, si v. C. Franch, «Il capitalismo dei monopoli intellettuali e l'editoria della sorveglianza. Un'analisi delle politiche europee sull'open science e sulla regolazione dei dati».

²³⁸ C. Angiolini, R. Ducato, A. Giannopoulou, G. Schneider, «Remote Teaching During the Emergency and Beyond: Four Open Privacy and Data Protection Issues of 'Platformised' Education», *Opinio Juris in Comparatione*, vol. 1, 2020, pp. 45-72.

<https://ssrn.com/abstract=3779238>.

²³⁹ Si v. C. Hodges, et al., «The difference between Emergency Remote Teaching and Online Learning», 27 marzo 2020, Educause.

<https://er.educause.edu/articles/2020/3/the-difference-between-emergency-remote-teaching-and-online-learning>.

Nello specifico, al centro del ragionamento deve essere posto l'articolo 33 della Costituzione: «*l'arte e la scienza sono libere e libere ne è l'insegnamento*».

Nelle pagine che seguono, si cercherà di comprendere come la libertà di insegnamento e di ricerca scientifica siano potenzialmente messe in pericolo dalla progressiva diffusione delle logiche di accumulazione dei dati del capitalismo della sorveglianza all'interno del mondo della scuola e dell'Università.²⁴⁰

2.2. Oligopoli e Università

2.2.1 L'editoria scientifica

Le grandi piattaforme sono riuscite a ricoprire un ruolo predominante all'interno del mondo della ricerca universitaria grazie ad una serie di fattori concorrenti.

In primo luogo, sono riuscite a impadronirsi dell'infrastruttura. In senso etnografico²⁴¹, essa può essere definita come una «*struttura materiale sprofondata in un ambiente naturale, culturale e sociale e in prassi, abitudini condivise e norme informali e formali*». ²⁴² Un'infrastruttura di importanza fondamentale nell'ambito degli atenei italiani è senza dubbio la posta elettronica: è attraverso questo strumento che avviene ogni giorno la comunicazione di migliaia di dati, non solo riguardanti gli studenti o il personale, ma anche dati di ricerca appartenenti ad articoli o esperimenti scientifici.²⁴³

In una recente indagine, da un campione di 68 Atenei, è risultato che 31 di questi fanno ricorso ai servizi di posta elettronica offerti da Google, 17 a quelli offerti da Microsoft, mentre 20 fanno ricorso ad un servizio di posta elettronica interno all'Ateneo.²⁴⁴

Prendendo come esempio Google, si noti come questo alleghi tutta una serie di servizi complementari come Google Calendar, Google Drive o Google Docs, che, se da un lato rendono il servizio estremamente appetibile, dall'altro consegnano in mano ai colossi delle Big Tech un'ingente quantità di dati personali.²⁴⁵

²⁴⁰ Si v. C. Angiolini, R. Ducato, A. Giannopoulou, G. Schneider, «Remote Teaching During the Emergency and Beyond: Four Open Privacy and Data Protection Issues of 'Platformised' Education», p.48. e T. Fiebig et al., «Heads in the Clouds: Measuring the Implications of Universities Migrating to Public Clouds», 2021. <https://arxiv.org/abs/2104.09462>.

Si v. anche A. Watters, «Education technology and the age of surveillance capitalism», Hack Education, 28 agosto 2019, <http://hackededucation.com/2019/08/28/>: «*the kinds of data extraction and behavioral modification that Zuboff identifies as central to surveillance capitalism are part of Google and Facebook's education efforts, even if laws like COPPA prevent these firms from monetizing the products directly through advertising*».

²⁴¹ Si v. S.L. Star, «The Ethnography of Infrastructure», *American Behavioral Scientist* 43 3, 1999, pp. 377–391, <https://purl.archive.org/purl/mcpievatolocit/star>.

²⁴² M. C. Pievatolo, «Sulle spalle dei mercanti? Teledidattica e civiltà tecnologica», *bollettino tematico di filosofia politica*, 10 aprile 2022, p.9.

<https://doi.org/10.5281/ZENODO.6461431>.

²⁴³ Ibidem.

²⁴⁴ Ibidem.

²⁴⁵ Ibidem, p. 10.

Inoltre, piattaforme proprietarie come Google o grandi colossi del mondo dell'editoria scientifica, come ad esempio *Elsevier*, *Springer Nature* e *Clarivate*, hanno trovato il modo di controllare l'intero *workflow* dell'attività della ricerca, vale a dire l'iter attraverso il quale una ricerca scientifica vede la luce tramite la fase finale della pubblicazione.²⁴⁶ Questo iter si compone di diverse fasi: la prima fase è necessariamente quella di ricerca delle risorse economiche e tecnologiche necessarie, successivamente vi è la fase più importante, ovvero quella della ricerca: accademici e studiosi lavorano da soli o in gruppi di ricerca per formulare una proposta. La proposta viene presentata ad uno specifico editore e ad una specifica rivista, che grazie all'ausilio dei comitati scientifici andranno a fornire, tramite un meccanismo denominato *peer review*, un parere favorevole per la pubblicazione. L'articolo viene quindi pubblicato e distribuito. Sarà poi importante una valorizzazione dell'articolo, che spetterà tanto all'editore, con la diffusione di metadati di qualità, quanto all'autore tramite i canali a sua disposizione. Così facendo verrà aumentato il suo prestigio e contestualmente sarà possibile ottenere i finanziamenti per future ricerche.²⁴⁷

La prima delle immagini riportate mostra la ciclicità del work flow. La seconda, invece, mira a fornire una rappresentazione grafica di come questi operatori oligopolistici abbiano sostanzialmente inglobato ogni fase di questa attività.

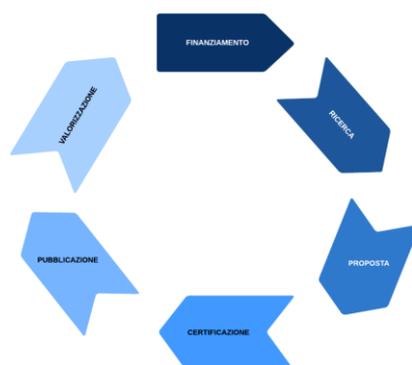


Figura 4: Il workflow. FONTE: G. Salucci, «Il flusso della pubblicazione scientifica», Academic Publishing Services, servizi e soluzioni per l'editoria accademica, 2009, 1, p.1.

²⁴⁶ G. Salucci, «Il flusso della pubblicazione scientifica», *Academic Publishing Services, servizi e soluzioni per l'editoria accademica*, 2019, 1,1.

<https://www.academic-publishing-services.it/flusso-della-pubblicazione-nella-editoria-accademica/>.

²⁴⁷ *Academic Publishing Services* (blog), «Il flusso della pubblicazione nella editoria accademica», 23 marzo 2019, consultabile al link: <https://www.academic-publishing-services.it/flusso-della-pubblicazione-nella-editoria-accademica/>.

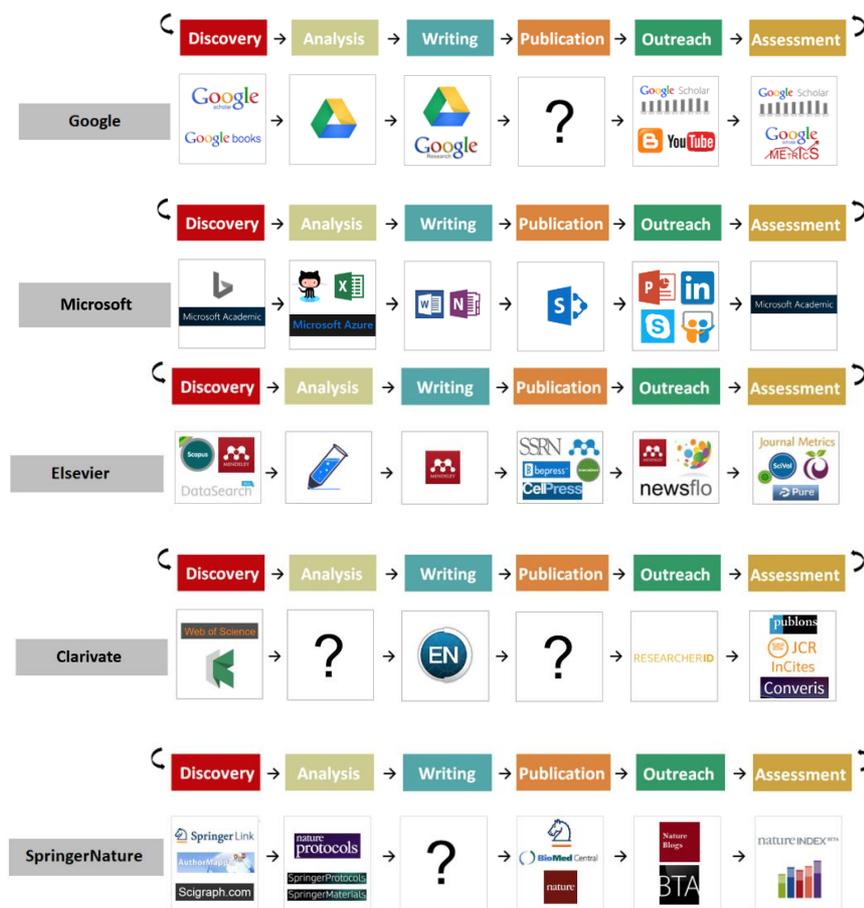


Figura 5: operatori oligopolistici e workflow. FONTE: B. Kramer, J. Bosman, «101 Innovations in Scholarly Communication - the Changing Research Workflow», 1805291 Bytes,figshare, 2015, <https://doi.org/10.6084/M9.FIGSHARE.1286826>.

In queste situazioni si verifica un fenomeno che in economia prende il nome di «lock-in», vale a dire una situazione in cui «un agente, un insieme di agenti, o un intero settore sono intrappolati all'interno di una scelta o di un equilibrio economico dai quali è difficile uscire, anche se sono disponibili alternative potenzialmente più efficienti».²⁴⁸ Nel caso del «vendor lock-in» un cliente (in questo caso l'Università o un ente di ricerca) è legato a un fornitore di servizi in maniera tale da essere quasi impossibile, dal punto di vista finanziario, legarsi a un altro fornitore.²⁴⁹

Gli operatori oligopolistici del mondo dell'editoria scientifica, come Elsevier, hanno inoltre aumentato il loro potere di controllo della ricerca tramite lo strumento

²⁴⁸ Per la definizione di «lock-in» si v. Enciclopedia Treccani:

[https://www.treccani.it/enciclopedia/lock-in_\(Dizionario-di-Economia-e-Finanza\)](https://www.treccani.it/enciclopedia/lock-in_(Dizionario-di-Economia-e-Finanza)).

²⁴⁹ B. Brems, K. Förstner, M. Goedicke, U. Konrad, K. Wannemacher, J. Kett, «Plan I - Towards a Sustainable Research Information Infrastructure», 21 gennaio 2021, p.4.

<https://zenodo.org/record/4454640>.

degli indicatori bibliometrici e degli indici citazionali. Nell'ambito dell'analisi scientometrica, infatti, vengono utilizzati questi sistemi matematico-statistici che hanno la finalità di misurare e valutare l'impatto delle pubblicazioni scientifiche, sia da un punto di vista quantitativo che qualitativo.²⁵⁰

Tra questi annoveriamo gli indici citazionali, ovvero un numero che esprime la quantità di citazioni ottenute da ciascuna pubblicazione. In particolare, l'idea di questo strumento si deve a Eugene Garfield,²⁵¹ il quale immaginava un meccanismo che permettesse agli scienziati e accademici di individuare le ricerche scientifiche più affidabili e rilevanti.

Sulla base di questo è poi nato il criterio dell'Impact Factor che *«misura il numero medio di citazioni ricevute, nell'anno di riferimento considerato, dagli articoli pubblicati da una rivista scientifica nei due anni precedenti: è pertanto un indicatore della performance dei periodici scientifici, che esprime l'impatto di una pubblicazione sulla comunità scientifica di riferimento»*.²⁵²

Le criticità sono iniziate quando le Università stesse hanno cominciato a valutare i propri ricercatori sulla base di tali indici: in particolar modo, i ricercatori che erano in grado di far pubblicare i loro saggi o monografie in riviste scientifiche con un alto fattore d'impatto erano valutati positivamente; pertanto, sempre più ricercatori hanno cercato di far pubblicare i propri risultati in suddette riviste. Le biblioteche, dal canto loro, sono state quindi spinte ad acquistare sempre più abbonamenti a queste riviste scientifiche. Si è creato perciò un vero e proprio oligopolio caratterizzato da una domanda inelastica, ovvero che né cresce né decresce al diminuire o all'aumentare dei prezzi. Gli oligopoli, poi, formano delle vere e proprie barriere all'entrata del mercato, che non permettono a nuove riviste scientifiche di entrare in gioco.²⁵³

Oggi, in Italia, il sistema di valutazione è gestito dall'Agenzia Nazionale di Valutazione del Sistema Universitario (ANVUR)²⁵⁴.

L'ANVUR svolge prevalentemente funzioni di valutazione esterna e di indirizzo, e la sua attività si declina nell'indicazione di criteri uniformi ai nuclei di valutazione, nella valutazione esterna della qualità della ricerca negli atenei italiani e nell'attività di supervisione dei programmi pubblici di finanziamento alle attività di ricerca.²⁵⁵ Nella

²⁵⁰ Per una definizione di «Indicatori Bibliometrici», si v. il link:

<http://biblioteche.unipv.it/home/risorse/indicatori-bibliometrici>.

²⁵¹ Garfield va ricordato anche per aver fondato l'Institute for Scientific Information nel 1960, ora proprietà di Clarivate.

²⁵² Per una definizione di «Impact Factor (IF)», si v. il link:

<http://biblioteche.unipv.it/home/risorse/indicatori-bibliometrici/impact-factor-if>.

²⁵³ R. Caso, «The Darkest Hour: Private Information Control and the End of Democratic Science», Trento Law and Technology Research Group Research Papers nr. 35, 2018, p. 19-20.

SSRN: <https://ssrn.com/abstract=3189519>

²⁵⁴ Si v. <https://www.anvur.it/>.

²⁵⁵ Più nello specifico, «L'Agenzia svolge le seguenti attività: a)Valuta la qualità dei processi, i risultati e i prodotti delle attività di gestione, formazione, ricerca, trasferimento tecnologico delle attività delle Università e degli Enti di Ricerca; b)Definisce i criteri e le metodologie per la valutazione delle sedi e dei corsi di studio, ivi compresi i dottorati di ricerca, i master e le scuole di specializzazione, ai fini dell'accreditamento periodico delle strutture da parte del Ministro; c)Esercita funzioni di indirizzo delle attività di valutazione demandate ai nuclei di ateneo; d)Predispone in collaborazione con i Nuclei le procedure per la rilevazione della valutazione della soddisfazione dei corsi da parte degli studenti;

valutazione dell'ANVUR, finalizzata alla procedura per l'abilitazione di professore universitario, i criteri di maggiore rilievo sono il conteggio delle citazioni e il numero di articoli pubblicati su due piattaforme specifiche.²⁵⁶ In particolare, L'ANVUR, per la valutazione dei settori bibliometrici, utilizza solamente le banche dati commerciali ISI WoS e Scopus per il calcolo degli indicatori di riferimento, rispettivamente di proprietà di Web of Science e Elsevier. Come già illustrato, Elsevier è il più grande editore al mondo e, secondo autorevole dottrina, «è in palese conflitto di interessi: pubblica riviste e libri scientifici e poi li valuta attraverso le proprie banche dati bibliometriche».²⁵⁷

2.2.2 Il ruolo del capitalismo della sorveglianza nel mondo della ricerca universitaria

I capitalisti della sorveglianza nel mondo della ricerca universitaria riescono a raccogliere due diverse categorie di dati: la prima riguarda i dati della ricerca, ovvero i dati generati dalle Università durante lo svolgimento dell'attività di ricerca; accanto ad essi si hanno poi i dati cosiddetti «grigi», ovvero i dati prodotti dall'Università fuori dall'attività di ricerca e che si riferiscono ai membri della comunità accademica.²⁵⁸

Secondo un report²⁵⁹ di SPARC²⁶⁰ del 2019, il mondo dell'editoria scientifica sta attualmente attraversando un momento di transizione: dalla fornitura di contenuti, i grandi colossi dell'editoria scientifica stanno iniziando a fornire agli istituti universitari

e)Elabora e propone al Ministro i requisiti quantitativi e qualitativi ai fini dell'istituzione, fusione o federazione ovvero soppressione di università o sedi distaccate, ovvero per l'attivazione, la chiusura o l'accorpamento di corsi universitari; f)Elabora, su richiesta del Ministro, i parametri di riferimento per l'allocazione dei finanziamenti statali, ivi inclusa la determinazione dei livelli essenziali di prestazione e dei costi unitari riferiti a specifiche tipologie di servizi; g)Valuta, sulla base dei risultati attesi e di parametri predefiniti, i risultati degli accordi di programma ed il loro contributo al miglioramento della qualità complessiva del sistema della ricerca; h)Valuta l'efficienza e l'efficacia dei programmi pubblici di finanziamento ed incentivazione alle attività didattiche, di ricerca e innovazione; i)Svolge su richiesta del Ministro ulteriori attività di valutazione nonché di definizione di standard di parametri e normativa tecnica». Si v. <https://www.anvur.it/anvur/missione/>.

²⁵⁶ Si v. Decreto Ministeriale 7 giugno 2012 n.76 (Regolamento recante criteri e parametri per la valutazione dei candidati ai fini dell'attribuzione dell'abilitazione scientifica nazionale per accesso alla prima e alla seconda fascia dei professori universitari, nonché le modalità di accertamento della qualificazione dei Commissari, ai sensi dell'articolo 16, comma 3, lettere a), b) e c) della legge 30 dicembre 2010, n.240, e degli articoli 4 e 6, commi 4 e 5, del decreto del presidente della Repubblica 14 settembre 2011, n. 222).

²⁵⁷ R. Caso, «La valutazione autoritaria e la privatizzazione della conoscenza contro la scienza aperta», Zenodo, 2022., p.5.

<https://doi.org/10.5281/zenodo.7396228>.

²⁵⁸ C. L. Borgman, «Open Data, Grey Data, and Stewardship: Universities at the Privacy Frontier», 2018, pp. 365-412,

<https://doi.org/10.15779/Z38B56D489>.

Sono ad esempio dati «grigi», quelli che si riferiscono ai risultati accademici, ai documenti di identità, sondaggi, video di sorveglianza, o che derivano dall'uso di internet.

²⁵⁹ C. Aspesi, N. Starr Allen, R. Crow, S. Daugherty, H. Joseph, J.T.W. McArthur, N. Shockey, «SPARC Landscape Analysis: The Changing Academic Publishing Industry – Implications for Academic Institutions», preprint, LIS Scholarship Archive, 3 aprile 2019. <https://doi.org/10.31229/osf.io/58yhb>.

²⁶⁰ SPARC è un'organizzazione non profit di advocacy che sostiene sistemi per la ricerca e l'istruzione che siano aperti «by default» ed equi «by design». Si v. il link <https://sparcopen.org/who-we-are/>.

sistemi di valutazione della ricerca e della produttività, nonché sistemi di gestione dell'apprendimento online.

Tutto ciò segna un vero e proprio passaggio ad un'attività di data analytics. La classica fetta di mercato appannaggio delle grandi multinazionali dell'editoria scientifica sta infatti vivendo un momento non particolarmente favorevole: gli studenti universitari acquistano libri di seconda mano, così come si registra che i gestori delle biblioteche tendono a non rinnovare gli abbonamenti a riviste scientifiche. Il tutto si colloca poi in un contesto in cui la digitalizzazione ha permesso un incremento della pirateria nel download non autorizzato di specifici contenuti. Le risposte a queste situazioni sono state, per un verso, scontate: si è implementata una politica di controllo ferreo di eventuali violazioni di copyright e si è scelto di abbassare i prezzi. Tuttavia, si registra anche come i grandi operatori oligopolistici come Elsevier si stiano trasformando in aziende di data analytics basate sui loro contenuti. È bene sin da subito sottolineare che l'attività tradizionale non viene abbandonata, ma semplicemente affiancata da questa nuova strategia di data analytics. Questo perché, non solo è possibile registrare un grande fatturato nel mondo dell'editoria scientifica, ma anche perché senza contenuti sarebbe sostanzialmente impossibile ottenere i dati su cui capitalizzare.²⁶¹

Grazie alla loro attività di analisi dei dati, per queste aziende si apre la pericolosa possibilità di influenzare invisibilmente e strategicamente le decisioni chiave dell'Università. I dati afferenti all'intera comunità accademica o relativi alle produzioni scientifiche rappresentano un potenziale valore di mercato di miliardi di dollari, che diventano migliaia di miliardi quando si parla anche di proprietà intellettuale.²⁶²

Nel report di SPARC si registrano dati empirici che dimostrano la volontà di Elsevier di spostarsi verso questo mercato: vi è infatti un'intenzione di fidelizzare anche le amministrazioni universitarie, gli organismi di finanziamento e i governi, attraverso l'implementazione di strumenti finalizzati a valutare la produttività della ricerca, ottimizzando le decisioni di finanziamento.

SPARC ipotizza diverse strategie che Elsevier potrebbe implementare²⁶³: tramite le sue banche dati sulle citazioni, potrebbe identificare quali ricercatori hanno più probabilità di diventare leader nel loro rispettivo campo e offrire loro un posto nei comitati editoriali, con un vantaggio competitivo di anni rispetto ad altri editori; potrebbe isolare nuove tendenze negli studi interdisciplinari, oppure individuare quale segmento delle singole discipline è più probabile che si evolva negli anni futuri, osservando i modelli di partecipazione ai progetti, la dimensione del team e le decisioni degli organismi di ricerca, così da andare a sua volta a guidare decisioni di finanziamento per ottenere una più veloce crescita nei campi di ricerca rilevati.

Elsevier, inoltre, già da tempo fornisce alle Università strumenti finalizzati a valutare la produttività di determinate ricerche. Tramite questi strumenti, non solo si può guidare l'allocazione delle risorse, ma è anche possibile guidare interi processi decisionali del mondo accademico, come assunzioni o promozioni di docenti o

²⁶¹ Si v. C. Aspesi, N. Starr Allen, R. Crow, S. Daugherty, H. Joseph, J.T.W. McArthur, N. Shockey, «SPARC Landscape Analysis: The Changing Academic Publishing Industry – Implications for Academic Institutions».

²⁶² Ibidem, p.5.

²⁶³ Ibidem, p. 14 e ss.

ricercatori.²⁶⁴ Conoscendo poi quali campi della ricerca sono più propensi a essere oggetto di tendenza, l'Università potrebbe meglio controllare l'allocazione dei fondi.²⁶⁵ Infine, Elsevier potrebbe iniziare ad effettuare il *text and data mining*²⁶⁶ sui dati raccolti e poi vendere la conoscenza a terze parti: questo è senza dubbio il passo più audace che può compiere, e non si hanno indizi del fatto che l'editore stia effettivamente per dirigersi verso questa direzione; tuttavia, non si può completamente escludere questo scenario.²⁶⁷

Resta inoltre preoccupazione la possibilità che vengano create delle piattaforme contenenti database di testi completi, trascrizioni di conferenze, thread di discussione o addirittura offerte di lavoro: tramite l'intelligenza artificiale, potrebbe essere possibile estrarre numerosi dati con cui valutare con maggior precisione la produttività di un dato ricercatore o dipartimento.²⁶⁸

Vanno sicuramente condivise le perplessità e problematicità collegate a queste possibilità evidenziate da SPARC: può un algoritmo che valuta la produttività sostituirsi *in toto* alle decisioni amministrative dell'Università? Va per altro sottolineato che non è detto che l'algoritmo si adatti ai valori e alla politica interna di un'Università. Ma la criticità che in questa sede pare più opportuno sottolineare è quella relativa alla tutela dei dati personali: i dati raccolti saranno venduti a terze parti o forniti ad altre attività commerciali svolte dallo stesso editore? C'è la possibilità che vengano ceduti al governo, o che il governo stesso possa chiedere che questi siano condivisi per ragioni di interesse pubblico?²⁶⁹

Secondo SPARC, Elsevier, in questo processo, si trova in un'enorme posizione di vantaggio, dal momento che può fornire tanto pubblicazioni di riviste scientifiche, quanto strumenti di data analytics. Ancora una volta, le Università si trovano in uno stato di vendor lock-in, dal momento che i costi da sostenere per l'acquisto di servizi da più fornitori sono difficili da giustificare. Ecco che nel mercato dell'analisi dei dati, Elsevier si presta a diventare ben presto un vero e proprio monopolista: mentre nel mercato delle riviste scientifiche, si crea una forte agglomerazione in oligopoli in cui residua

²⁶⁴ C. Aspesi, N. Starr Allen, R. Crow, S. Daugherty, H. Joseph, J.T.W. McArthur, N. Shockey, «SPARC Landscape Analysis: The Changing Academic Publishing Industry – Implications for Academic Institutions», p 17.

²⁶⁵ Ibidem.

²⁶⁶ Si v. la definizione data da Springer Nature: «TDM (*Text and Data Mining*) is the automated process of selecting and analyzing large amounts of text or data resources for purposes such as searching, finding patterns, discovering relationships, semantic analysis and learning how content relates to ideas and needs in a way that can provide valuable information needed for studies, research, etc», al link: <https://www.springernature.com/gp/researchers/text-and-data-mining>.

²⁶⁷ C. Aspesi, N. Starr Allen, R. Crow, S. Daugherty, H. Joseph, J.T.W. McArthur, N. Shockey, «SPARC Landscape Analysis: The Changing Academic Publishing Industry – Implications for Academic Institutions», p 17.

²⁶⁸ C. Aspesi, A. Brand, «In Pursuit of Open Science, Open Access Is Not Enough», *Science* 368, fasc. 6491,8 maggio 2020, pp. 574-777, <https://doi.org/10.1126/science.aba3763>.

²⁶⁹ C. Aspesi, N. Starr Allen, R. Crow, S. Daugherty, H. Joseph, J.T.W. McArthur, N. Shockey, «SPARC Landscape Analysis: The Changing Academic Publishing Industry – Implications for Academic Institutions», p. 32.

ancora spazio per gli editori di nicchia, nel mondo dell'analisi dei dati gli utenti cercano la miglior soluzione possibile, indipendentemente dal costo.²⁷⁰

Per incrementare la sua forte posizione di mercato, Elsevier sta inoltre pensando di aggregare più fonti di dati tramite la creazione di piattaforme differenziate, che vanno, ad esempio, da strumenti di supporto alla comunità medica a strumenti per facilitare il dialogo tra esperti dell'ingegneria petrolifera. Così facendo, vengono costruite economie di scala, e difficilmente altre aziende avranno le risorse per operare come concorrenti sul mercato.²⁷¹

Tutto ciò genera gravissimi problemi in termini di perdita di diversificazione: una singola azienda, con il suo singolo algoritmo – tutt'altro che privo di condizionamenti e pregiudizi – potrebbe influenzare il mondo della ricerca, indicando quali dipartimenti meritano un budget maggiore, quale ricercatore merita di avanzare nella carriera universitaria, oppure quali ricerche finanziare.²⁷²

Jeff Pooley²⁷³ chiama questo fenomeno «*surveillance publishing*», poiché gli editori del calibro di Elsevier ricavano una sostanziale parte del proprio fatturato da prodotti di previsione, ovvero dal valore comportamento estratto. Esso è qualificato come un fenomeno rientrante nel più ampio concetto di «economie di sorveglianza» attribuibile ai giuristi Mariano-Florentino Cuéllar e Aziz Huq²⁷⁴, che descrivono con questo termine il fenomeno per cui interi settori scelgono di includere il surplus comportamentale all'interno dei loro modelli di business.

Secondo la lettura di Pooley, Elsevier è già un editore di sorveglianza: negli anni ha implementato una strategia di acquisizioni, disinvestimenti e lanci di prodotti che oggi gli permettono di raccogliere il surplus comportamentale in ogni fase del workflow: ad esempio, come è stato già osservato, traccia i risultati di laboratorio con Hivebench, acquistata nel 2016, ma riesce anche a coprire l'ultima fase della catena, tracciando l'impatto dell'articolo tramite Plum Analytics, acquistata nel 2017.²⁷⁵

Si rischia di lasciare il futuro della conoscenza alle sale riunioni aziendali: le aziende tecnologiche potrebbero, tra l'altro, dirigere il dibattito pubblico sulla base di interessi politici, piuttosto che di informazioni scientifiche.²⁷⁶

Sarebbe invece auspicabile che fossero le Università stesse a gestire il sistema delle metriche per la valutazione del personale accademico: la valutazione, infatti,

²⁷⁰ C. Aspesi, N. Starr Allen, R. Crow, S. Daugherty, H. Joseph, J.T.W. McArthur, N. Shockey, «2020 Update: SPARC Landscape Analysis & Roadmap for Action», preprint LIS Scholarship Archive, 22 giugno 2020, p.18-19.

<https://doi.org/10.31229/osf.io/2pwft>.

²⁷¹ Si v. C. Aspesi, A. Brand, «In Pursuit of Open Science, Open Access Is Not Enough».

²⁷² C. Aspesi, N. Starr Allen, R. Crow, S. Daugherty, H. Joseph, J.T.W. McArthur, N. Shockey, «2020 Update: SPARC Landscape Analysis & Roadmap for Action», p.21.

²⁷³ J. Pooley, «Surveillance Publishing».

²⁷⁴ M.F. Cuéllar, H. Aziz, «Economies of Surveillance» Harvard Law Review 133, no. 4, 2020, pp. 1280-1336.

²⁷⁵ J. Pooley, «Surveillance Publishing», p. 43.

²⁷⁶ K. Maex, «Protect independent and public knowledge», discorso tenuto l'8 gennaio 2021 per il 389° *dies natalis* dell'Università di Amsterdam.

<https://www.eua.eu/downloads/content/speech-karen-maex---dies-2021.pdf>

dovrebbe avvenire sulla base di criteri corrispondenti ai valori perseguiti dall'Università stessa.²⁷⁷

2.2.3 L'esperimento di Cody Hanson

Nel gennaio del 2019, Cody Hanson, bibliotecario presso l'Università del Minnesota, ha deciso di condurre un'indagine per verificare le operazioni di tracciamento svolte dalle piattaforme di editoria²⁷⁸. Dopo aver raccolto una lista di 100 Digital Object Identifiers (DOIs) più frequentemente utilizzati presso l'Università del Minnesota nei due anni precedenti, provenienti da quindici diverse piattaforme di editoria, e dopo aver scelto l'articolo più frequentemente consultato dalla lista di ciascuna delle quindici piattaforme, ha scaricato un archivio completo della pagina dell'articolo. Con Ghostery, un software che blocca gli annunci, ha analizzato il codice di terze parti caricato sulla pagina. Attraverso questa indagine, è emerso che in media, ogni sito di editori aveva diciotto risorse di JavaScript di terze parti caricate sulle loro pagine di articoli. L'unica esente è stata InformPubsOnline, mentre alcune ne avevano più di 100.

Le terze parti che inseriscono il proprio JavaScript riescono così ad avere accesso all'intero documento, leggendo i contenuti della pagina, nonché a ogni azione compiuta dall'utente, comprese le sue ricerche nella piattaforma dell'editore. Almeno quattro delle quindici piattaforme hanno incluso il codice di Facebook sulla pagina dell'articolo, mentre quattordici su quindici hanno incluso il codice di Google. Così facendo, si registra un'enorme quantità di dati tramite un *fingerprinting del browser* e vengono raccolti tutti i metadati possibili, che, presi insieme, rendono possibile l'identificazione dell'utente. Talvolta vengono creati dei veri e propri «profili ombra»: l'attività dell'utente viene ricombinata con altre sulla base di un cookie o di un indirizzo IP, così che, quando questi si autenticherà ad esempio a Google, tutta l'attività passata connessa a quell'indirizzo IP sarà associata proprio a quell'utente, a prescindere che si sia o meno autenticato nel sito della casa editrice.²⁷⁹

Tutto ciò solleva molti dubbi con riferimento alla libertà accademica, dal momento che questo tracciamento è idoneo a mettere i ricercatori a rischio in paesi in cui la ricerca è profondamente guidata da scelte politiche di fondo.²⁸⁰

La libertà accademica, infatti, rappresenta il punto di intersezione tra diritto alla privacy e diritto alla libera manifestazione del pensiero: il personale accademico deve

²⁷⁷ C. Aspesi, N. Starr Allen, R. Crow, S. Daugherty, H. Joseph, J.T.W. McArthur, N. Shockey, «SPARC Roadmap for Action: Academic Community Control of Data Infrastructure» p.7.

²⁷⁸ Si v. C. Hanson, «User Tracking on Academic Publisher Platforms», Prepared for the Coalition for Networked Information Spring 2019 Member Meeting, St. Louis, Missouri, April 8-9, 2019. <https://www.codyh.com/writing/tracking.html>.

²⁷⁹ Si v. P. O'Brien, S.W.H. Young, K. Arlitsch, K. Benedict, «Protecting Privacy on the Web: A Study of HTTPS and Google Analytics Implementation in Academic Library Websites», Online Information Review 42, fasc. 6, 13 settembre 2018, pp. 734-751. <https://doi.org/10.1108/OIR-02-2018-0056>.

²⁸⁰R. Siems, «When your journal reads you – user tracking on science publisher platforms», Elephant in the Lab, 2021. <https://doi.org/10.5281/zenodo.4683778>.

essere libero di condurre la ricerca, sviluppare ipotesi e persino sviluppare dibattiti portando alle estreme conseguenze le proprie tesi,²⁸¹ senza dover temere l'intrusione degli editori della sorveglianza.

Non resta quindi che prendere atto del fatto che ormai

*«le big tech della comunicazione scientifica hanno il controllo di tutto: infrastrutture, algoritmi e software applicati ai dati. Usano il proprio potere computazionale e le tecniche del c.d. capitalismo della sorveglianza per prevedere e, in ultima analisi, influenzare il comportamento dei ricercatori, dei professori e delle Università».*²⁸²

2.3 Il mondo dell'istruzione

2.3.1 *Emergency remote teaching* e capitalismo della sorveglianza

Le scuole e le Università, anche quando svolgono l'attività di istruzione e formazione in senso tradizionale, trattano una grandissima quantità di dati personali, relativi a studenti, genitori e personale. I dati raccolti, utilizzati e trattati in ambito scolastico vengono spesso definiti «dati relativi all'istruzione», i quali

*«consistono in dati registrati nei sistemi d'informazione sugli studenti, ad esempio il rendimento scolastico, il nome dei genitori, i voti ricevuti nonché i dati di microlivello generati con l'utilizzo di strumenti digitali. Quando gli studenti interagiscono con dispositivi digitali generano tracce digitali come i clic del mouse, i dati sulle pagine aperte, la tempistica degli eventi di interazione o le sequenze dei tasti premuti».*²⁸³

Con la dichiarazione da parte dell'Organizzazione Mondiale della Sanità della pandemia da Covid-19 nel marzo 2020, le Università e le scuole italiane – e non solo – per finalità di contenimento del virus, sono state costrette ad abbandonare gli spazi fisici dell'Università e passare a un diverso modello di didattica denominato «*didattica a distanza*» (DaD).²⁸⁴

²⁸¹ C.L. Borgman, «Open Data, Grey Data, and Stewardship: Universities at the Privacy Frontier», p. 390. <https://doi.org/10.15779/Z38B56D489>.

²⁸² R. Caso, «La valutazione autoritaria e la privatizzazione della conoscenza contro la scienza aperta», p. 6.

²⁸³ Commissione europea, Direttorato generale per l'istruzione, della gioventù, dello sport e della cultura, Ethical guidelines on the use of artificial intelligence (AI) and data in teaching and learning for educators, Publications Office of the European Union, 25 ottobre 2022, consultabile al link: <https://data.europa.eu/doi/10.2766/153756>.

²⁸⁴ Secondo uno studio condotto dall'UNESCO, nell'aprile del 2020, 191 paesi hanno disposto la chiusura delle scuole a livello nazionale, coinvolgendo circa 1.5 miliardi di bambini a livello globale. Per consultare lo studio, si v. UNESCO and McKinsey & Company, Covid-10 Response – Remote Learning Strategy, 2020. Qualcosa di simile è avvenuto anche nel mondo dell'istruzione superiore, con la sospensione delle lezioni in presenza fino all'estate del 2020, e in alcuni casi fino alla fine dell'anno. Si v. OECD, The State of Higher Education: One Year into the COVID-19 Pandemic, Organisation for Economic Co-operation and Development 2021, consultabile al link: <https://www.oecd-ilibrary.org/>.

Il Ministero dell’Istruzione italiano, nella nota inviata il 17 marzo 2020 alle scuole di ogni ordine e grado, contenente le prime indicazioni operative per le attività di organizzazione della DaD, descrive la didattica a distanza come:

*«il collegamento diretto o indiretto, immediato o differito, attraverso videoconferenze, videolezioni, chat di gruppo; la trasmissione ragionata di materiali didattici, attraverso il caricamento degli stessi su piattaforme digitali e l’impiego dei registri di classe in tutte le loro funzioni di comunicazione e di supporto alla didattica, con successiva rielaborazione e discussione operata direttamente o indirettamente con il docente, l’interazione su sistemi e app interattive educative propriamente digitali».*²⁸⁵

La didattica a distanza può essere svolta in modalità sincrona e modalità asincrona. Nel primo caso, gli studenti seguono la lezione collegati in videoconferenza, quindi vi è una presenza contestuale – seppur a distanza – di docenti e studenti, è quindi possibile per gli studenti porre domande o comunque partecipare attivamente alla lezione tramite la chat, oppure semplicemente attivando l’utilizzo del microfono del proprio dispositivo mobile. Nel secondo caso, invece, la lezione è registrata dal docente e successivamente resa disponibile agli studenti. In questo caso, dunque, studenti e docenti non sono in grado di interagire; pertanto, si rende necessario l’utilizzo di altri strumenti che consentano agli studenti di porre domande o semplicemente conversare con il docente. Sono poi disponibili soluzioni «ibride»: è possibile, infatti, registrare la lezione sincrona per metterla a disposizione degli studenti che necessitino di seguirla in un secondo momento.

A livello ministeriale è stata esplicitamente indicata la necessità di dover ricorrere a piattaforme digitali per finalità didattiche, tuttavia, il mondo della formazione italiano non conosceva ancora un florido dibattito sull’applicazione della tecnologia all’insegnamento, ed a ciò si affiancava anche una scarsa preparazione tecnica del corpo docenti.²⁸⁶ Non deve quindi sorprendere come, ad eccezione di pochi esempi²⁸⁷, le scuole e Università italiane abbiano dovuto fare ricorso alle piattaforme teledidattiche di *Microsoft* e *Google*, già identificati come i grandi operatori monopolistici nel capitalismo della sorveglianza.

Stando ad un’inchiesta condotta da *Altreconomia*²⁸⁸ sulla base di dati raccolti dal MIUR, le 7700 scuole che hanno fornito elementi (su poco più di 8000 istituti pubblici) hanno fatto ricorso, per la DaD, a *Google Suite for Education* circa nell’86,3% dei casi, a *Microsoft* nel 18%, a *Weschool* il 6,2%. La voce «altro» fa riferimento ad altre piattaforme non rientranti tra quelle citate. Si noti, peraltro, l’utilizzo di piattaforme «generaliste», come *WhatsApp* e *Zoom*.

²⁸⁵ MIUR, Ministero dell’istruzione e del merito, «Coronavirus, emanata la nota con le indicazioni operative per la didattica a distanza», 17 marzo 2020, consultabile al link <https://www.miur.gov.it/web/guest/-/coronavirus-emanata-la-nota-con-le-indicazioni-operative-per-la-didattica-a-distanza>.

²⁸⁶ P. Monella, «Istruzione e GAFAM: dalla coscienza alla responsabilità», *Umanistica Digitale* No. 11,25 gennaio 2022, pp. 27-45, p. 40, <https://doi.org/10.6092/ISSN.2532-8816/13685>.

²⁸⁷ Si v., ad esempio, il Politecnico di Torino.

²⁸⁸ S. Zoja, «La scuola italiana al mercato dei dati. Così il controllo sulla didattica rafforza lo strapotere delle multinazionali», *Altreconomia*, marzo 2022.

LE PIATTAFORME UTILIZZATE PER SVOLGERE LE LEZIONI A DISTANZA DALLE SCUOLE ITALIANE

Secondo il Miur Google è stata scelta in 6.614 istituti su un totale di circa 8mila, oltre l'86% dei casi

	Descrizione	Numero scuole	Incidenza
Tipo di piattaforma utilizzata	Google Suite for Education	6.614	86,28%
	Microsoft 365 Education	1.381	18,01%
	Weschool	473	6,17%
	Altro	1.126	14,69%
Altri servizi di videoconferenza utilizzati, oltre a quelli resi disponibili dalle piattaforme	GoToWebinar/GoToMeeting	2.816	36,73%
	WhatsApp	2.519	32,86%
	Zoom	2.442	31,85%
	Skype	984	12,84%
	Webex	607	7,92%
	Jitsi	556	7,25%
	Altro	1.987	25,92%
Altri strumenti digitali utilizzati in aggiunta o in alternativa ai precedenti	Registro elettronico	7.579	98,97%
	Repository per materiali didattici su cloud (es. Dropbox, Google Drive, iCloud, pCloud, etc.)	5.296	69,08%
	Piattaforme di libri di testo digitali	4.159	54,25%
	Social network aperto (es. Facebook, Twitter Instagram, etc.)	1.667	21,75%
	Moodle	902	11,77%
	Learning Management System o social network chiuso (es. Edmodo, Fidenia, etc.)	850	11,09%
	Altro	506	6,60%

Fonte: elaborazione a cura di *Altreconomia* sulla base dei dati forniti dal ministero dell'Istruzione, 2022

Anche nel mondo universitario si è registrata la medesima tendenza²⁸⁹; in realtà, è possibile parlare di un terreno che di per sé era già estremamente fertile: i grandi colossi delle piattaforme avevano già abbondantemente colonizzato intere infrastrutture ed ecosistemi dell'editoria scientifica, non deve quindi sorprendere come, con la pandemia, milioni di studenti universitari abbiano dovuto fare ricorso alle grandi piattaforme proprietarie della galassia GAFAM per lo svolgimento delle attività didattiche.

Se è vero che nell'ambito universitario molte Università già disponevano di strumenti tecnologici di supporto alla didattica²⁹⁰, la didattica a distanza, sviluppatasi in

²⁸⁹ Si v. C. Angiolini, R. Ducato, A. Giannopoulou, G. Schneider, «Remote Teaching During the Emergency and Beyond: Four Open Privacy and Data Protection Issues of 'Platformised' Education».

²⁹⁰ Basti pensare, ad esempio, alle «comunità moodle», in cui i docenti non solo caricano materiali didattici, ma possono anche richiedere agli studenti di partecipare attivamente a dibattiti sul cd. «forum», traendo dalla partecipazione un criterio di assegnazione del voto finale. Le Università già da tempo si servono di piattaforme proprietarie per lo svolgimento del c.d. «learning analytics», ovvero uno strumento di monitoraggio dell'attività degli studenti online, tipicamente come parte di un sistema di gestione dell'apprendimento, che, sebbene giustificato in termini di supporto agli studenti e promozione di gruppi vulnerabili e svantaggiati, potrebbe essere considerato principalmente guidato dalle logiche dei sistemi di audit nazionali imposti all'istruzione superiore. Per un

seguito all'emergenza pandemica, va considerata un fenomeno autonomo. Non va infatti sottovalutata la velocità con cui intere scuole e Università hanno abbandonato le aule per svolgere le attività accademiche online, così come va sottolineato che gli strumenti precedentemente utilizzati erano sì un sussidio alla didattica, ma non la sostituivano in tutte le sue componenti.²⁹¹ Con l'emergenza della pandemia da Covid-19, intere attività didattiche sono state spostate su piattaforme, che peraltro all'inizio non offrivano tutti gli strumenti necessari, costringendo quindi i soggetti interessati ad utilizzare più piattaforme per poter svolgere le attività in maniera completa. Si parla, in questo caso, di «*platformisation of education*», ovvero «*istruzione delle piattaforme*».²⁹² L'accelerazione pandemica ha quindi contribuito a rendere ancora più evidente l'importanza delle tecnologie digitali nel mondo dell'istruzione.²⁹³

La didattica a distanza così strutturata fa sostanzialmente ricorso a un *cloud computing*²⁹⁴, che risponde alle esigenze di risorse di calcolo materiali e immateriali, rendendole disponibili e condivisibili a richiesta, senza obbligare l'utente ad acquistarle o amministrarle; quando però si sceglie di affidarsi al cloud dei grandi oligopolisti del capitalismo della sorveglianza, non si fa altro che affidare i propri dati personali a chi, con molta probabilità, decide di venderli o comunque comunicarli a terzi.²⁹⁵ Fenomeni come l'effetto rete, le economie di scala e il controllo di miliardi di dati personali permettono inoltre a queste grandi piattaforme proprietarie di controllare i flussi di dati generati dagli utenti, e in ultima istanza di orientarne le azioni sulla base di algoritmi.²⁹⁶

Nel prossimo capitolo verrà affrontato con maggiore approfondimento il problema della tutela dei dati personali nell'ambito della didattica a distanza svolto su queste piattaforme proprietarie, con particolare attenzione al problema del trasferimento di detti dati personali in territori extra UE, in particolar modo negli Stati Uniti. Infatti, merita particolare attenzione il problema del controllo statale dei dati raccolti per finalità di sicurezza nazionale, si guarderà dunque con dettaglio all'evoluzione giurisprudenziale in materia, grazie all'intervento della Corte di Giustizia dell'Unione Europea nella sua attività di interpretazione e applicazione del General Data Protection Regulation. Anche oltreoceano, negli Stati Uniti, gli istituti e i distretti scolastici hanno iniziato a dubitare che i grandi capitalisti della sorveglianza nel mondo dell'istruzione come Google rispettino la normativa a tutela della privacy.²⁹⁷ Google,

approfondimento, si v. L. Gourlay, «Surveillance and Datafication in Higher Education: Documentation of the Human», *Postdigit Sci Educ*, 2022.

<https://doi.org/10.1007/s42438-022-00352-x>.

²⁹¹ C. Angiolini, R. Ducato, A. Giannopoulou, G. Schneider, «Remote Teaching During the Emergency and Beyond: Four Open Privacy and Data Protection Issues of 'Platformised' Education», p. 47.

²⁹² *Ibidem*.

²⁹³ L. Piromalli, «L'università digitale», Roma, Carocci editore, 2023, p. 14.

²⁹⁴ Il termine *cloud computing*, o *cloud*, «non individua solo la capacità di archiviare in remoto, ma anche e soprattutto la possibilità di usufruire di risorse di calcolo e di applicativi situati su macchine diverse e distanti da quella che si sta usando». Si v. G. Pascuzzi, «Il diritto dell'era digitale», p. 259.

²⁹⁵ Si v. M. C. Pievatolo, «Sulle spalle dei mercanti? Teledidattica e civiltà tecnologica», *bollettino tematico di filosofia politica*, 10 aprile 2022,

<https://doi.org/10.5281/ZENODO.6461431>.

²⁹⁶ *Ibidem*.

²⁹⁷ Per un approfondimento su alcuni reclami di distretti scolastici statunitensi contro Google e sull'idoneità della normativa statunitense in materia di privacy a contrastare l'attività di Google nel mondo

infatti, pur dovendosi conformare alle leggi federali statunitensi, ha continuato a perpetrare una politica di noncuranza rispetto alle norme in materia di privacy degli studenti.²⁹⁸

Durante l'esperienza didattica, infatti, centinaia di migliaia di informazioni vengono implicitamente o esplicitamente condivise: credo religioso, orientamento politico, difficoltà nell'apprendimento, rendimento scolastico, eventuali situazioni familiari di disagio. In questa sede, si ritiene necessario segnalare che le privacy policy di molte di queste piattaforme risultano estremamente vaghe o comunque non trasparenti, perciò risulta spesso complicato comprendere la finalità del trattamento e la base giuridica dello stesso.²⁹⁹

Il discorso si complica quando si parla della scuola, visto che le piattaforme riescono a trattare dati che riguardano bambini e minori. Il rischio è che la grande mole di informazioni così raccolte seguano il percorso del fanciullo in tutte le fasi dell'istruzione, fino all'ingresso nel mondo del lavoro, condizionando il curriculum e le scelte di vita dei bambini.³⁰⁰ Peraltro, nel caso dell'istruzione primaria, l'uso di una determinata architettura tecnologica può portare alla creazione di dipendenza e abitudine a determinati software e tecnologie, trasformando gli studenti in potenziali clienti per il futuro.³⁰¹

Oltre le criticità in materia di protezione dei dati personali, la diffusione dell'utilizzo di queste piattaforme fa sorgere il rischio che i grandi capitalisti della sorveglianza, servendosi dell'utilizzo dell'«intelligenza delle macchine» descritta al capitolo precedente, riescano ad operare un condizionamento culturale della didattica stessa.³⁰² Le aziende che forniscono servizi di edtech partecipano non solo alla (re)infrastrutturazione tecnologica delle istituzioni educative, ma anche alle attività di progettazione educativa e culturale, operando nella costruzione pratica e culturale del governo del mondo dell'istruzione in direzione imprenditoriale.³⁰³ L'incursione di capitalisti della sorveglianza come Google nell'istruzione rischia di svalutare il ruolo dei docenti, tradizionalmente considerati fonte del sapere ed esperti in pedagogia.³⁰⁴

dell'istruzione, si v. D. G. Krukta, R.M. Smits, T. A. Wilhelm, «Don't be evil: should we use Google in schools?», *TechTrends*. 65(4), 2021, pp. 421–431, p. 423.

doi:10.1007/s11528-021-00599-4.

²⁹⁸ Ibidem.

²⁹⁹ Si v. R. Ducato, G. Priora, C. Angiolini, A. Giannopoulou, B.J. Jutte, G. Noto La Diega, L. Pascauti, G. Schneider, «Didattica di emergenza o Emergency Remote Teaching: un'analisi empirica in tema di privacy e diritto d'autore dei termini e condizioni dei servizi online più diffusi» e il III capitolo del presente lavoro.

³⁰⁰ Consiglio d'Europa, Consultative committee of the convention for the protection of individuals with regard to automatic processing of personal data, Convention 108, Children's Data Protection in Education Systems: Challenges and Possible Remedies, 15 novembre 2019, p.49, consultabile al link: <chrome-extension://efaidnbmninnibpcjpcglclefindmkaj/https://rm.coe.int/t-pd-2019-06final-eng-report-children/1680a01b47>.

³⁰¹ E. Celeste, G. De Gregorio, «Towards a Right to Digital Education? Constitutional Challenges of Edtech», *JIPITEC* 234 para 1, 14,2023, pp. 234-250, p. 245.

<https://www.jipitec.eu/issues/jipitec-14-2-2023/5735>.

³⁰² S. Zoja, «La scuola italiana al mercato dei dati. Così il controllo sulla didattica rafforza lo strapotere delle multinazionali».

³⁰³ L. Piromalli, «L'università digitale», p. 64.

³⁰⁴ D. G. Krukta, R.M. Smits, T. A. Wilhelm, «Don't be evil: should we use Google in schools?», p. 426.

Il processo di «datificazione» descritto nel capitolo precedente riguarda oggi anche il mondo dell'istruzione, e trasforma l'insegnamento e l'apprendimento, fino alla creazione di una vera e propria industria globale dell'istruzione, dominata da organizzazioni for profit che hanno costruito un ampio reticolo di app e piattaforme che inglobano ogni fase dell'attività didattica.³⁰⁵ In questo senso, l'emergenza pandemica è stata una vera e propria «*opportunità catalitica*» per la penetrazione delle aziende edtech nel mondo dell'istruzione e per l'implementazione di politiche *market-oriented*.³⁰⁶

Complice di questo clima è stata anche l'attenzione delle Università al monitoraggio della performance e la mercificazione della conoscenza. Secondo alcuni, tramite l'attività di tracciamento e monitoraggio dei dati sarebbe infatti possibile migliorare le performance di attori e sistemi, così da rendere le attività di insegnamento e apprendimento più efficaci.³⁰⁷ La datificazione della didattica, abilitata dalle piattaforme, potrebbe tuttavia esacerbare le criticità legate all'attenzione ossessiva nei confronti di ranking e classifiche. Il rischio è che si introducano misure di performance in tempo reale con una crescente sorveglianza degli studenti e del personale accademico e scolastico.³⁰⁸

È stato inoltre osservato³⁰⁹ che l'utilizzo di algoritmi nel mondo dell'istruzione superiore, implementati per supporto agli studenti, ad esempio per tenere traccia di eventuali miglioramenti nel rendimento scolastico, o per ausilio ai professori, per finalità di didattica personalizzata, mettono a rischio l'indipendenza del mondo accademico stesso. Il funzionamento degli algoritmi è infatti non trasparente e discriminatorio: «*algorithms are de facto by definition discriminatory: they necessarily discriminate to have a meaning in the world*».³¹⁰

Ciò che maggiormente sorprende, e che in questa sede si guarda con sospetto, è che la scelta di utilizzare particolari piattaforme proprietarie per far fronte alle esigenze di contenimento del virus sia stata caldeggiata dallo stesso Ministero dell'Istruzione italiano: nel periodo dal 2020 al 2021, infatti, nel sito dedicato alla DaD venivano indicate solo tre piattaforme private: Google Suite for Education Office 365 Education A1 di Microsoft e WeSchool di TIM.³¹¹ Non solo: ad ottobre 2021 tanto il Ministero dell'Istruzione quanto la Conferenza dei Rettori delle Università Italiane hanno, rispettivamente, siglato con protocollo d'intesa con Apple³¹² e rinnovato la convenzione con Microsoft.

³⁰⁵ B. Williamson, «Datificazione e governo algoritmico dell'Università durante e dopo il Covid 19», Roars, 3 luglio 2020,

<https://www.roars.it/datificazione-e-governo-algoritmico-delluniversita-durante-e-dopo-il-covid-19/>.

³⁰⁶ L. Piromalli, «L'università digitale», p. 65.

³⁰⁷ Ibidem, p. 56.

³⁰⁸ B. Williamson, «Datificazione e governo algoritmico dell'Università durante e dopo il Covid 19».

³⁰⁹ K. Maex, M. Bakker, «The university in the age of platforms and algorithms» in A. M. Cauce, Y. Flückiger, B. van der Zwaan (Eds) *Universities as fifth Power? Opportunities, Risks and Strategies*, Geneva, The Glion Colloquium, Volume Nr. 13, 2022, p.42.

<https://glion.org/universities-as-fifth-poweropportunities-risks-and-strategies/>.

³¹⁰ Ibidem.

³¹¹ P. Monella, «Istruzione e GAFAM: dalla coscienza alla responsabilità», p. 40.

³¹² Protocollo d'intesa tra Ministero dell'Istruzione, Apple Distribution International Limited e Osservatorio Permanente Giovani – Editori, 4 gennaio 2021, consultabile al link:

La problematicità di questo approccio è brillantemente descritta da Monella:

*«La formazione va considerata un settore strategico sia del Paese sia dell'Unione Europea, "per l'impatto che ha sul progresso materiale e spirituale della società". Di conseguenza, le istituzioni pubbliche non possono 'appaltarne' le infrastrutture (anche digitali) ad aziende multinazionali estere e disinteressarsene, così come non appaltano le forze armate, la pubblica sicurezza, la sanità e la previdenza sociale».*³¹³

2.3.2 Il fenomeno dell'*e-proctoring*

Al fine di garantire un regolare svolgimento degli esami e di ottenere risultati e valutazioni attendibili³¹⁴, nell'ambito della DaD, soprattutto Universitaria, si è fatto uso di strumenti di cosiddetto *e-proctoring*.³¹⁵

Nell'inglese americano «*proctor*» descrive la persona incaricata di svolgere la sorveglianza durante gli esami, dunque con il termine *e-proctoring* si intende descrivere un sistema finalizzato a garantire la validità degli esami svolti in modalità scritta e online, monitorando gli studenti tramite la webcam e il microfono dei dispositivi elettronici.³¹⁶ I software per l'*e-proctoring* sono stati forniti per la maggior parte da società private sotto licenza, come nel caso di software come *Proctorio* e *Respondus*. Si tratta di software che si servono di particolari algoritmi in grado non solo di registrare l'attività della webcam e del microfono e dei siti web visitati, ma anche di ricavare le misure corporee e rilevare ogni movimento che possa essere indizio di un non onesto svolgimento dell'esame. Infatti, i creatori del software *Proctorio* individuano l'attività del suddetto software come essenziale per «*proteggere la reputazione della tua istituzione*»³¹⁷ ed «*essenziale per proteggere il valore di un titolo o corso di Laurea*».³¹⁸

Tali strumenti spostano il luogo dello svolgimento dell'esame dall'ambiente universitario a quello dell'interno delle mura domestiche, spesso richiedendo una registrazione degli ambienti circostanti.³¹⁹ I docenti hanno accesso a tutti i dati così

<https://www.miur.gov.it/-/protocollo-di-intesa-tra-ministero-istruzione-apple-distribution-international-limited-e-osservatorio-permanente-giovani-editori>.

³¹³ P. Monella, «Istruzione e GAFAM: dalla coscienza alla responsabilità», p. 35.

³¹⁴ A. Giannopoulou, R. Ducato, C. Angiolini, G. Schneider, «From data subjects to data suspects: challenging e-proctoring systems as a university practice», *JIPITEC* 278, para 1, 14, 2023, pp. 278-306, p. 280.

<https://www.jipitec.eu/issues/jipitec-14-2-2023/5737>.

³¹⁵ Tali strumenti erano già utilizzati in alcune realtà accademiche, si v. K. A. D'Souza, D. V. Siegfeldt, «A Conceptual Framework for Detecting Cheating in Online and Take-Home Exams», *Decision Sciences Journal of Innovative Education* 370, 2017.

³¹⁶ A. Giannopoulou, R. Ducato, G. Schneider, C. Angiolini, «Critical Notes on 'Platformised' Education: Untangling Privacy and Data Protection in Postpandemic Universities», *European Law Blog*, 8 marzo 2021, consultabile al link:

<https://europeanlawblog.eu/2021/03/08/critical-notes-on-platformised-education-untangling-privacy-and-data-protection-in-postpandemic-universities/>.

³¹⁷ Si v. <https://proctorio.com/>.

³¹⁸ Si v. <https://proctorio.com/products/online-proctoring>.

³¹⁹ Si v. S. Swauger, «Software That Monitors Students during Tests Perpetuates Inequality and Violates Their Privacy», *MIT Technology Review*, 2020,

raccolti in qualsiasi momento, e riescono anche a rintracciare la geolocalizzazione degli studenti tramite l'accesso all'indirizzo IP.³²⁰

Descrivendo maggiormente nello specifico il funzionamento di tali strumenti di *e-proctoring*, con il software *Proctorio* viene offerta una doppia possibilità: un *automated proctoring* oppure un *live proctoring*; la differenza principale tra i due sistemi riguarda la presenza solamente in quello *live* di un *live proctor pop in*, vale a dire un sistema che permette di rilevare, contestualmente allo svolgimento dell'esame, eventuali irregolarità³²¹, mentre nel caso del software *automated*, un eventuale verifica sarà possibile solo dopo la consegna dell'esame, sulla base delle funzioni di controllo abilitate.

Respondus, fornito dalla società statunitense *Respondus Inc.*, invece, utilizza un *lockdown browser*: l'intero schermo del dispositivo elettronico è occupato dal software per lo svolgimento dell'esame, senza possibilità di minimizzazione, ossia di usare il dispositivo per altri scopi. Non è possibile uscire dalla pagina dello svolgimento dell'esame senza consegnare il proprio elaborato, così come non è possibile stampare, utilizzare le funzioni di copia e incolla o semplicemente aprire ogni altra pagina tanto online quanto offline.³²² Questo browser può essere utilizzato sia singolarmente, sia nel pacchetto «*respondus monitor*», che affianca a queste funzionalità le classiche funzionalità di *e-proctoring*. In particolar modo, il software cattura le immagini video e lo schermo dello studente, ed eventuali comportamenti sospetti vengono segnalati (cosiddetto «*flag*») tramite istantanee dello schermo o brevi video, affinché possano essere, al termine dello svolgimento dell'esame, controllati dal docente, attraverso un sistema di «*Review Priority*». Prima dell'esame, inoltre, può essere chiesto allo studente di mostrare un documento d'identità o riprendere gli ambienti circostanti.³²³

Le criticità in materia di protezione dei dati personali verranno illustrate nel prossimo capitolo, riportando una decisione dell'Autorità Garante per la protezione dei dati personali italiana e alcune decisioni di omologhe autorità europee. Si vedranno poi alcune problematiche evidenziate oltreoceano, negli Stati Uniti.

In questa sede, si riporta come in dottrina sia stato segnalato che questi strumenti di monitoraggio pervasivo possano inficiare la «*educational privacy*» degli studenti, ovvero il diritto «*that safeguards the ability for a student to safely explore ideas and knowledge, to develop their intellectual selves and their personal selves, as well as the ability for educators and researchers to facilitate and participate in intellectual endeavours in the education context*».³²⁴ Le scelte di utilizzare i sistemi di *e-proctoring* contribuiscono infatti a plasmare le infrastrutture educative, con un potenziale effetto sull'istruzione stessa. In questo modo, le criticità legate al fenomeno dell' *e-proctoring*

<https://www.technologyreview.com/2020/08/07/1006132/software-algorithms-proctoring-online-tests-ai-ethics/>.

³²⁰ Ibidem.

³²¹ Si v. <https://proctorio.com/products>: «*Continuous monitoring by a live, human proctor allows immediate intervention during an exam and provides full reporting for exam administrators on demand*».

³²² Si v. <https://web.respondus.com/he/lockdownbrowser/>.

³²³ Si v. <https://web.respondus.com/he/monitor/>.

³²⁴ T. C. Li, «*Privacy in Pandemic: Law, Technology, and Public Health in the COVID-19 Crisis*», 52 *Loyola University of Chicago Law Journal*, 2021, pp. 767-865, p. 791.

rilevano non più solamente a livello individuale, ma rappresentano un problema anche a livello sociale.³²⁵

2.4 Le case editrici della sorveglianza e i libri di testo

Il report di SPARC del 2019 già citato³²⁶ registra perdite anche per il mercato dei libri di testo stampati. Un grandissimo operatore di questo settore è rappresentato dalla casa editrice Pearson. Secondo SPARC, la casa editrice ha in progetto di abbandonare il mercato del libro stampato per focalizzarsi completamente sulla produzione di libri digitali, a cui verranno presumibilmente affiancati tutta una serie di strumenti, come sistemi per svolgimento di compiti a casa o per lo svolgimento di verifiche. Si apriranno così per Pearson numerose possibilità di collezionare dati da analizzare, che potrebbero contenere preziosissime informazioni, come la capacità di apprendimento di uno studente, il tempo necessario di cui un dato studente ha bisogno per completare un determinato compito, oppure quali librerie digitali consulta.

Le perplessità evidenziate da SPARC sono pressoché le medesime dei grandi editori della sorveglianza: vi è il rischio che ci sia un utilizzo dei dati raccolti per finalità che esulano il mero miglioramento del servizio offerto. Potrebbe addirittura aprirsi la pericolosa possibilità di classificare gli studenti in base al rendimento e utilizzare dette classificazioni per l'accesso all'Università. Peraltro, durante le attività didattiche, non è infrequente che lo studente finisca per condividere in maniera più o meno esplicita categorie particolari di dati, come, *ex multis*, le sue opinioni politiche, con il rischio che le case editrici vendano illegittimamente questi dati a terze parti.

Non va peraltro dimenticato che nel mondo della scuola la scelta di un determinato libro di testo, in questo caso in forma digitale, è una decisione unilaterale dell'istituto scolastico: lo studente, quindi, non ha concretamente la possibilità di scegliere di prestare il consenso a un trattamento dei suoi dati personali simile a quelli appena citati.

2.5 Alternative: infrastrutture open source

Tra le soluzioni prospettate da SPARC³²⁷ affinché sia possibile mantenere il controllo sui dati rientra la possibilità di implementare un'infrastruttura controllata dalla comunità accademica stessa. Al momento, infatti, l'infrastruttura è in mano a grandi operatori monopolistici del capitalismo della sorveglianza, e, per quanto possa essere auspicabile un maggior controllo sulle loro attività, implementare un'infrastruttura propria della comunità accademica sembra una migliore soluzione a lungo termine.

³²⁵ A. Giannopoulou, R. Ducato, C. Angiolini, G. Schneider, «From data subjects to data suspects: challenging e-proctoring systems as a university practice», p. 282.

³²⁶ C. Aspesi, N. Starr Allen, R. Crow, S. Daugherty, H. Joseph, J.T.W. McArthur, N. Shockey, «SPARC Landscape Analysis: The Changing Academic Publishing Industry – Implications for Academic Institutions», p.48 e ss.

³²⁷ C. Aspesi, N. Starr Allen, R. Crow, S. Daugherty, H. Joseph, J.T.W. McArthur, N. Shockey, «SPARC Roadmap for Action: Academic Community Control of Data Infrastructure», Preprint, LIS Scholarship Archive, 19 novembre 2019.

<https://doi.org/10.31229/osf.io/a7nk8>.

SPARC ipotizza diverse alternative: le istituzioni universitarie potrebbero scegliere di costruire da soli una nuova infrastruttura: questo avrebbe il vantaggio di garantire un'infrastruttura che si ponga in maniera coerente con i valori dell'Università stessa. Al contempo, però, questa alternativa comporta dei costi molto alti, nonché delle tempistiche molto lunghe. Un'alternativa potrebbe essere quella di fondare un'infrastruttura gestita tanto da attori pubblici quanto da attori privati, servendosi o finanziando delle start-up già esistenti o fondando delle nuove. L'indubbio vantaggio di questo approccio è quello di avere già disponibili competenze tecniche e manageriali, ma vi è il rischio che a lungo termine si crei un conflitto di vedute sui valori da porre a fondamento del servizio. L'alternativa più veloce, ma al contempo più dispendiosa dal punto di vista economico, è quella di acquistare strumenti già esistenti. È chiaro che la decisione di uno o dell'altro approccio dipende dai fondi disponibili, è importante però sottolineare che questo processo di acquisizione di una nuova infrastruttura «*will require institutions to be willing to invest in digital infrastructure with the same commitment as they currently invest in physical infrastructure*». ³²⁸ In altre parole, così come diversi milioni vengono stanziati per la costruzione di strade e ponti, un'ingente quantità di denaro sarà necessaria per l'implementazione di un'infrastruttura appartenente alla comunità accademica. L'investimento iniziale, che secondo SPARC ammonterebbe a circa 40-50 milioni di dollari, va ricercato attraverso consorzi tra Università, attori privati, ONG e istituzioni governative. ³²⁹

Anche Karen Maex, nel discorso pronunciato l'8 gennaio 2021 per il 389esimo *Dies Natalis* dell'Università di Amsterdam, in cui denuncia il pericolo che il mondo dell'istruzione e della ricerca finiscano completamente nelle mani dei grandi capitalisti della sorveglianza, auspica l'implementazione di un'infrastruttura pubblica che permetta alle Università di mantenere il controllo sui dati e sul loro utilizzo: «*what applies to the future of democracy applies equally to the future of universities and of independent education and research as vital building blocks for the organisation of knowledge. We cannot simply leave the future of knowledge to the corporate boardrooms*». ³³⁰

2.4.1. L'esperienza italiana: GARR e il Politecnico di Torino

Esistono già alternative ³³¹ alle grandi piattaforme proprietarie utilizzate per la didattica a distanza e per il mondo della ricerca, un esempio tutto italiano è l'infrastruttura di calcolo del cloud GARR: «*una rete nazionale a banda ultralarga dedicata alla comunità dell'istruzione e della ricerca*», il cui principale obiettivo è

³²⁸ Ibidem, p. 25.

³²⁹ C. Aspesi, N. Starr Allen, R. Crow, S. Daugherty, H. Joseph, J.T.W. McArthur, N. Shockey, «2020 Update: SPARC Landscape Analysis & Roadmap for Action», Preprint, LIS Scholarship Archive, 22 settembre 2021, p.39.

³³⁰ K. Maex, «Protect independent and public knowledge».

³³¹ R. Caso, M.C. Pievatolo, «A Liberal Infrastructure in a Neoliberal World: The Italian Case of GARR», *Journal of Intellectual Property, Information Technology and Electronic Commerce*, 2023. <https://zenodo.org/record/7561821#.Y8655BPMK3I>.

*«fornire connettività ad alte prestazioni e di sviluppare servizi innovativi per le attività quotidiane di docenti, ricercatori e studenti e per la collaborazione a livello internazionale.(...) Diversamente da quanto avviene con i provider commerciali, gli utenti sulla rete GARR non sono solo fruitori di dati, contenuti e servizi ma grazie ad essa sono in grado di renderne disponibili di nuovi a beneficio della comunità scientifica, diventando elementi attivi».*³³²

Essa è gestita dal Consortium GARR, un'associazione senza fini di lucro che riunisce Università italiane ed enti di ricerca, sostenuta dal Ministero dell'Istruzione, Università e Ricerca (oggi Ministero dell'Istruzione e del Merito).

La rete è interamente basata su soluzioni open source³³³ ed è finalizzata a rispondere alle esigenze interne di calcolo flessibile, rappresentando uno strumento tanto per ricercatori singoli quanto per gruppi di ricerca. Il modello sottostante è un modello di tipo federato e collaborativo, finalizzato a realizzare infrastrutture digitali comuni, permettendo alle istituzioni partecipanti di condividere le risorse di calcolo di cui dispongono.³³⁴ Con questo modello, non solo è possibile realizzare un risparmio importante grazie all'abbandono delle piattaforme proprietarie, ma si raggiunge anche uno standard di tutela di dati personali maggiore, dal momento che essi saranno raccolti e trattati in Italia in conformità, dunque, al GDPR.³³⁵ Il GARR insieme al CNR ha inoltre realizzato il portale «*io resto a casa*»,³³⁶ tramite il quale è possibile svolgere videochiamate gratuite.

La piattaforma del GARR realizza in pieno quello che Karen Maex immagina: è un'infrastruttura pubblica, indipendente da qualsivoglia cloud commerciale, pensata per la ricerca e costruita da ricercatori.³³⁷ È quindi naturale interrogarsi sul perché tanto le Università, quanto il Governo, durante l'emergenza pandemica non abbiano indicato il GARR quale strumento per svolgere la didattica a distanza, e sul perché il mondo della ricerca faccia ricorso a questo strumento solamente in minima parte.³³⁸

Il Politecnico di Torino rappresenta un virtuoso esempio di Università che, sin dall'inizio dell'emergenza pandemica, non ha affidato le attività didattiche alle piattaforme dei grandi capitalisti della sorveglianza. L'Università ha infatti scelto di affidarsi al software open-source «*Big Blue Button*», su cui lavorava già da diversi anni e che ha adattato per le esigenze di teledidattica.³³⁹

³³² «Consortium GARR», consultabile al link: <https://www.garr.it/it/chi-siamo>.

³³³ Tali soluzioni open source sarebbero basate su un software distribuito tramite una licenza che permette la modifica, il miglioramento e la redistribuzione del codice sorgente (di qui, appunto, *open source*). In particolare, il GARR è basato sulla tecnologia open source OpenStack. Per un approfondimento, si v. A. Barchiesi et al., «Fare cloud senza rinunciare al controllo di dati e risorse: la ricetta GARR» *Agenda Digitale*, 13 gennaio 2022, <https://www.agendadigitale.eu/infrastrutture/fare-cloud-senza-rinunciare-al-controllo-di-dati-e-risorse-la-ricetta-garr/>.

³³⁴ A. Barchiesi et al., «Fare cloud senza rinunciare al controllo di dati e risorse: la ricetta GARR».

³³⁵ *Ibidem*.

³³⁶ Si v. www.iorestoacasa.work.

³³⁷ R. Caso, M.C. Pievatolo, «A Liberal Infrastructure in a Neoliberal World: The Italian Case of GARR», p. 14.

³³⁸ *Ibidem*.

³³⁹ POLIFLASH MAGAZINE - Il Politecnico digitale, «Al via con successo la didattica online», 13 marzo 2020, https://poliflash.polito.it/in_ateneo/il_politecnico_digitale_al_via_con_successo_la_didattica_online.

2.5.2 Il mondo della scuola

La risoluzione del problema, nel mondo della scuola, è invece nelle mani del Ministero dell'Istruzione. A dicembre del 2020, l'allora Ministra per l'Istruzione Azzolina ha annunciato la costituzione di un gruppo di lavoro per la creazione di una piattaforma digitale unica, integrata con tutti i servizi e le funzionalità utili per le scuole, compresa la didattica digitale.³⁴⁰ A marzo del 2021 è stato poi presentato al Senato il disegno di legge numero 2142 «*Istituzione della Rete di interconnessione unica nazionale dell'istruzione – UNIRE*».³⁴¹

Le finalità della rete di interconnessione unica nazionale sono puntualmente descritte all'articolo 1 del disegno di legge: assicurare il coordinamento informativo e informatico delle piattaforme, dei sistemi e dei dati tra le scuole di ogni ordine e grado, l'omogeneità nell'elaborazione e trasmissione dei dati, il funzionamento della didattica digitale integrata, la gestione della rete telematica di interconnessione, la realizzazione e la gestione, attraverso un cloud computing privato, dei servizi collegati a tali attività, compresi quelli amministrativi e connessi alle procedure di assunzione. La funzione di UNIRE è, ex articolo 2, lettera e) quella di «*fornire servizi di sicurezza informatica e ambienti protetti per la didattica e per la didattica digitale integrata*».

Il disegno di legge propone di affidare la gestione di UNIRE ad una società per azioni interamente partecipata dallo Stato, con una copertura finanziaria di 20 milioni di euro. La somma desta qualche perplessità circa la sua idoneità a raggiungere davvero l'obiettivo di sottrarre la scuola ai capitalisti della sorveglianza.³⁴² È stato inoltre sottolineato come il disegno di legge non attenzi il problema dell'inclusività e della pedagogia³⁴³, dal momento che come è stato brillantemente segnalato³⁴⁴, le piattaforme di Google o Microsoft, hanno loro stesse la loro pedagogia: «*digital minority (...) they are designed to make administrators, technicians, teachers and students, each in their own way, passive, disengaged, dependent, ignorant, addicted*».³⁴⁵ L'etica dietro piattaforme come Google orienta l'istruzione verso i suoi obiettivi, ovvero produttività, quantificazione, sorveglianza e apprendimento online.³⁴⁶

2.5.3 Spunti comparatistici: l'esempio francese

³⁴⁰ MIUR, Ministero dell'istruzione e del merito, «Scuola, Ministero al lavoro su piattaforma digitale unica Azzolina: "Acceleriamo innovazione, costruiamo la scuola del futuro"», 11 dicembre 2020. <https://www.miur.gov.it/web/guest/-/scuola-ministero-al-lavoro-su-piattaforma-digitale-unica-azzolina-acceleriamo-innovazione-costruiamo-la-scuola-del-futuro->.

³⁴¹ Si v. disegno di legge n. 2142 del 2021 al link:

<https://www.senato.it/leg/18/BGT/Schede/Ddliter/53821.htm>.

³⁴² Binario Etico, «UNIRE, la Rete di interconnessione unica nazionale dell'istruzione», 24 marzo 2021, https://binarioetico.it/digital_transformation/2021/03/24/unire/.

³⁴³ G. Scialpi, «Didattica a distanza, Ministero lavora ad una piattaforma unica. Abbia anche impronta pedagogica», Orizzonte Scuola Notizie, 28 giugno 2020, <https://www.orizzontescuola.it/didattica-a-distanza-ministero-lavora-ad-una-piattaforma-unica-abbia-anche-impronta-pedagogica/>.

³⁴⁴ R. Caso, M.C. Pievatolo, «A Liberal Infrastructure in a Neoliberal World: The Italian Case of GARR».

³⁴⁵ Ibidem, p. 13.

³⁴⁶ D. G. Krukta, R.M. Smits, T. A. Willhelm, «Don't be evil: should we use Google in schools?», p. 427.

Sin dai primi momenti della pandemia e del necessario confinamento, il Ministero dell'Istruzione francese ha efficacemente evitato l'utilizzo di software di piattaforme proprietarie grazie al portale «apps education»,³⁴⁷ ovvero «una piattaforma sviluppata all'interno del Dipartimento digitale per l'istruzione per offrire strumenti quotidiani essenziali a tutti i funzionari dell'istruzione nazionale».³⁴⁸ Il successo della piattaforma francese sta nel prevedere tutte le funzionalità concretamente indispensabili per lo svolgimento della didattica online: *Peertube* consente la condivisione di video, *Classe Virtuelle* le lezioni in streaming, *Nextcloud* permette l'upload di file. Il tutto è perfettamente in linea con quanto puntualmente previsto dal GDPR. Il Ministero dell'Istruzione francese, tramite l'ente dallo stesso controllato Centre National d'Enseignement à Distance (CNEd), ha creato il portale «mes classes virtuelles».³⁴⁹

La creazione da parte del governo di tali strumenti ha rappresentato terreno fertile affinché la *Commission nationale de l'informatique ed des libertés* (CNIL), autorità garante per i dati personali in Francia, interrogata dalla *Conférence des présidents d'université e dalla Conférence des grandes écoles*, si pronunciasse circa l'incompatibilità con il GDPR dell'utilizzo delle piattaforme proprietarie nel settore dell'istruzione. Non solo, ha potuto richiedere un progressivo abbandono di queste piattaforme, sottolineando come nascano sempre maggiori preoccupazioni con riferimento al controllo dei flussi di dati a livello internazionale e alla sovranità digitale dell'Unione europea.³⁵⁰

Nel novembre del 2022, il Ministro dell'Istruzione francese Pap N'Diaye ha poi preso apertamente posizione sulla questione, chiedendo di interrompere l'implementazione delle soluzioni di Microsoft e di Google poiché contrari alla strategia nazionale per il cloud.³⁵¹ Questa strategia era stata annunciata a settembre dello stesso anno congiuntamente dal Commissario Europeo per il Mercato Interno, il Ministro dell'Economia, delle Finanze e della Sovranità Industriale e Digitale e dal Ministro Delegato per il Digitale e le Telecomunicazioni. L'intento è chiaro: intensificare le offerte cloud nazionali per contrastare le offerte poco affidabili delle Big Tech.³⁵²

2.5.4 Verso una soluzione europea: GAIA-X

Ancor prima che l'esperienza pandemica esacerbasse i problemi di sovranità digitale, da una partnership tra il governo tedesco e quello francese nasce l'idea di GAIA-

³⁴⁷ Si v. <https://portail.apps.education.fr/signin>.

³⁴⁸ Ibidem.

³⁴⁹ Si v. <https://www.cned.fr/maclassealamaison>.

³⁵⁰ CNIL, «La CNIL chiede cambiamenti nell'uso degli strumenti di collaborazione statunitensi per l'istruzione superiore e la ricerca», consultabile al link: <https://www.cnil.fr/fr/la-cnil-appelle-evolutions-dans-utilisation-outils-collaboratifs-etatsuniens-enseignement-superieur-recherche>.

³⁵¹ S. Rolland, «Fin de la récréation : Microsoft et Google exclus de l'école par l'Éducation nationale», *La Tribune*, 24 novembre 2022, <https://www.latribune.fr/technos-medias/internet/fin-de-la-recreation-microsoft-et-google-exclus-de-l-ecole-par-l-education-nationale-942051.html>.

³⁵² L. Garofalo, «Cloud sovrano in Francia, il governo voltafaccia ai Gafam», *Key4biz* (blog), 15 settembre 2022, <https://www.key4biz.it/cloud-sovrano-in-francia-il-governo-voltafaccia-ai-gafam-e-sostiene-lecosistema-nazionale-e-litalia/415944/>.

X³⁵³: «*a trustworthy and sovereign digital infrastructure for Europe*». ³⁵⁴ Il progetto è stato presentato al resto degli Stati membri dell'Unione europea con una conferenza di lancio il 4 giugno 2020. L'obiettivo è quello di implementare la data economy all'interno del territorio UE, facilitando gli scambi di dati tra aziende, enti di ricerca ed enti pubblici e rispettando il quadro normativo europeo, in particolare il GDPR.

Sul sito web ufficiale dell'iniziativa si legge che:

«our goal is to establish an ecosystem, whereby data is shared and made available in a trustworthy environment. Our intention is that we give the control back to the users by retaining sovereignty over their data. Our outcome will not be a cloud. It is a federated system linking many cloud service providers and users together in a transparent environment that will drive the European data economy of tomorrow». ³⁵⁵

Gaia-X è composto da quattro elementi principali³⁵⁶:

- (i) *federation services*, ovvero requisiti tecnici e servizi necessari per rendere operativo l'ecosistema Gaia-X federato, garantendo elevati livelli di sicurezza e la protezione della privacy;
- (ii) ambienti virtuali dove è possibile conservare i dati alla fonte e condividere e scambiare dati su base volontaria per sviluppare progetti, chiamati *data spaces*;
- (iii) *standard* tecnici e regolatori per garantire sicurezza elevata;
- (iv) *servizi*: con le regole standard comuni, GaiaX sarà in grado di creare valore per le aziende incentivando la collaborazione. Focalizzandosi sull'economia dei dati, sarà quindi possibile generare nuove opportunità di business.

Al centro, dunque, vi è il concetto di «*data space*», ovvero un «*sistema virtuale e basato sull'interoperabilità tra diversi provider di servizi cloud, che permette ai propri utenti di scambiare dati quando necessario. I data space possono essere organizzati per filiera, settore o ambito*». ³⁵⁷ In questi data space, è possibile creare delle vere e proprie federazioni tra attori appartenenti, ad esempio, alla stessa filiera, così da permettere una condivisione di dati semplificata. Al momento, GAIA-X ha definito nove ecosistemi. ³⁵⁸

Il punto di partenza è la presa d'atto del fatto che i dati e le infrastrutture digitali ricoprono un ruolo fondamentale nell'economia; tuttavia, vi sono alcuni ostacoli che GAIA-X intende superare, come la mancanza di trasparenza con riferimento al trattamento dei dati personali, così come all'infrastruttura su cui il trattamento si

³⁵³ Per un approfondimento, si v. H. Tardieu, «Role of Gaia-X in the European Data Space Ecosystem», In: Otto, B., ten Hompel, M., Wrobel, S. (eds) *Designing Data Spaces*. Springer, Cham. 2022 https://doi.org/10.1007/978-3-030-93975-5_4

³⁵⁴ Si v. «Gaia-X: The European Project kicks off next phase», Si v. https://www.data-infrastructure.eu/GAIAX/Redaktion/EN/Publications/gaia-x-the-european-project-kicks-of-the-next-phase.pdf?__blob=publicationFile&v=7.

³⁵⁵ Si v. «About Gaia-X - Gaia-X: A Federated Secure Data Infrastructure», <https://gaia-x.eu/what-is-gaia-x/about-gaia-x/>.

³⁵⁶ Ibidem.

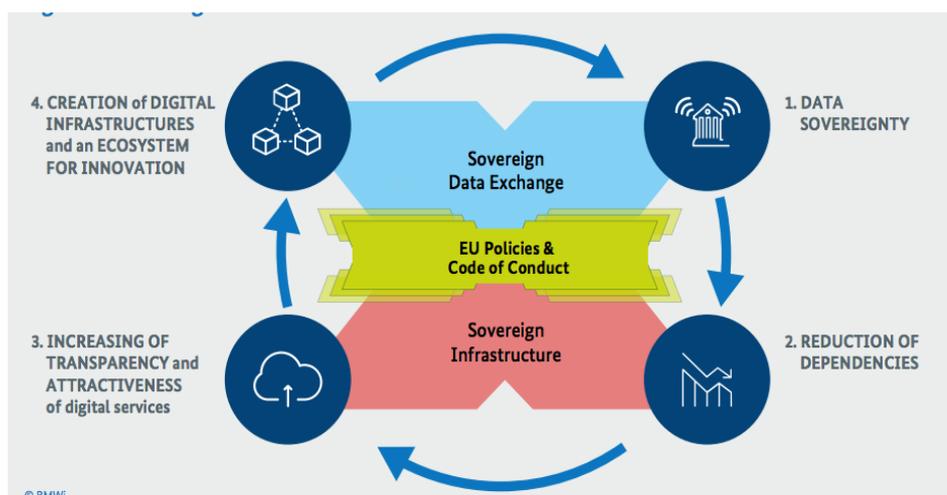
³⁵⁷ «Cos'è Gaia-X», Gaia-X Hub Italia, <https://www.gaiax-italia.eu/cosa-facciamo>.

³⁵⁸ Ibidem.

basa.³⁵⁹ Con la creazione di un ecosistema che rispetti i valori e gli standard europei, GAIA-X annovera tra i suoi obiettivi quello di rinforzare la *digital sovereignty*³⁶⁰ per le imprese, la scienza e il governo. I *core values* sono inoltre la protezione dei dati personali, la trasparenza, l'autenticità, la fiducia, la possibilità di autodeterminazione, il mercato libero, l'interoperabilità.³⁶¹

In questo modo, la sovranità digitale europea viene intesa come un mezzo per giungere a una protezione efficace dei diritti fondamentali dei cittadini dell'Unione e per promuovere i valori e i principi delle democrazie liberali, al fine di limitare l'esercizio del potere delle grandi piattaforme digitali.³⁶²

GAIA-X mira, inoltre, a ridurre le situazioni di dipendenza. Questo sarà possibile incrementando i servizi accessibili, così da limitare la dipendenza delle imprese e dei singoli cittadini da singoli internet service provider. Applicando la normativa UE, ritiene di poter facilitare la promozione dei valori europei, così da aprire al legislatore europeo nuove strade. Inoltre, GAIA-X intende garantire l'accesso a service di alto livello a un grande pubblico di utenti: se da un lato si pone l'obiettivo di aumentare la trasparenza, dall'altro ritiene importante abbattere le barriere che si pongono davanti al concreto rispetto dei sopra menzionati principi, così da risultare più attraente anche per le piccole e medie imprese o per le pubbliche amministrazioni.³⁶³



³⁵⁹ Si v. «GAIA-X: Driver of Digital Innovation in Europe», consultabile al link:

https://www.data-infrastructure.eu/GAIA-X/Redaktion/EN/Publications/gaia-x-driver-of-digital-innovation-in-europe.pdf?__blob=publicationFile&v=8.

³⁶⁰ Ibidem. La definizione accolta di digital sovereignty, ovvero sovranità digitale, è: «*possibility of independent self-determination by the state and by organisations' with regard to the 'use and structuring of digital systems themselves, the data produced and stored in them, and the processes depicted as a result*». All'interno di tale concetto, rientra anche quello di «*data sovereignty*», ovvero «*complete control over stored and processed data and also the independent decision on who is permitted to have access to it*», p. 3.

³⁶¹ «GAIA-X: Driver of Digital Innovation in Europe».

³⁶² M. Santaniello, «Sovranità digitale e diritti fondamentali: un modello europeo di Internet governance», *Rivista italiana di informatica e diritto*, 4, 1, mar. 2022, pp. 47-51, p. 50. <https://doi.org/10.32091/RIID0058>.

³⁶³ «GAIA-X: Driver of Digital Innovation in Europe».

Figura 6: Il funzionamento di GAIA-X. FONTE: «GAIA-X: Driver of Digital Innovation in Europe», consultabile al link: https://www.data-infrastructure.eu/GAIA-X/Redaktion/EN/Publications/gaia-x-driver-of-digital-innovation-in-europe.pdf?__blob=publicationFile&v=8

GAIA-X non intende fornire alcun servizio: si limita a progettare i componenti tecnologici necessari a realizzare gli obiettivi prefissati, creando degli «*standard de facto*» sul mercato.³⁶⁴

In sostanza, comunque, essa è fondata su una base di *mutual agreements* grazie ai quali è possibile avere la certezza giuridica del rispetto dei principi alla base di GAIA-X e, quindi, del GDPR.³⁶⁵ Proprio per questo, nel 2023 GAIA-X intende implementare servizi di «*clearing house*»: organismi indipendenti che si faranno carico di verificare l'effettiva compliance ai principi dell'infrastruttura.³⁶⁶

L'obiettivo è creare un circolo virtuoso di domanda e offerta di servizi cloud tramite una struttura federata di hub tra loro interoperabili. Una volta raccolti i dati, si mira a far sì che il valore da essi estratto vada completamente a vantaggio dei cittadini e delle imprese europee, sia in termini di competitività che di produttività.³⁶⁷ Questo obiettivo è racchiuso nell'idea di una Structura-X, ovvero una tecnologia open source condivisa.³⁶⁸

GAIA-X si organizza poi in *hub*, che coinvolgono utenti e fornitori di una determinata area.³⁶⁹ Essi operano come ambasciatori locali, non solo facendosi promotori delle esigenze locali e collaborando con le amministrazioni *in loco*, ma anche implementando collaborazioni finalizzate a creare data space comuni nel territorio UE.

GAIA-X è aperta anche ad aziende extraeuropee che abbraccino i valori di fondo e quindi, sostanzialmente, la normativa europea; tuttavia, l'accesso al consiglio di amministrazione è riservato a soli partner europei.

GAIA-X non nasce per il mondo dell'istruzione, ma potrebbe trovare applicazioni anche in questo settore.³⁷⁰

Da un punto di vista squisitamente teorico, considerando l'attenzione per la privacy e tutela dei dati personali, nonché per le questioni politiche, normative e tecnologiche, GAIA-X potrebbe essere uno strumento idoneo per il raggiungimento della

³⁶⁴ G. Arcidiacono, «Gaia-X: lo standard europeo per il cloud e i suoi progetti principali», Agenda Digitale, 27 aprile 2022, <https://www.agendadigitale.eu/infrastrutture/gaia-x-lo-standard-europeo-per-il-cloud-e-i-suoi-progetti-principali/>.

³⁶⁵ V. Pagnanelli, «Conservazione dei dati e sovranità digitale. Una rilettura della (big) data governance pubblica alla luce delle nuove sfide globali», Rivista italiana di informatica e diritto 3, fasc. 1, 3 luglio 2022, pp. 11–26, <https://doi.org/10.32091/RIID0022>.

³⁶⁶ Ibidem.

³⁶⁷ A. Fontana, «Gaia-X, 2023 anno della crescita: opportunità per aziende e fornitori Ict», Il Sole 24 ORE, 23 gennaio 2023, consultabile al link: <https://amp24-ilsole24ore-com.cdn.ampproject.org/c/s/amp24.ilsole24ore.com/pagina/AEC90TeC>.

³⁶⁸ Ibidem.

³⁶⁹ Si v., ad esempio, l'hub italiano al link: <https://www.gaiax-italia.eu/>.

³⁷⁰ P. Monella, «Istruzione e GAFAM: dalla coscienza alla responsabilità», p.38.

sovranità digitale.³⁷¹ Tuttavia, va segnalata una criticità: essendo aperta ad aziende non europee, vi è il rischio che si trasformi in un cavallo di Troia per i fornitori dei cloud stranieri; infatti, la scelta di consentire la partecipazione di aziende non appartenenti all'UE potrebbe comportare che gran parte del valore dell'economia dei dati europea continui a fluire fuori dal territorio unionale.³⁷²

2.6 Lo spazio europeo dell'istruzione e il piano d'azione per l'istruzione digitale

Il 30 settembre 2020, la Commissione dell'Unione europea ha adottato due importanti iniziative che si collocano nella cornice degli interventi finalizzati a realizzare un'Europa verde e digitale e delle misure finalizzate a superare la crisi generata dalla pandemia da Covid-19.

La prima di queste iniziative è la realizzazione di uno spazio europeo dell'istruzione entro il 2025³⁷³, per eliminare gli ostacoli all'apprendimento e migliorare l'accesso a un'istruzione di qualità per tutti. Al centro del progetto vi è la cooperazione tra gli Stati membri, che potrà migliorare la qualità, l'inclusività e le dimensioni verde e digitale del mondo dell'istruzione. Tale spazio comprende sei dimensioni: qualità, inclusione e parità di genere, transizioni verde e digitale, insegnanti, istruzione superiore e un'Europa più forte nel mondo.

All'interno di questa cornice si colloca poi il piano d'azione per l'istruzione digitale 2021-2027.³⁷⁴ Il piano riconosce, tra le sue premesse, il fatto che la pandemia da Covid-19 abbia portato a un uso senza precedenti della tecnologia nel mondo dell'istruzione e della formazione, e intende fronteggiare le sfide e le opportunità che da questo evento sono emerse. In particolar modo, la pandemia ha esacerbato una serie di problematiche: disuguaglianze sociali nell'accesso alle tecnologie digitali e alla rete internet e scarse competenze digitali nel mondo dell'istruzione, soprattutto con riferimento ad alcuni Stati membri.

Il piano d'azione per l'istruzione digitale presenta due priorità.

La prima è promuovere lo sviluppo di un ecosistema altamente efficiente di istruzione digitale. Si intende fare ciò attraverso un dialogo strategico con gli Stati membri sui fattori che possono contribuire a realizzare il successo dell'istruzione digitale, promuovendo la connettività, fornendo attrezzature digitali per l'istruzione e piani di trasformazione digitale per gli istituti di istruzione e formazione. La Commissione sottolinea anche la necessità di fornire orientamenti etici per gli educatori sull'uso dell'intelligenza artificiale e dei dati: se è vero che questi ultimi possono giocare un ruolo fondamentale nel mondo dell'istruzione, perché potrebbero ad esempio compensare

³⁷¹ S. Autolitano, A. Pawlowska, «Europe's Quest for Digital Sovereignty: GAIA-X as a Case Study», IAI Papers, n. 21. 2021, p. 15, consultabile al link:

<https://www.iai.it/en/pubblicazioni/europes-quest-digital-sovereignty-gaia-x-case-study>

³⁷² Ibidem.

³⁷³ Commissione europea, uno spazio europeo per l'istruzione entro il 2025, 30 settembre 2020, si v. <https://education.ec.europa.eu/it/about-eea/the-eea-explained>.

³⁷⁴ Commissione europea, piano d'azione per l'istruzione digitale 2021-2027, 30 settembre 2020, consultabile al link: <https://education.ec.europa.eu/it/focus-topics/digital-education/action-plan>.

eventuali difficoltà dell'apprendimento, è altrettanto vero che possono nascere innumerevoli rischi.³⁷⁵

La Commissione europea, nell'ottobre del 2022, ha quindi pubblicato degli orientamenti etici per gli educatori sull'uso dell'intelligenza artificiale³⁷⁶ e dei dati nell'insegnamento e nell'apprendimento. Tra questi, si annoverano una serie di misure di base che gli educatori e dirigenti scolastici possono adottare per utilizzare al meglio i dati personali e l'IA. La scuola, in particolare, deve rispettare quanto previsto dal GDPR: deve elencare i dati che sta raccogliendo e le finalità per cui sono raccolti, e deve poi verificare se sia possibile raggiungere lo stesso risultato raccogliendo informazioni meno specifiche. Deve inoltre decidere per quanto tempo i dati saranno conservati, e assicurarsi che non siano conservati per un tempo maggiore a quello necessario. Nell'istituire in sistema di intelligenza artificiale, la scuola deve assicurare un'IA antropocentrica e una sorveglianza umana, garantendo che i dati di input siano pertinenti alle finalità dell'IA stessa e sempre coerenti con il GDPR.³⁷⁷

La seconda priorità del piano per l'istruzione digitale è migliorare le competenze e le abilità digitali per la trasformazione digitale. In questa cornice, si rende necessario aggiornare il quadro europeo delle competenze digitali per includervi le competenze in materia di IA e di dati.³⁷⁸ L'obiettivo è fare in modo che non solo gli educatori e gli studenti, ma tutti i cittadini, siano in grado di utilizzare le tecnologie digitali e l'intelligenza artificiale con dimestichezza, ma con consapevolezza rispetto ai problemi connessi a questi strumenti.

³⁷⁵ Commissione europea, piano d'azione per l'istruzione digitale - azione 6, si v. in link: <https://education.ec.europa.eu/it/focus-topics/digital-education/action-plan/action-6?>

³⁷⁶ Commissione europea, Direttorato generale per l'istruzione, della gioventù, dello sport e della cultura, Ethical guidelines on the use of artificial intelligence (AI) and data in teaching and learning for educators, 25 ottobre 2022.

³⁷⁷ Ibidem, p. 26.

³⁷⁸ Commissione europea, piano d'azione per l'istruzione digitale - azione 8, si v. il link: <https://education.ec.europa.eu/it/focus-topics/digital-education/action-plan/action-8?>

III CAPITOLO

IL TRATTAMENTO DEI DATI PERSONALI DELLA DIDATTICA A DISTANZA

3.1 General Data Protection Regulation e mondo dell'istruzione: l'ordine del ragionamento

Nel presente capitolo si intende illustrare le criticità legate alla didattica a distanza dal punto di vista della protezione dei dati personali, così come disciplinati dal GDPR.

In primo luogo, si intende procedere a una descrizione dei ruoli ricoperti dai vari protagonisti della didattica a distanza.

Successivamente, si procederà alla descrizione della base giuridica e della finalità del trattamento dei dati personali durante la DaD, riportando lo studio, svolto da Rossana Ducato *et al.*³⁷⁹, delle privacy policy di nove esempi software³⁸⁰ per la gestione di gruppi di utenti online, piattaforme di condivisione di contenuti, social networks e servizi di videocomunicazione impiegati durante la DaD. Il contenuto di tali informative è analizzato con riferimento alla formulazione disponibile alla data del 27 aprile 2020, nel pieno dell'emergenza pandemica e dello svolgimento delle attività didattiche di scuole e Università online. Tale analisi verterà anche sulla verifica del rispetto dei diritti dell'interessato previsti dal GDPR. Successivamente, si procederà all'analisi della formulazione attuale privacy policy³⁸¹, al fine di verificare se vi siano stati miglioramenti rispetto alle problematiche evidenziate con riferimento alla formulazione del 2020.

Preliminarmente all'analisi delle privacy policy, occorre prestare attenzione agli articoli 13 e 14 del GDPR, i quali descrivono il contenuto delle informative privacy che il titolare deve comunicare al soggetto interessato.³⁸²

L'articolo 12 prevede che il titolare del trattamento adotti misure appropriate per fornire all'interessato le informazioni di cui agli articoli 13 e 14 in «*forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori*».

Il principio di trasparenza, enunciato anche dall'articolo 5 del GDPR,³⁸³ è quindi un obbligo che i titolari del trattamento devono tenere in considerazione quando redigono le informative, e costituisce il fondamento della possibilità per i soggetti interessati al trattamento di esercitare i diritti riconosciuti dal GDPR.³⁸⁴ La trasparenza è dunque indispensabile per veicolare adeguatamente tutte le informazioni sul trattamento, sulle

³⁷⁹ R. Ducato, G. Priora, C. Angiolini, A. Giannopoulou, B.J. Jutte, G. Noto La Diega, L. Pascault, G. Schneider, «Didattica di emergenza o Emergency Remote Teaching: un'analisi empirica in tema di privacy e diritto d'autore dei termini e condizioni dei servizi online più diffusi».

³⁸⁰ Le piattaforme analizzate nello studio sono: *Discord, Facebook, G-Suite for Education, Jitsi Meet, MoodleCloud, Microsoft Teams, Skype, YouTube, Zoom*.

³⁸¹ In particolare, si fa riferimento alla formulazione alla data del 6 luglio 2023.

³⁸² Per un approfondimento, si v. G.M. Riccio, G. Scorza, E. Bellisario, «GDPR e normativa privacy, commentario».

³⁸³ «I dati personali sono: a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato (...)».

³⁸⁴ C. Angiolini, R. Ducato, A. Giannopoulou, G. Schneider, «Remote Teaching During the Emergency and Beyond: Four Open Privacy and Data Protection Issues of "Platformised" Education», p. 54.

relative finalità, modalità e rischi, nonché tutte le comunicazioni collegate all'esercizio dei diritti delle persone. La trasparenza, inoltre, rende concreto il principio della responsabilizzazione, diventando anche la chiave per rendere effettivi i principi di liceità e correttezza del trattamento.³⁸⁵

Nei paragrafi successivi si intende gettare luce sul mancato rispetto del suddetto principio da parte dei titolari del trattamento: si registrano infatti privacy policy poco chiare, che denotano un approccio superficiale alla tutela dei diritti dell'interessato.³⁸⁶

L'analisi verterà poi sulla ricostruzione della disciplina in materia di trasferimento dei dati personali verso gli Stati Uniti, ove le piattaforme maggiormente utilizzate per l'emergency remote teaching sono incorporate. Si cercherà di verificare se, a seguito della sentenza Schrems II della Corte di Giustizia dell'Unione europea, permanga in capo alle piattaforme proprietarie la possibilità di effettuare un trasferimento dei dati personali verso gli Stati Uniti.

Come già descritto nel precedente capitolo, durante lo svolgimento delle attività didattiche, numerose Università hanno utilizzato strumenti di cosiddetto *e-proctoring* al fine di garantire un corretto e onesto svolgimento degli esami. Tali strumenti sollevano numerose perplessità in materia di protezione dei dati personali, sicché nel presente capitolo si riporterà la decisione dell'Autorità Garante per la protezione dei dati personali italiana di sanzionare l'Università "Luigi Bocconi" di Milano per l'utilizzo di tali software, ripercorrendo successivamente decisioni simili da parte di altre autorità garanti europee e illustrando come tali preoccupazioni siano state avvertite anche negli Stati Uniti.

Si ipotizzeranno inoltre soluzioni finalizzate a prestare una maggiore tutela dei dati personali di fanciulli e minori, quali soggetti considerati vulnerabili ai sensi del GDPR.

Infine, si guarderà ad una nuova sfida comune al mondo della didattica e della protezione dei dati personali: l'intelligenza artificiale e in particolar modo il chatbot ChatGPT.

3.2 Titolare e responsabile del trattamento nella didattica a distanza

La distribuzione dei ruoli previsti dal GDPR ogni qualvolta si trattino dati personali per finalità legate alla didattica può diversamente declinarsi a seconda del caso di specie.

Gli studenti sono sempre i soggetti interessati al trattamento. Idealmente, l'Università e le istituzioni scolastiche dovrebbero rappresentare il titolare del trattamento ai sensi dell'articolo 4, numero 7 del GDPR, mentre i docenti assumono due diversi ruoli. *In primis*, anche i docenti possono essere considerati soggetti interessati al trattamento, dal momento che l'Università e la scuola – ad esempio – effettuano il trattamento dei loro dati personali per finalità retributive. I docenti, tuttavia, ricoprono anche il ruolo di persona autorizzata al trattamento ai sensi dell'articolo 29³⁸⁷ del GDPR,

³⁸⁵ G.M. Riccio, G. Scorza, E. Bellisario, «GDPR e normativa privacy, commentario», p. 49.

³⁸⁶ Si v. C. Angiolini, R. Ducato, A. Giannopoulou, G. Schneider, «Remote Teaching During the Emergency and Beyond: Four Open Privacy and Data Protection Issues of 'Platformised' Education», p.55.

³⁸⁷ «Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri».

dal momento che hanno la possibilità di accedere ai dati degli studenti seguendo le istruzioni impartite dalle istituzioni accademiche e scolastiche.³⁸⁸

La pandemia da Covid-19 e il passaggio alla didattica a distanza ha ampliato il numero dei soggetti coinvolti nel trattamento. Come già precedentemente illustrato, infatti, per far fronte alle difficoltà sorte in seguito alla necessità di contenimento del virus, quasi l'intero mondo dell'istruzione ha fatto ricorso a piattaforme commerciali esterne.

Il passaggio alla «*platformised education*» rappresenta un rischio per le modalità con cui tanto le scuole quanto le Università svolgono le loro attività di istruzione, determinando, in ultima istanza, dei rischi circa la liceità del trattamento dei dati personali degli studenti e dei docenti.

Ciò comporta che, come sapientemente illustrato in dottrina³⁸⁹, la scelta di svolgere le attività didattiche con l'ausilio di piattaforme estranee all'organigramma universitario debba essere guidata da estrema cautela e attenzione, dal momento che la tutela della privacy e dei dati personali è strumentale al rispetto di altri diritti costituzionalmente garantiti, quali la libertà d'espressione o il diritto all'istruzione o la libertà di insegnamento e ricerca.

Quando il 4 marzo 2020 il Governo italiano ha disposto per la prima volta la sospensione delle attività didattiche in presenza, la mancanza di indicazioni precise circa le soluzioni per l'implementazione delle attività didattiche ha fatto sì che molti docenti cercassero soluzioni autonome. La scelta di un grande numero di docenti di continuare le attività didattiche tramite l'utilizzo di piattaforme esterne ha alterato l'ideale divisione di ruoli precedentemente descritta, poiché anche i docenti sono diventati titolari del trattamento, dal momento che sono stati in grado di determinare le finalità e i mezzi del trattamento stesso.³⁹⁰

Quando le Università e le scuole hanno scelto di fare ricorso a specifiche piattaforme, hanno coinvolto queste ultime nel "circuito del trattamento"³⁹¹, facendo sì che queste piattaforme assumessero il ruolo di responsabili del trattamento ai sensi dell'articolo 4, numero 8 del GDPR. Il rapporto che intercorre tra titolare e responsabile del trattamento deve, ai sensi dell'articolo 28 del GDPR, essere disciplinato da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri. È fondamentale che siano fissate la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento. In ogni caso, l'istituto scolastico o l'Università che scelga di esternalizzare la propria attività di trattamento di dati personali nei

³⁸⁸ C. Angiolini, R. Ducato, A. Giannopoulou, G. Schneider, «Remote Teaching During the Emergency and Beyond: Four Open Privacy and Data Protection Issues of 'Platformised' Education», p. 49.

³⁸⁹ Ibidem, p.48: «*We argue that the implementation of the right to privacy and data protection in the ERT environment is not merely an issue of compliance, but a substantial measure that Universities shall ensure to guarantee the fundamental rights of our students and colleagues. The right to privacy and data protection are in fact constitutional enablers of other fundamental rights such as the freedom of expression, education, research, and interests, as our digital well-being*».

³⁹⁰ Ibidem, p. 50.

³⁹¹ R. Ducato, G. Priora, C. Angiolini, A. Giannopoulou, B.J. Jutte, G. Noto La Diega, L. Pascault, G. Schneider, «Didattica di emergenza o Emergency Remote Teaching: un'analisi empirica in tema di privacy e diritto d'autore dei termini e condizioni dei servizi online più diffusi», p.9.

confronti di piattaforme terze che assumono il ruolo di responsabili del trattamento, deve farlo ricorrendo «unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato». ³⁹² Tale obbligo è da considerarsi un obbligo permanente, non scalfito dalla circostanza che titolare e responsabile del trattamento concludano un contratto. ³⁹³

Dal punto di vista pratico, ciò significa che l'Università – o la scuola - deve valutare l'adeguatezza delle garanzie che le piattaforme offrono, che consistono, sovente, in tutta una serie di documenti pertinenti (come – *ex multis* – il registro delle attività di trattamento), che possano dimostrare al titolare il rispetto delle disposizioni del GDPR. ³⁹⁴

Il Comitato europeo per la protezione dei dati spiega che non è possibile fornire un elenco esaustivo dei documenti che il responsabile del trattamento deve fornire per provare la sufficienza delle garanzie prestate. Si tratta, infatti, di una valutazione che va fatta caso per caso, «tenendo conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento nonché dei rischi per i diritti e le libertà delle persone fisiche» ³⁹⁵. In ogni caso, è necessario che il titolare del trattamento valuti alcune caratteristiche del responsabile del trattamento, quali le conoscenze specialistiche, l'affidabilità e le risorse disponibili, nonché la reputazione sul mercato. È inoltre opportuno che periodicamente il titolare del trattamento effettui ispezioni e revisioni per verificare le garanzie offerte dal responsabile del trattamento. ³⁹⁶

L'Autorità Garante per la protezione dei dati personali, nel provvedimento del 26 marzo 2020 ³⁹⁷ contenente le prime indicazioni in materia di didattica a distanza ha *expressis verbis* richiesto che il rapporto di fornitura tra scuola o università e responsabile fosse redatto con contratto o altro atto giuridico, in conformità all'articolo 28 del GDPR.

Il Garante ha inoltre raccomandato di utilizzare, laddove possibile, le funzionalità dei registri elettronici già da tempo utilizzati, ma ha permesso che si facesse ricorso a piattaforme definite «generaliste», ovvero che non erogano solo servizi rivolti alla didattica, purché si attivino, di default, solo i servizi necessari alla formazione, in ossequio al principio di minimizzazione dei dati personali.

Vi è tuttavia il rischio che nella definizione del rapporto tra titolare e responsabile del trattamento, le piattaforme godano di una maggiore forza contrattuale e finiscano

³⁹² European Data Protection Board, Linee guida 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR, versione 2.0, 7 luglio 2021, paragrafo 99.

Consultabile al link:

https://edpb.europa.eu/system/files/2022-02/eppb_guidelines_202007_controllerprocessor_final_it.pdf.

³⁹³ Ibidem.

³⁹⁴ Ibidem, paragrafi 94-96.

³⁹⁵ Ibidem, paragrafo 96.

³⁹⁶ Ibidem, paragrafo 99.

³⁹⁷ Autorità Garante per la protezione dei dati personali, didattica a distanza, prime indicazioni, provvedimento del 26 marzo 2020, consultabile al link:

<https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9300784>.

per fissare, in luogo dell'Università o della scuola, le modalità del trattamento dei dati personali e i limiti di quest'ultimo.³⁹⁸ Da un'analisi giuridica di alcune privacy policy di piattaforme utilizzate per fini didattici³⁹⁹, è emerso che queste spesso impongono ulteriori trattamenti dei dati personali raccolti per finalità proprie e imposte unilateralmente. Si comprende dunque che l'originale assetto e divisione di poteri disciplinato a mente dell'articolo 28 del GDPR sembra non rispettato.

La possibilità per le piattaforme di dettare unilateralmente i mezzi e le finalità del trattamento fa sì che anche la piattaforma ricopra il ruolo di titolare del trattamento con riferimento ai dati della didattica di cui effettua il trattamento per finalità proprie. Ciò comporta che l'Università (oppure l'istituto scolastico) e la piattaforma possano essere considerati entrambe titolari del trattamento,⁴⁰⁰ sviluppandosi tra queste eventualmente un rapporto di *joint controllership*, disciplinato dall'articolo 26 del GDPR.⁴⁰¹

Sul concetto di co-titolarietà del trattamento si è *in primis* espressa la Corte di Giustizia dell'Unione europea⁴⁰² e, in un secondo momento, il Comitato europeo per la protezione dei dati nelle linee guida sui concetti di titolare del trattamento e responsabile del trattamento.⁴⁰³

La situazione di contitolarietà del trattamento si verifica ogni qualvolta la determinazione di finalità e mezzi del trattamento sia concretamente appannaggio di più soggetti in maniera congiunta. La partecipazione congiunta nella fissazione concreta dei mezzi e delle finalità del trattamento non implica solamente la presenza di una decisione comune ai due o più soggetti, ma è possibile anche in presenza di decisioni convergenti. Si è infatti in presenza di decisioni convergenti ogni qualvolta esse « *si integrano a vicenda e sono necessarie affinché il trattamento abbia luogo, in modo tale*

³⁹⁸ C. Angiolini, R. Ducato, A. Giannopoulou, G. Schneider, «Remote Teaching During the Emergency and Beyond: Four Open Privacy and Data Protection Issues of 'Platformised' Education», p. 51.

³⁹⁹ Si v. R. Ducato, G. Priora, C. Angiolini, A. Giannopoulou, B.J. Jutte, G. Noto La Diega, L. Pascault, G. Schneider, «Didattica di emergenza o Emergency Remote Teaching: un'analisi empirica in tema di privacy e diritto d'autore dei termini e condizioni dei servizi online più diffusi», ma anche *infra* nel presente lavoro.

⁴⁰⁰ C. Angiolini, R. Ducato, A. Giannopoulou, G. Schneider, «Remote Teaching During the Emergency and Beyond: Four Open Privacy and Data Protection Issues of 'Platformised' Education», p.51.

⁴⁰¹ «*Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento. Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14, a meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti. Tale accordo può designare un punto di contatto per gli interessati.2. L'accordo di cui al paragrafo 1 riflette adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati. Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato.3. Indipendentemente dalle disposizioni dell'accordo di cui al paragrafo 1, l'interessato può esercitare i propri diritti ai sensi del presente regolamento nei confronti di e contro ciascun titolare del trattamento».*

⁴⁰² Corte di Giustizia, Sentenza della Corte (Seconda Sezione), 29 luglio 2019, Fashion ID GmbH & Co. KG contro Verbraucherzentrale NEW eV, Causa C-40/17, consultabile al link: <https://curia.europa.eu/juris/document/document.jsf?jsessionid=031958705DEB419CB2DC5D5FE6A4AC69?text=&docid=216555&pageIndex=0&doclang=IT&mode=lst&dir=&occ=first&part=1&cid=286775>.

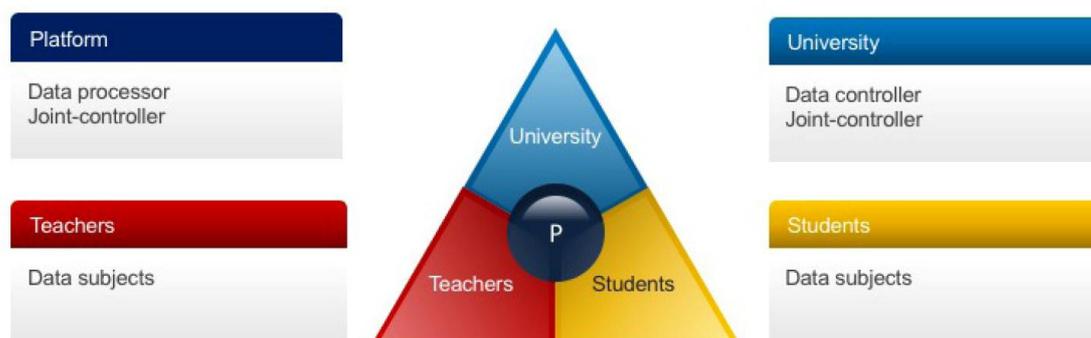
⁴⁰³ European Data Protection Board, Linee guida 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR.

da avere un impatto tangibile sulla determinazione delle finalità e dei mezzi del trattamento»⁴⁰⁴. Inoltre occorre «verificare se il trattamento non sarebbe possibile senza la partecipazione di entrambe le parti alle finalità e ai mezzi, nel senso che i trattamenti di ciascuna parte sono tra loro indissociabili, ovvero sia indissolubilmente legati».⁴⁰⁵

Il Comitato europeo per la protezione dei dati, inoltre, sottolinea che non è necessario che le finalità del trattamento siano determinate in maniera congiunta, ma che vi è spazio per una contitolarità del trattamento ogni qualvolta siano perseguite finalità collegate o complementari.⁴⁰⁶ Allo stesso modo, per la determinazione congiunta dei mezzi, non è necessario che tutti i soggetti coinvolti determinino tutti i mezzi, ma si configura contitolarità anche ogni qualvolta i contitolari determinino i mezzi in misura diversa, in diverse fasi del trattamento o a livelli diversi.⁴⁰⁷

Seguendo l'interpretazione proposta dal Comitato europeo per la protezione dei dati, il rapporto tra istituzioni scolastiche o accademiche e piattaforme può essere definito come indissociabile, dal momento che, se mancasse il trattamento dei dati per finalità di istruzione da quest'ultima perpetrato, la piattaforma non avrebbe alcun tipo di accesso a questi dati, e dunque perderebbe la possibilità di processarli per finalità proprie.⁴⁰⁸

Dal momento che l'articolo 26 del GDPR postula la necessità di un accordo interno che determini in modo trasparente le responsabilità delle parti coinvolte rispetto al GDPR e rispetto ai soggetti coinvolti, è anche in questa sede necessario che tanto l'Università quanto la scuola, nella stipulazione del contratto, siano guidate da particolare attenzione nella scelta delle piattaforme da utilizzare per la didattica a distanza.⁴⁰⁹



⁴⁰⁴ Ibidem, par. 55.

⁴⁰⁵ Ibidem.

⁴⁰⁶ Ibidem, par. 60.

⁴⁰⁷ Ibidem, par. 63.

⁴⁰⁸ C. Angiolini, R. Ducato, A. Giannopoulou, G. Schneider, «Remote Teaching During the Emergency and Beyond: Four Open Privacy and Data Protection Issues of 'Platformised' Education», p. 52.

⁴⁰⁹ Ibidem.

Figura 7: sommario dei ruoli ricoperti dai vari soggetti coinvolti nel trattamento dei dati personali durante la didattica a distanza nel mondo universitario.

FONTE: C. Angiolini, R. Ducato, A. Giannopoulou, G. Schneider, «Remote Teaching During the Emergency and Beyond: Four Open Privacy and Data Protection Issues of ‘Platformised’ Education», Opinio Juris in Comparatione, vol. 1, 2020, November 13, 2020, pp. 45-72, p.55.

3.3 Osservazioni sulle privacy policy delle piattaforme maggiormente diffuse in ambito di didattica a distanza

3.3.1 La base giuridica e la finalità del trattamento nella didattica a distanza

Le Università e le scuole, in quanto, a seconda dei casi, titolari o contitolari del trattamento, determinano la finalità del trattamento, che deve necessariamente avvenire in conformità a delle basi giuridiche individuate dell’articolo 6 o dall’articolo 9 del GDPR. Ciò significa che la scelta che le Università e le scuole sono chiamate a compiere quando scelgono di far entrare nel circuito del trattamento anche soggetti terzi devono essere guidate da peculiare attenzione al fatto che anche le piattaforme effettuino un trattamento di dati rispettoso delle prescrizioni del GDPR.⁴¹⁰ Infatti, è importante ricordare che a mente del combinato disposto degli articoli 5 e 6 del GDPR, il trattamento dei dati personali può avvenire solamente per le specifiche finalità per cui sono raccolti, essendo preclusa ogni possibilità di effettuare il trattamento per finalità incompatibili con quelle inizialmente indicate.

Durante l’*emergency remote teaching*, i dati personali vengono trattati per finalità proprie delle esigenze istituzionali dell’ateneo o dell’istituto scolastico, legate allo svolgimento della didattica e degli esami. Ciò significa che il trattamento viene effettuato rispettando la base giuridica dell’esecuzione di un compito di interesse pubblico,⁴¹¹ o, in altri ordinamenti, secondo la base giuridica della necessità di eseguire un contratto⁴¹² di cui è parte il soggetto interessato al trattamento.⁴¹³

In Italia, l’Autorità Garante per i dati personali, nel provvedimento del 26 marzo 2020⁴¹⁴ contenente le prime indicazioni in materia di didattica a distanza, ha così statuito:

«Non deve pertanto essere richiesto agli interessati (docenti, alunni, studenti, genitori) uno specifico consenso al trattamento dei propri dati personali funzionali allo svolgimento dell’attività didattica a distanza, in quanto riconducibile – nonostante tali modalità innovative – alle funzioni istituzionalmente assegnate a scuole ed atenei».(...)

⁴¹⁰ C. Angiolini, R. Ducato, A. Giannopoulou, G. Schneider, «Remote Teaching During the Emergency and Beyond: Four Open Privacy and Data Protection Issues of ‘Platformised’ Education», p.53.

⁴¹¹ Articolo 6, par. 1, lett. e) del GDPR.

⁴¹² C. Angiolini, R. Ducato, A. Giannopoulou, G. Schneider, «Remote Teaching During the Emergency and Beyond: Four Open Privacy and Data Protection Issues of ‘Platformised’ Education», p.53.

⁴¹³ Articolo 6, par. 1, lett. b) del GDPR.

⁴¹⁴ Autorità Garante per la protezione dei dati personali, didattica a distanza, prime indicazioni.

«Le istituzioni scolastiche e universitarie dovranno assicurarsi (anche in base a specifiche previsioni del contratto stipulato con il fornitore dei servizi designato responsabile del trattamento), che i dati trattati per loro conto siano utilizzati solo per la didattica a distanza». (...)

«Ancora, con riferimento al trattamento dei dati degli studenti svolti dalle piattaforme quali responsabili del trattamento stesso, si ricorda che esso deve limitarsi a quanto strettamente necessario per la fornitura dei servizi richiesti ai fini della didattica on line, senza l'effettuazione di operazioni ulteriori, preordinate al perseguimento di finalità proprie del fornitore».

Nella pratica, ciò comporta che l'Università e la scuola debbano verificare se le piattaforme responsabili del trattamento effettuino un trattamento per finalità diverse e assicurarsi che tale finalità non sia incompatibile con quelle appena illustrate.

Il provvedimento testé citato rappresenta una risposta piuttosto timida⁴¹⁵ del Garante, che si è limitato a ricordare che il trattamento effettuato dalle piattaforme, quali responsabili, debba essere limitato a quanto strettamente necessario per la fornitura dei servizi necessari per la DaD, senza possibilità di operazioni finalizzate al perseguimento di finalità proprie del fornitore.

Le istituzioni scolastiche e universitarie sono perciò chiamate a verificare che i responsabili del trattamento scelti effettuino il trattamento dei dati personali per finalità collegate alla sola didattica a distanza, impegnandosi a vigilare sull'operato dei fornitori delle principali piattaforme per verificare il rispetto del GDPR.

3.3.2 Alcune osservazioni critiche sulle privacy policy delle piattaforme della DaD

Nel capitolo precedente si è illustrato come, nel repentino passaggio dalla didattica tradizionale alla didattica a distanza per finalità di contenimento del virus, alcuni istituti scolastici abbiano utilizzato servizi di videoconferenza «generalisti»⁴¹⁶, ovvero estranei al mondo dell'istruzione e non pensati per essere responsabili del trattamento.

Riportando lo studio precedentemente citato⁴¹⁷, si noti come altri istituti sia scolastici che di istruzione superiore abbiano anche fatto affidamento a piattaforme come MoodleCloud e G-Suite for Education, che nascono come servizi finalizzati a usi scolastici ed educativi e pertanto permettono di essere nominati responsabili del trattamento.

⁴¹⁵ R. Caso, «Università delle piattaforme: la DAD, il business dei dati personali e la fine dell'autonomia», Agenda Digitale, 12 agosto 2021, consultabile al link:

<https://www.agendadigitale.eu/sicurezza/privacy/universita-delle-piattaforme-la-dad-il-business-dei-dati-personali-e-la-fine-dellautonomia/>.

⁴¹⁶ Ad esempio, l'applicazione di messaggistica istantanea *Whatsapp*, parte dell'universo *Meta*. Si v. capitolo II, par. 2.3.2 e S. Zoja, «La scuola italiana al mercato dei dati. Così il controllo sulla didattica rafforza lo strapotere delle multinazionali», *Altreconomia*, marzo 2022.

⁴¹⁷ Il presente paragrafo, e il successivo, riprendono l'analisi delle privacy policy effettuata da R. Ducato, G. Priora, C. Angiolini, A. Giannopoulou, B.J. Jutte, G. Noto La Diega, L. Pascault, G. Schneider in «Didattica di emergenza o Emergency Remote Teaching: un'analisi empirica in tema di privacy e diritto d'autore dei termini e condizioni dei servizi online più diffusi».

Tuttavia, per la dottrina citata, solleva comunque criticità il fatto che molte di queste piattaforme mettano in atto un trattamento dei dati personali per finalità proprie e diverse da quelle legate alle attività didattiche, contrariamente a quanto raccomandato dal Garante.

Ad esempio, nello studio è segnalato che le privacy policy di piattaforme come G-Suite for Education o Zoom, pur fornendo una lista di categorie di dati trattati e una lista dettagliata delle finalità, non rendono intellegibile il rapporto tra singoli dati e finalità.

In altri casi, come in Jitsi, la finalità risulta descritta in maniera estremamente vaga, ovvero nel «miglioramento del servizio», o oscura, come nel caso di MoodleCloud, in cui la finalità del trattamento è quella di «*central code repository o developer code repository*».

Volgendo l'analisi alle previsioni in materia di liceità del trattamento, si sottolineano i seguenti elementi critici.

La privacy policy di G-Suite for Education, ad esempio, non riporta la base giuridica del trattamento di determinati dati.

Talvolta, come nel caso di Zoom e Discord, la base giuridica del trattamento riportata dall'informativa del 2020 è il consenso, descritto spesso in termini incompatibili con la disciplina descritta nel GDPR. Nel caso di Zoom, infatti, all'utente è data la possibilità di procedere alla registrazione di un incontro, lasciando agli altri utenti la scelta se accettare la registrazione e dunque il trattamento dei dati, oppure rifiutare e abbandonare l'incontro. Risulta quindi chiaro che tale consenso non sarà liberamente prestato ai sensi dell'articolo 4 numero 11 del GDPR.

Nel caso di Discord, invece, l'informativa analizzata ammette la possibilità di prestare un consenso implicito, contrariamente a quanto previsto dal GDPR, che postula la necessità di un consenso espresso in maniera libera, specifica, informata e inequivocabile.

Dall'analisi della privacy policy di Zoom, piattaforma ampiamente utilizzata per la DaD, emerge anche il trattamento dei dati personali sulla base giuridica del legittimo interesse, che necessita un'attività di bilanciamento tra l'interesse legittimo del titolare del trattamento e quello dell'interessato, di cui però non v'è traccia nell'informativa. Tale test comparativo rappresenta un *quid pluris* rispetto ad un mero confronto tra due pesi facilmente quantificabili e comparabili: occorre infatti tenere conto di diversi fattori quali i) la natura e l'origine dell'interesse legittimo, nonché l'eventualità che il trattamento dei dati sia necessario per l'esercizio di un diritto fondamentale o per l'esecuzione di un compito di interesse pubblico o sia riconosciuto dalla comunità interessata; ii) l'impatto sugli interessati e sulle loro aspettative circa ciò che accadrà ai dati; iii) la natura dei dati e le modalità del trattamento; iv) le garanzie supplementari in grado di limitare l'impatto sull'interessato, come, *ex multis*, la minimizzazione dei dati, una maggiore trasparenza, il diritto di «opt-out» e la portabilità dei dati.⁴¹⁸

⁴¹⁸Per un approfondimento sul bilanciamento tra l'interesse legittimo del titolare del trattamento e quello dell'interessato, si v. Gruppo di Lavoro ex articolo 29 per la protezione dei dati, parere 6/2014 sul concetto di interesse legittimo del responsabile del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE, adottato il 9 aprile 2014, consultabile al link: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_it.pdf.

Si è inoltre precedentemente osservato che durante le attività di DaD è frequente il trattamento di categorie particolari di dati ai sensi dell'articolo 9 del GDPR. Nel campione analizzato, composto da 9 piattaforme, è emerso che solamente le privacy policy di Facebook e MoodleCloud descrivono la diversa base giuridica necessaria per il trattamento di categorie particolari di dati.

3.3.3 Come le privacy policy delle piattaforme DaD descrivono i diritti dell'interessato previsti del GDPR

Il capo III del GDPR, rubricato «diritti dell'interessato», contiene una serie di norme che declinano il nuovo catalogo dei diritti riconosciuto in capo al soggetto interessato al trattamento. Tali diritti sono: diritto a ricevere informazioni (artt. 13 e 14); diritto di accesso (art. 15); diritto alla rettifica (art. 16); diritto alla cancellazione («diritto all'oblio») (art. 17); diritto alla limitazione di trattamento (art. 18); diritto alla portabilità dei dati (art. 20); diritto di opposizione (art. 21); diritto a non essere sottoposto ad una decisione interamente automatizzata.⁴¹⁹ Queste disposizioni del GDPR, particolarmente rilevanti, sono state descritte come il marchio di fabbrica del legislatore europeo.⁴²⁰

Tutte le informative analizzate dallo studio contengono un riferimento ai diritti appena enunciati, ad eccezione di G-Suite for Education. Le criticità, tuttavia, si riscontrano con riferimento al modo in cui tali diritti vengono descritti. Infatti, nonostante il rispetto *pro forma* degli obblighi di informazione, nella sostanza non è possibile parlare di informative trasparenti e intelligibili.

Ad esempio, Zoom utilizza il condizionale («*potresti avere il diritto di*»), senza peraltro chiarire quale tra le due privacy policy presenti sul sito web si applichi al trattamento in questione.

Microsoft Teams, invece, rende particolarmente complessa la consultazione delle informazioni riguardanti i diritti dell'interessato al trattamento, obbligandolo a un'operazione di ricostruzione dei suoi diritti tra una serie di link e documenti.

Per quanto riguarda, invece, il diritto di presentare un reclamo ad un'autorità di controllo ex articolo 77 GDPR, MoodleCloud, pur riconoscendo il diritto di presentare il reclamo in questione, fornisce i dettagli dell'autorità di controllo irlandese. Tale indicazione è in contrasto con le previsioni del GDPR, che all'articolo 77 riconosce all'interessato il diritto di proporre reclamo a un'autorità di controllo, segnatamente nello Stato membro di residenza abituale oppure del luogo ove si è verificata la presunta violazione. L'informativa di MoodleCloud, fornendo solamente i dettagli dell'autorità di controllo irlandese, pone dunque l'interessato nelle condizioni di credere di poter esercitare il diritto di presentare un reclamo solamente nei confronti di tale autorità, contrariamente a quanto previsto dal Regolamento.⁴²¹

⁴¹⁹ Per un'analisi dei diritti menzionati, si v. G.M. Riccio, G. Scorza, E. Bellisario, «GDPR e normativa privacy, commentario».

⁴²⁰ F. Calisai. «I diritti dell'interessato», in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), I dati personali nel diritto europeo, Torino, Giappichelli, 2019, pp.327-351.

⁴²¹ La disciplina italiana in materia di reclamo si trova invece agli articoli 140-bis-143 del Codice della privacy. Più nello specifico, l'articolo 140-bis permette all'interessato che ritenga che i diritti di cui gode siano stati violati di proporre reclamo al Garante per la protezione dei dati personali o, alternativamente, ricorso dinanzi all'autorità giudiziaria. L'articolo 141 permette all'interessato di rivolgersi al Garante

In generale, nello studio è stata riportata una preoccupante e sistematica violazione del principio di trasparenza, che finisce per impattare sulla possibilità stessa di esercizio, anche in giudizio, dei diritti da parte degli interessati.⁴²²

mediante reclamo ai sensi dell'articolo 77 del Regolamento. Il reclamo (i) contiene: un'indicazione per quanto possibile dettagliata dei fatti e delle circostanze su cui si fonda; (ii) delle disposizioni che si presumono violate e delle misure richieste; (iv) gli estremi identificativi del titolare o del responsabile del trattamento ove conosciuto, (v) sottoscrizione dell'interessato o, su mandato di questo, di un ente del terzo settore che sia attivo nel settore della tutela dei dati e delle libertà degli interessati con riguardo alla protezione dei dati personali (articolo 142, commi 1-2). Il modello del reclamo è messo a disposizione del Garante ed è disponibile al link:

[https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/4535524#:~:text=L'apposita%20istanza%20all'Autorit%C3%A0,rpd%40gdpd.it\).](https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/4535524#:~:text=L'apposita%20istanza%20all'Autorit%C3%A0,rpd%40gdpd.it).)

Il Garante decide il reclamo entro nove mesi dalla data di presentazione e, in ogni caso, entro tre mesi dalla predetta data informa l'interessato sullo stato del procedimento (articolo 143 comma 3).

⁴²² R. Ducato, G. Priora, C. Angiolini, A. Giannopoulou, B.J. Jutte, G. Noto La Diega, L. Pascault, G. Schneider, «Didattica di emergenza o Emergency Remote Teaching: un'analisi empirica in tema di privacy e diritto d'autore dei termini e condizioni dei servizi online più diffusi», p.13: «*seri dubbi rimangono circa la possibilità che l'interessato possa effettivamente esercitare quei diritti se alcune informazioni sostanziali sul trattamento mancano o non sono chiare. Si ritiene, infatti, che l'impossibilità di poter controllare il flusso informativo dovuto alla violazione del principio di trasparenza finisca per impattare sulla possibilità stessa di esercizio, anche in giudizio, dei diritti da parte degli interessati, possibilità garantita dagli Artt.47 e 8 CDFUE*».

Finalità	Liceità		Diritti dell'interessato		
	Base giuridica	Eccezione al divieto di trattamento dei dati sensibili	Esistenza dei diritti	Come esercitare i diritti	Diritto di proporre reclamo a un'autorità di controllo
Discord	■	■	■	□	□
Facebook	■	□	□	■	□
G-Suite for Education	■	■	■	■	■
Jitsi Meet	■	■	□	□	□
MoodleCloud	■	□	□	□	■
Microsoft Teams	■	■	□	□	□
Skype	■	■	□	□	□
YouTube	■	■	□	■	■
Zoom	■	■	■	■	□

Clausola non problematica
 Clausola problematica

Figura 8: visione d'insieme dello studio delle privacy policy.

FONTE: R. Ducato, G. Priora, C. Angiolini, A. Giannopoulou, B.J. Jutte, G. Noto La Diega, L. Pascault, G. Schneider, «Didattica di emergenza o Emergency Remote Teaching: un'analisi empirica in tema di privacy e diritto d'autore dei termini e condizioni dei servizi online più diffusi», *Law and Media working paper series*, no.2/2020, p. 10.

A conclusioni sostanzialmente analoghe giunge anche il report di Noyb (sigla per il motto «*my privacy is none of your business*»)⁴²³, organizzazione senza scopo di lucro fondata dall'attivista austriaco Maximilian Schrems, che analizza le privacy policy dei sei software di videoconferenza (Zoom, Webex Meetings, GoToMeeting, Skype, Teams,

⁴²³ Noyb, «La telecamera nel soggiorno: la privacy nei sistemi di videoconferenza», 2 aprile 2020, consultabile al link: <https://noyb.eu/it/>.

Wire) utilizzati, non solo per finalità didattiche, per far fronte alle esigenze di confinamento durante la pandemia da SARS-Cov-2.

L'analisi verte sulle privacy policy così come formulate alla data del 31 marzo 2020 e sottolinea, anche in questo caso, la mancanza di trasparenza. Ad esempio Microsoft, proprietario tanto di Teams quanto di Skype, mette a disposizione un'informativa sulla privacy lunga ben sessanta pagine, rendendo complessa la lettura per il soggetto interessato al trattamento.

Anche Noyb ha rilevato che le privacy policy esaminate non specificano per quali finalità e grazie a quali basi giuridiche specifiche sono trattate le singole categorie di dati. Inoltre, non è chiaro se e in quali termini i dati raccolti siano condivisi con terze parti (si veda, infatti, l'utilizzo di locuzioni al condizionale come «*may share*» ovvero «potrebbe condividere»).

Il principio di trasparenza non è rispettato nemmeno per quanto riguarda la durata della conservazione dei dati raccolti. Non solo non è specificato per quanto tempo le singole categorie di dati raccolti sono conservati, ma si utilizzano, anche in questo caso, formule generiche come «*as long as necessary*».

Symbols:  means mostly satisfactory.  means partly satisfactory.  means not satisfactory.

Information according to Article 13 GDPR	Zoom	Webex Meetings (Cisco)	GoToMeeting (LogMeIn)	Skype (Microsoft)	Teams (Microsoft)	Wire
Identity and contact details of the controller						
Contact details of the DPO						
Purposes of processing						
Legal basis for processing						
In case of legitimate interests: What are the interests of the controller or third parties?		Not applicable				
Interconnection: categories of personal data, purposes, and legal bases						
Recipients or categories of recipients of the personal data						
Transfers outside of the EU/EEA						
Retention periods						
GDPR right to withdraw the consent						
GDPR right to lodge a complaint						
Existence of automated decision making						

Figura 9: Panoramica sul rispetto degli obblighi di informativa ex articolo 13 GDPR.
 FONTE: Noyb, «La telecamera nel soggiorno: la privacy nei sistemi di videoconferenza»,
 2 aprile 2020, consultabile al link: <https://noyb.eu/it/>.

3.3.4. Analisi delle privacy policy attuali

In questa sede si intende analizzare le privacy policy dei nove esempi di software per la gestione di contenuti online, piattaforme di condivisione di contenuti, social networks e servizi di comunicazione impiegati durante la DaD, così come attualmente formulate in riferimento al tipo di dati personali raccolti, alla base giuridica del trattamento e ai diritti dell'interessato, cercando di evidenziare eventuali cambiamenti nella formulazione rispetto a quella oggetto di analisi critica nei paragrafi precedenti.

La piattaforma Discord⁴²⁴ contiene un elenco delle informazioni che vengono raccolte, che vengono suddivise in informazioni fornite dall'utente, raccolte automaticamente, e informazioni ricevute da altre fonti. Con riferimento a quest'ultimo insieme di informazioni, si noti l'utilizzo del condizionale:

«potremmo ricevere informazioni sull'utente da altre fonti, ivi incluso da altri utenti e terzi, e potremmo raggruppare tali le informazioni con altre informazioni che abbiamo sull'utente. Ad esempio, se l'utente interagisce con il nostro account di social media su un'altra piattaforma, potremmo ricevere determinate informazioni sull'utente, come per esempio il suo nome utente su tale piattaforma».

Permangono dunque alcune criticità in forza di una descrizione del tipo di dati trattati estremamente vaga. Per quanto riguarda la base giuridica del trattamento, essa è ricondotta: (i) alla necessità dell'esecuzione di un contratto di cui l'interessato è parte; (ii) per il perseguimento dell'interesse legittimo commerciale del titolare; (iii) per ottemperare a obblighi legali; (iv) sulla base del consenso dell'interessato; (v) per la salvaguardia degli interessi vitali dell'interessato. Con riferimento alla base giuridica dell'interesse legittimo, è omesso il riferimento al bilanciamento tra il legittimo interesse del titolare del trattamento e quello dell'interessato. Inoltre, ogni riferimento al trattamento di categorie particolari di dati ex articolo 9 GDPR e la descrizione di una base giuridica adeguata al trattamento di questi ultimi risulta assente. Le criticità precedentemente evidenziate non risultano dunque superate. Discord contiene inoltre delle informazioni aggiuntive per gli utenti residenti nell'Unione europea, Regno Unito, Svizzera e Brasile, riferendo la possibilità di poter godere di diritti ulteriori (*«you may have additional rights»*). Anche questa formulazione risulta vaga e poco intelligibile, non chiarendo quali dei diritti enunciati spettino nello specifico ai sensi del GDPR. Inoltre, manca il riferimento al diritto ex articolo 77 del GDPR, che riconosce all'interessato la possibilità di proporre reclamo all'autorità di controllo dello Stato membro in cui risiede quando questi ritenga che il trattamento effettuato violi il GDPR.

L'informativa privacy del social network Facebook⁴²⁵ contiene un puntuale elenco delle informazioni raccolte, così come delle diverse basi giuridiche individuate. Per ogni base giuridica, è poi possibile accedere all'elenco dei dati personali oggetto di trattamento. In ogni caso, l'informativa specifica che *«le effettive informazioni»* usate *«potrebbero variare in base alle circostanze concrete»*, ma potrebbero comprendere alcune di quelle riportate a titolo esemplificativo. Non è presente il riferimento al bilanciamento necessario in caso di trattamento sulla base giuridica dell'interesse legittimo, mentre è presente una peculiare attenzione alle categorie particolari di dati,

⁴²⁴ Si v. <https://discord.com/privacy#control>.

⁴²⁵ Si v. <https://mbasic.facebook.com/privacy/policy/printable/#2>.

raccolte sulla sola base giuridica del consenso e sottoposto a «protezione speciale». Per quanto riguarda il riconoscimento dei diritti ai sensi del GDPR, essi sono puntualmente e chiaramente enunciati, con una descrizione sulle modalità di esercizio. In ogni caso, l'informativa è lunga 135 pagine, dunque certamente non in forma «*concisa*» ai sensi dell'articolo 12 del GDPR.

G-Suite for Education è stato sostituito da Google Workspace for Education.⁴²⁶ Tale informativa sulla privacy risulta poco chiara, poiché presenta numerosi richiami alle norme sulla privacy di Google,⁴²⁷ valide per i servizi principali come Google Calendar e Classroom, e all'informativa sulla privacy di Google Cloud⁴²⁸, valida invece per i servizi aggiuntivi, come YouTube e Maps. Tali informative sono applicabili nelle parti non diversamente regolate dall'informativa di Google Workspace for Education. La privacy policy della piattaforma didattica di Google riporta l'elenco di alcune informazioni che vengono raccolte tramite i servizi, tanto principali che aggiuntivi, associati a Google Workspace for Education, ma per avere informazioni sulla base giuridica del trattamento e sui diritti dell'interessato, è necessario accedere alle altre informative. Le norme sulla privacy di Google presentano un'apposita sezione dedicata ai «*requisiti europei*», in cui vengono descritte le basi giuridiche del trattamento, ma senza spiegare quale sia la base giuridica per il trattamento associato alle singole categorie di dati raccolte. Particolarmente criticabile è inoltre il riferimento ai diritti dell'interessato, infatti l'informativa non presenta un elenco dei diritti previsti dal GDPR, lasciando all'interessato l'onere di contattare l'ufficio di Google responsabile della protezione dei dati per ricevere maggiori informazioni in merito ai suoi diritti. L'informativa sulla privacy di Google Cloud, invece, risulta in parte più completa, dal momento che, pur contenendo un breve elenco dei dati raccolti, contiene un'apposita voce «*standard europei sulla privacy e GDPR*», in cui a ogni base giuridica viene associata la tipologia di dati di servizio trattati. Anche in questa informativa manca tuttavia un puntuale elenco dei diritti dell'interessato. Entrambe le informative riconoscono la base giuridica del trattamento nel legittimo interesse del titolare, senza tuttavia alcun riferimento al bilanciamento tra i legittimi interessi di quest'ultimo e dell'utente. Inoltre, non è presente alcun riferimento alle categorie particolari di dati ex articolo 9 GDPR.

La privacy policy di Jitsi⁴²⁹ non è stata aggiornata rispetto a quella oggetto dell'analisi prima riportata: l'ultimo aggiornamento risulta infatti quello del 30 marzo 2020.

La privacy policy di MoodleCloud⁴³⁰, già nel 2020, non destava particolari elementi di criticità rispetto alla base giuridica del trattamento e alla particolare attenzione alla base giuridica per il trattamento di categorie particolari di dati ai sensi dell'articolo 9 del GDPR. Anche nell'attuale formulazione tali riferimenti risultano puntualmente riportati, anche grazie alla presenza di un «*Register of GDPR Information*» che descrive in maniera puntuale i dati raccolti e la finalità del trattamento collegate. Anche il riferimento ai

⁴²⁶ Si v.

https://workspace.google.com/terms/education_privacy.html#privacy-police-revamp-your-info.

⁴²⁷ Si v. <https://policies.google.com/privacy?hl=it#europeanrequirements>.

⁴²⁸ Si v. <https://cloud.google.com/terms/cloud-privacy-notice?hl=it>.

⁴²⁹ Si v. <https://jitsi.org/meet-jit-si-privacy/>.

⁴³⁰ Si v. <https://moodle.com/privacy-notice/>.

diritti dell'interessato rimane chiaro, tuttavia, è ancora presente il riferimento alla sola autorità di controllo irlandese: sono pertanto ancora valide le criticità in riferimento all'articolo 77 del GDPR sottolineate nei paragrafi precedenti.

Microsoft Teams, invece, rende tutt'ora disponibile per gli utenti una privacy policy⁴³¹ che non specifica in maniera chiara i dati raccolti e la base giuridica del trattamento. Essa fa infatti solo riferimento alla sola base giuridica dell'interesse legittimo nel caso di un trattamento di dati personali per lo svolgimento di attività commerciali legittime, senza ulteriori specificazioni circa il bilanciamento dell'interesse del titolare del trattamento con quello dell'interessato. Per ricevere maggiori informazioni circa il trattamento dei dati personali, l'utente dovrebbe consultare altre pagine web, come l'informativa sulla privacy di Microsoft⁴³² e il riepilogo del GDPR⁴³³ reso disponibile da Microsoft, tra le cui «*frequently asked questions*» è riportato l'elenco dei diritti dell'interessato. Le informazioni che il titolare è tenuto a dare non sono quindi «*facilmente accessibili*» ai sensi dell'articolo 12 del GDPR, dal momento che l'utente è chiamato a reperire le informazioni da diverse fonti.

Consultando la privacy policy di Skype,⁴³⁴ si viene ricondotti al sito web dell'informativa della Privacy di Microsoft, che ha acquistato Skype nel 2011.

Per quanto riguarda YouTube, alcune informazioni vengono fornite presso la pagina web «panoramica delle nozioni di base sulla privacy per le app YouTube»⁴³⁵, ma le informazioni relative ai dati oggetto di trattamento, alla base giuridica e ai diritti dell'interessato sono accessibili all'utente presso le norme sulla privacy di Google già analizzate.

Infine, l'informativa sulla privacy di Zoom⁴³⁶ contiene una sezione appositamente dedicata alle informazioni specifiche sulla protezione dei dati nell'Unione europea. Essa contiene il riferimento alla base giuridica del trattamento e, diversamente dalla formulazione precedente, riporta che il trattamento dei dati personali sulla base degli interessi legittimi del titolare sarà possibile solamente «*a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali*». Continua a destare criticità la possibilità per un utente di procedere alla registrazione di un incontro, lasciando agli altri partecipanti la scelta se acconsentire alla registrazione dei dati e quindi al trattamento oppure abbandonare l'incontro: si dubita infatti che tale trattamento avvenga grazie alla base giuridica del consenso liberamente prestato ai sensi dell'articolo 4 del GDPR. Inoltre, manca ogni riferimento al trattamento di categorie particolari di dati ai sensi dell'articolo 9 del GDPR. I diritti dell'interessato sono formulati in maniera chiara e trasparente, abbandonando la formulazione al condizionale precedentemente criticata; tuttavia, viene spiegato solamente come esercitare il diritto d'accesso tramite un apposito *form*⁴³⁷ e come

⁴³¹ Si v. <https://learn.microsoft.com/en-us/microsoftteams/teams-privacy>.

⁴³² Si v. <https://privacy.microsoft.com/it-it/privacystatement>.

⁴³³ Si v. <https://learn.microsoft.com/it-it/compliance/regulatory/gdpr?view=o365-worldwide#gdpr-faqs>.

⁴³⁴ Si v. <https://www.skype.com/en/legal/>.

⁴³⁵ Si v. <https://support.google.com/youtube/answer/10364219?hl=it#zippy=>.

⁴³⁶ Si v. <https://explore.zoom.us/it/privacy/>.

⁴³⁷ Si v.

<https://zoom-privacy.my.onetrust.com/webform/65962359-ef0d-4399-9db4-572d06de08aa/f277f9f7-bfee-4233-815e-80e290139bc2>.

esercitare il diritto alla revoca del consenso: manca invece una spiegazione circa le modalità di esercizio del diritto alla cancellazione, all'opposizione, rettifica e limitazione del trattamento. Analogamente alla privacy policy del 2020, l'informativa contiene l'espresso riferimento alla possibilità di sporgere un reclamo al Garante per la protezione dei dati locale.

3.4 La disciplina del trasferimento dei dati personali della didattica ai sensi del GDPR

3.4.1 Il trasferimento transfrontaliero nella direttiva 95/46/CE e nel GDPR

Pur mancando una definizione di «trasferimento transfrontaliero», è comunque possibile comprendere il fenomeno attraverso la lettura dell'articolo 44 del GDPR, che lo descrive come:

«Qualunque trasferimento di dati personali oggetto di un trattamento o destinati a essere oggetto di un trattamento dopo il trasferimento verso un paese terzo o un'organizzazione internazionale, compresi trasferimenti successivi di dati personali da un paese terzo o un'organizzazione internazionale verso un altro paese terzo o un'altra organizzazione internazionale».

Un primissimo tentativo di definire il concetto di trasferimento transfrontaliero di dati si ha con la sentenza della Corte di Giustizia dell'Unione europea *Bodil Lindqvist*⁴³⁸. Il caso riguardava una volontaria svedese che aveva condiviso sul suo blog di un *hosting provider* stabilito fuori dall'Unione europea una serie di informazioni riguardanti i suoi compagni volontari, divulgando dati sanitari. Tali dati furono resi accessibili per chiunque, ma la Corte di Giustizia non qualificò tale vicenda come un trasferimento transfrontaliero dei dati, ritenendo non sufficiente una mera messa a disposizione verso altri soggetti, essendo piuttosto necessario un atto positivo del titolare e del responsabile del trattamento.

È opportuno sottolineare che il trasferimento transfrontaliero dei dati personali era già disciplinato dalla direttiva 95/46/CE⁴³⁹, che per prima riconosceva l'importanza del fenomeno. Nel Considerando 56, infatti, il trasferimento dei dati personali oltre la frontiera dell'allora Comunità europea era presentato quale necessario per lo sviluppo degli scambi internazionali.

Il titolo IV della suddetta direttiva, in particolare l'articolo 25, vietava un trasferimento transfrontaliero dei dati personali ogni qualvolta non vi fosse un «livello di protezione adeguato». Tale livello di protezione adeguato andava valutato

⁴³⁸ Corte di Giustizia dell'Unione europea, Sentenza della Corte, 24 ottobre 1995, Causa C-101/01, consultabile al

link: <https://curia.europa.eu/juris/document/document.jsf?docid=48382&doclang=IT>.

⁴³⁹ Direttiva 95/46/CE del Parlamento europeo e del Consiglio, 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione dei dati, consultabile al link:

<https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:31995L0046>.

«con riguardo a tutte le circostanze relative ad un trasferimento o ad una categoria di trasferimenti di dati; in particolare sono presi in considerazione la natura dei dati, le finalità del o dei trattamenti previsti, il paese d'origine e il paese di destinazione finale, le norme di diritto, generali o settoriali, vigenti nel paese terzo di cui trattasi, nonché le regole professionali e le misure di sicurezza ivi osservate».⁴⁴⁰

Veniva peraltro disciplinato un particolare meccanismo di confronto tra Stati membri e Commissione, prevedendo che questi si comunicassero a vicenda eventuali dubbi circa l'adeguatezza del livello di protezione offerto dai paesi terzi.

Ogni qualvolta un paese terzo non avesse offerto un livello di protezione adeguato, ai sensi dell'articolo 25, paragrafo 6, la Commissione avrebbe potuto adottare una decisione di adeguatezza, permettendo dunque il trasferimento transfrontaliero. In ogni caso, pur in assenza di una decisione di adeguatezza e in assenza di un livello di protezione adeguato, a mente dell'articolo 26 il trasferimento era possibile non solo nel caso in cui l'interessato avesse prestato il consenso inequivocabile, ma anche per l'esecuzione di un contratto o per la salvaguardia di un interesse vitale della persona interessata. Il trasferimento era inoltre possibile, sempre ai sensi dell'articolo 26, quando necessario o prescritto dalla legge per la salvaguardia di un interesse pubblico rilevante, oppure per constatare, esercitare o difendere un diritto per via giudiziaria, e infine nel caso in cui il trasferimento avvenisse a partire da un registro pubblico predisposto per l'informazione del pubblico in forza di legge e regolamento e fosse aperto alla consultazione del pubblico o di chiunque potesse dimostrare un interesse legittimo.

Come già chiarito, la disciplina in materia di protezione dei dati personali è oggi contenuta nel GDPR, che dedica al trasferimento transfrontaliero dei dati il capo V. Nel dettare un insieme di condizioni che rendono possibile il trasferimento dei dati personali in paesi estranei, detti appunto «paesi terzi» al territorio dell'Unione europea e dello Spazio Economico europeo⁴⁴¹, è previsto un generale divieto di trasferimento dei dati personali verso paesi terzi quando non si rispettino le indicazioni contenute al capo V.

In generale, è possibile notare che il GDPR presta molta attenzione al trasferimento transfrontaliero dei dati personali. Viene infatti *expressis verbis* previsto che se il titolare del trattamento intenda effettuare un trasferimento transfrontaliero di dati personali, dovrà necessariamente farne comunicazione nell'informativa privacy, sottostando agli obblighi di trasparenza e chiarezza previsti dal GDPR stesso (articoli 12, 13 e 14 GDPR).

In primis, ai sensi dell'articolo 45 del GDPR, il trasferimento è possibile in presenza di una decisione di adeguatezza adottata dalla Commissione, in cui essa decide che un paese terzo, un territorio o uno o più settori specifici all'interno del paese terzo o dell'organizzazione internazionale, garantiscono un livello di protezione adeguato, in modo tale da assicurare che il livello protezione delle persone fisiche previsto dal GDPR non sia pregiudicato dal trasferimento.

Per accertare che il livello di protezione offerto dai paesi terzi sia adeguato, la Commissione deve ottenere il parere favorevole del Comitato europeo per la protezione dei dati ed è chiamata a prendere in considerazione una serie di elementi puntualmente

⁴⁴⁰ Articolo 25, par. 2 Direttiva 95/46/CE.

⁴⁴¹ Che comprende, oltre all'UE, Norvegia, Liechtenstein e Islanda.

descritti dal secondo paragrafo dello stesso articolo. *Ex multis*, occorrerà prendere in considerazione elementi quali la presenza di uno stato di diritto, il rispetto dei diritti umani e delle libertà fondamentali, la pertinente legislazione e l'attuazione della stessa, l'esistenza e l'effettivo funzionamento di un'autorità di controllo indipendente con competenza a garantire e controllare il rispetto dei dati personali, nonché gli impegni internazionali assunti dal paese terzo o dall'organizzazione internazionale.

È previsto un meccanismo di riesame periodico almeno ogni quattro anni che tenga conto degli eventuali sviluppi avvenuti nel paese terzo o nell'organizzazione internazionale. Se risulta che non sia più garantito un livello di protezione adeguato, la Commissione ha il potere di revocare, modificare o sospendere nella misura necessaria la decisione di adeguatezza. Successivamente, la Commissione è chiamata ad avviare consultazioni con il paese terzo o l'organizzazione internazionale per porre rimedio alla decisione di revocare, modificare o sospendere la decisione di adeguatezza.

Ad oggi, sono state adottate decisioni di adeguatezza nei confronti dei seguenti Paesi terzi: Andorra; Argentina; Australia; Canada (soltanto per i trattamenti soggetti al PIPEDA⁴⁴²); Giappone; Guernsey; Isola di Man; Isole Faroe; Israele; Jersey; Nuova Zelanda; Regno Unito (soltanto per l'adeguamento al GDPR e alla Direttiva 2016/680⁴⁴³); Repubblica di Korea; Svizzera; Stati Uniti; Uruguay.⁴⁴⁴

La portata innovativa del GDPR rispetto alla direttiva 95/45/CE si legge nel fatto che, in mancanza di una decisione di adeguatezza, il GDPR, all'articolo 46, ammette il trasferimento transfrontaliero dei dati in presenza di garanzie adeguate ed a condizione che gli interessati al trattamento dispongano di diritti azionabili e mezzi di ricorso effettivi.

Il secondo paragrafo dell'articolo 46 contiene un puntuale elenco di garanzie adeguate in presenza delle quali il trasferimento transfrontaliero è possibile, senza alcuna necessità di ogni qualsivoglia tipo di autorizzazione da parte di autorità di controllo, mentre nel terzo paragrafo si richiede, oltre alla presenza delle garanzie adeguate ivi descritte, un'autorizzazione dell'autorità di controllo competente.

La prima garanzia riportata dal secondo paragrafo dell'articolo 46 (articolo 46, paragrafo 2, lettera a) GDPR) è «*uno strumento giuridicamente vincolante e avente efficacia esecutiva tra autorità pubbliche o organismi di controllo*», su cui il Comitato europeo per la protezione dei dati (EDPB) fornisce delle importanti linee guida⁴⁴⁵,

⁴⁴² The Personal Information Protection and Electronic Documents Act (PIPEDA), si v. <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/>.

⁴⁴³ Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio, consultabile al link:

<https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32016L0680&from=RO>.

⁴⁴⁴ L'elenco è consultabile al seguente link: <https://eur-lex.europa.eu/homepage.html>.

⁴⁴⁵ European Data Protection Board, Linee guida 2/2020 sull'articolo 46, paragrafo 2, lettera a), e paragrafo 3, lettera b), del Regolamento 2016/679 per i trasferimenti di dati personali tra autorità ed organismi pubblici del SEE e di paesi non appartenenti al SEE, versione 2.0, 15 dicembre 2020. Consultabili al link:

analizzando tale garanzia congiuntamente a quella presente al terzo paragrafo, lettera b), ovvero «*disposizioni da inserire in accordi amministrativi tra autorità pubbliche o organismi pubblici che comprendono diritti effettivi e azionabili per gli interessati*».

Più nello specifico, affinché sia possibile rientrare nell'ambito di applicazione dell'articolo 46, paragrafo 2, lettera a), il Comitato europeo per la protezione dei dati spiega che è possibile utilizzare trattati internazionali, trattati di diritto pubblico o accordi amministrativi direttamente applicabili. In ogni caso, qualsiasi strumento giuridicamente vincolante e avente efficacia esecutiva deve contenere indicazioni circa i principi in materia di protezione dei dati e i diritti dell'interessato in ossequio a quanto previsto dal GDPR. L'accordo, affinché non sia compromesso il livello di tutela offerto dal GDPR, deve anche indicare le modalità con cui l'organismo pubblico destinatario applica i principi fondamentali in materia di dati personali e di diritti dell'interessato. L'EDPB chiarisce inoltre l'importanza della presenza effettiva di possibilità di ricorso giurisdizionale, e, laddove questa non sia presente, è necessario cercare un meccanismo di ricorso alternativo, lasciando il compito preventivo agli organismi pubblici dello Spazio economico europeo di consultare l'autorità di controllo competente.⁴⁴⁶

Con riferimento alla previsione di cui all'articolo 46, paragrafo 3, lettera b), invece, postula la necessità di strumenti amministrativi alternativi, quali ad esempio un protocollo d'intesa, che dovranno garantire all'interessato mezzi di ricorso effettivi. È peraltro fondamentale che i diritti individuali siano pienamente garantiti dalla legislazione nazionale del paese terzo, e che possano essere esercitati dalle persone fisiche dello spazio economico europeo alle stesse condizioni dei cittadini e residenti del paese terzo. Quando non possibile, le parti sono chiamate ad assumere impegni specifici e mezzi procedurali finalizzati a garantire effettivi mezzi di ricorso per i soggetti interessati, affinché si ottenga un livello di protezione sostanzialmente equivalente a quello garantito dall'interno dell'UE grazie al GDPR.⁴⁴⁷

Il GDPR ammette il trasferimento transfrontaliero dei dati personali, in assenza di una decisione di adeguatezza, anche in presenza di «*norme vincolanti d'impresa in conformità dell'articolo 47*». ⁴⁴⁸ Tali norme vincolanti d'impresa devono essere approvate dall'autorità di controllo competente in conformità al meccanismo di coerenza descritto dagli articoli 63 e successivi del GDPR. Secondo la procedura descritta, l'autorità di controllo comunica un progetto di decisione al Comitato europeo per la protezione dei dati, che emette un parere entro un termine di otto settimane – prorogabile di sei settimane, in caso di particolare complessità - a maggioranza semplice. L'autorità di controllo è chiamata a tenere in massima considerazione il parere del Comitato, e, nel caso in cui intenda modificare il progetto di decisione, è tenuta a darne comunicazione entro due settimane al presidente del Comitato.

In ogni caso, l'articolo 47 postula che le norme vincolanti d'impresa possano essere adottate a condizione che queste siano giuridicamente vincolanti e si applichino a tutti i membri interessati del gruppo imprenditoriale o del gruppo di imprese che

[/https://edpb.europa.eu/system/files/2021-05/edpb_guidelines_202002_art46guidelines_internationaltransferspublicbodies_v2_it.pdf](https://edpb.europa.eu/system/files/2021-05/edpb_guidelines_202002_art46guidelines_internationaltransferspublicbodies_v2_it.pdf).

⁴⁴⁶ Ibidem, par. 65-68.

⁴⁴⁷ Ibidem, par. 70-77.

⁴⁴⁸ Articolo 46, paragrafo 2, lett. b) GDPR.

svolgono un'attività economica comune, compresi i loro dipendenti, che conferiscano agli interessati diritti azionabili in relazione al trattamento dei loro dati personali e che rispettino un lungo elenco di requisiti puntualmente descritto al secondo paragrafo dello stesso articolo.

Le altre garanzie adeguate indicate dal secondo paragrafo del GDPR sono: le clausole contrattuali tipo (o standard) di protezione dei dati⁴⁴⁹ adottate dalla Commissione oppure quelle adottate da un'autorità di controllo e approvate dalla Commissione, un codice di condotta approvato a mente dell'articolo 40⁴⁵⁰ del GDPR o un meccanismo di certificazione approvato a norma dell'articolo 42⁴⁵¹, unitamente all'impegno vincolante ed esigibile da parte del titolare o del responsabile del trattamento nel paese terzo ad applicare le garanzie adeguate, anche con riferimento ai diritti dell'interessato. Da ultimo, il terzo paragrafo ritiene che rappresenti una garanzia adeguata la presenza di clausole contrattuali tra il titolare del trattamento o il

⁴⁴⁹ Si v. Commissione europea, Decisione di esecuzione (UE) 2021/914, relativa alle clausole contrattuali tipo per il trasferimento dei dati personali verso paesi terzi a norma del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, 4 giugno 2021. Con la decisione di esecuzione numero 914 del 2021, la Commissione europea ha stabilito che le clausole tipo allegate alla decisione rappresentano garanzie adeguate, ai sensi dell'articolo 46, par. 1, e par. 2, lett. c), del Regolamento (UE) 2016/679, ai fini del trasferimento di dati da un titolare o un responsabile del trattamento soggetto al Regolamento UE 2016/679 (esportatore) a un titolare o un (sub-)responsabile del trattamento rispetto al quale non trova applicazione il predetto Regolamento (importatore). La Commissione - che ha contestualmente abrogato, a far data dal 27 settembre 2021, le precedenti decisioni in materia (cfr. Decisione 2001/497/CE del 15 giugno 2001 e decisione 2010/87/UE del 5 febbraio 2010) - ha comunque previsto che per quanto concerne i contratti conclusi prima di tale data, essi rimanessero validi fino al 27 dicembre 2022, purché i trattamenti ivi indicati fossero rimasti invariati e il ricorso a tali clausole avesse garantito che un trasferimento di dati personali soggetto a garanzie adeguate.

La decisione è consultabile al link:

<https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32021D0914>.

⁴⁵⁰ I codici di condotta ex art. 40 del GDPR sono, a mente delle Linee guida 1/2019 del Comitato europeo della protezione dei dati sui codici di condotta e sugli organismi di monitoraggio di giugno 2019, «*strumenti di responsabilizzazione volontari che stabiliscono specifiche norme di protezione dei dati per categorie di titolari e di responsabili del trattamento. Essi possono essere un utile ed efficace strumento di responsabilizzazione in quanto forniscono una descrizione dettagliata dei comportamenti più appropriati, in termini giuridici ed etici, con riguardo a un determinato settore. Dal punto di vista della protezione dei dati, i codici possono quindi fungere da decalogo per i titolari e i responsabili del trattamento che progettano e svolgono attività di trattamento dei dati conformi al regolamento, conferendo un significato operativo ai principi di protezione dei dati stabiliti dalla legislazione europea e nazionale*».

Per un maggiore approfondimento, si v. European Data Protection Board, Linee guida 1/2019 sui codici di condotta e sugli organismi di monitoraggio a norma del GDPR, versione 2.0, 4 giugno 2019, consultabili al link:

https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201901_v2.0_codesofconduct_it.pdf.

⁴⁵¹ Per un approfondimento, si v. European Data Protection Board, Linee guida 1/2018 relative alla certificazione e all'identificazione di criteri di certificazione in conformità degli articoli 42 e 43 del regolamento (UE) 2016/679, versione 3.0, 4 giugno 2019, consultabile al link: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteri_a_annex2_it.pdf.

Si v. inoltre European Data Protection Board, Linee guida 7/2022 sulla certificazione come strumento per i trasferimenti, versione 2.0, 14 febbraio 2023, consultabile al link:

https://edpb.europa.eu/system/files/2023-05/edpb_guidelines_07-2022_on_certification_as_a_tool_for_transfers_v2_it_0.pdf.

responsabile del trattamento e il titolare del trattamento, il responsabile del trattamento o il destinatario dei dati personali nel paese terzo o nell'organizzazione internazionale, purché sia presente l'autorizzazione dell'autorità di controllo competente.

Il Comitato europeo per la protezione dei dati personali, nelle raccomandazioni di novembre 2020⁴⁵², indica con chiarezza i comportamenti che il titolare o il responsabile del trattamento è chiamato a mettere in atto quando debba effettuare un trasferimento transfrontaliero dei dati in un paese terzo non oggetto di una decisione di adeguatezza da parte della Commissione. Gli esportatori sono chiamati *in primis* a conoscere, attraverso una puntuale mappatura, i trasferimenti perpetrati, con particolare attenzione a verificare che i dati trasferiti siano adeguati, pertinenti e limitati con riferimento alle finalità per cui vengono trasferiti nel paese terzo.⁴⁵³ Quando il trasferimento avvenga sulla base dell'articolo 46, occorre valutare se vi siano disposizioni normative o prassi del paese terzo che possano incidere sull'efficacia delle garanzie adeguate degli strumenti di trasferimento su cui si fa affidamento. La valutazione deve concentrarsi principalmente sulla legislazione del paese terzo rilevante per il trasferimento e sullo strumento di trasferimento ai sensi dell'articolo 46 del GDPR su cui si fa affidamento e che potrebbe pregiudicare il livello di protezione.⁴⁵⁴

Se dall'analisi risulta che la legislazione del paese terzo incide sull'efficacia dello strumento di trasferimento, occorre individuare e adottare le misure supplementari necessarie per rendere il livello di protezione dei dati «*sostanzialmente equivalente*»⁴⁵⁵ a quello dell'UE. Sarà poi necessario adottare passaggi procedurali formali richiesti dall'adozione della misura supplementare, conducendo una vigilanza continua circa eventuali sviluppi che possano pregiudicare il livello di protezione dei dati personali.⁴⁵⁶

Nel caso in cui manchi una decisione di adeguatezza ai sensi dell'articolo 45, paragrafo 3, o una delle garanzie adeguate descritte dall'articolo 46, il GDPR ammette delle deroghe speciali a patto che si verifichi una delle condizioni previste dall'articolo 49. L'articolo 49 contiene una serie di eccezioni alle regole generali descritte dagli articoli 45 e 46, dunque è necessario che detto articolo sia interpretato in maniera restrittiva, come comprovato anche dal titolo dell'articolo 49, «*deroghe in specifiche situazioni*». Le suddette deroghe verranno analizzate con l'ausilio delle linee guida del

⁴⁵² European Data Protection Board, Raccomandazioni 1/2020 relative alle misure che integrano gli strumenti di trasferimento al fine di garantire il rispetto del livello di protezione dei dati personali dell'UE, 10 novembre 2020.

Consultabili al link:

https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_it.pdf.

⁴⁵³ Ibidem, par. 8-13.

⁴⁵⁴ Ibidem, p.3.

⁴⁵⁵ Si v. Corte di Giustizia dell'Unione europea, Sentenza della Corte (Grande Sezione), 16 luglio 2020, Data Protection Commissioner contro Facebook Ireland Limited e Maximilian Schrems, Causa C-311/18, consultabile al link:

<https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A62018CJ0311>.

⁴⁵⁶ European Data Protection Board, Raccomandazioni 1/2020 relative alle misure che integrano gli strumenti di trasferimento al fine di garantire il rispetto del livello di protezione dei dati personali dell'UE, par. 45-60.

Comitato europeo per la protezione di dati di maggio 2018 «sulle deroghe di cui all'articolo 49 del GDPR».⁴⁵⁷

La prima condizione al trasferimento prevista dall'articolo 49 è quella per cui «*l'interessato abbia esplicitamente acconsentito al trasferimento proposto, dopo essere stato informato dei possibili rischi di siffatti trasferimenti per l'interessato, dovuti alla mancanza di una decisione di adeguatezza e di garanzie adeguate*». Il consenso deve essere espresso in conformità a quanto previsto dall'articolo 4, paragrafo 11 e all'articolo 7 del GDPR. In realtà, la *littera legis* dell'articolo 49 richiede un *quid pluris*, dal momento che postula che il consenso, oltre ad essere una manifestazione di volontà libera, specifica, informata e inequivocabile sia anche «esplicito».

Il consenso deve essere «*specifico*» nel senso che deve essere specificamente prestato per il trasferimento dei dati. Proprio per questo, talvolta esso non può essere prestato contestualmente alla raccolta dei dati, poiché per il titolare o il responsabile è ancora non prospettabile l'idea di effettuare un trasferimento; ciò significa che colui che effettua il trasferimento dovrà accertare di raccogliere il consenso specifico prima di mettere in atto il trasferimento transfrontaliero, anche quando questo dovesse avvenire molto tempo dopo la raccolta dei dati coinvolti.⁴⁵⁸

La previsione che chiede che il consenso sia «*informato*» postula la necessità che l'interessato sia informato, anche mediante avviso standardizzato, anche dei rischi specifici derivanti dal trasferimento verso un paese terzo non rientrante in una delle situazioni di cui all'articolo 45 e 46.⁴⁵⁹

La seconda condizione riportata dall'articolo 49 ammette il trasferimento transfrontaliero quando questo «*sia necessario all'esecuzione di un contratto concluso tra l'interessato e il titolare del trattamento ovvero all'esecuzione di misure precontrattuali adottate su istanza dell'interessato*». Tale disposizione, a mente delle linee guida dell'EDPB, può essere congiuntamente alla terza condizione riportata dal GDPR (per cui è possibile il trasferimento transfrontaliero quando sia necessario per la conclusione o l'esecuzione di un contratto stipulato tra il titolare del trattamento e un'altra persona fisica o giuridica a favore dell'interessato), ed assieme al Considerando 111, che limita l'applicazione di queste condizioni alle situazioni di «necessità» - ovvero la presenza di un nesso stretto e significativo fra il trasferimento dei dati e la finalità del contratto - e «*occasionalità*», da valutare invece caso per caso.⁴⁶⁰

Ai sensi dell'articolo 49, paragrafo 1, lettera d), è inoltre possibile effettuare il trasferimento quando questo sia «*necessario per importanti motivi di interesse pubblico*», riconosciuto dal diritto dell'Unione o dal diritto dello Stato membro cui è soggetto il titolare del trattamento. Secondo l'EDBP, per valutare l'esistenza di un interesse pubblico, è possibile utilizzare come indizio l'esistenza di un accordo o di una convenzione internazionale che stabilisca un determinato obiettivo. A tale condizione, peraltro, non si applica la condizione dell'occasionalità, pertanto è possibile effettuare

⁴⁵⁷ European Data Protection Board, Linee guida 2/2018 sulle deroghe di cui all'articolo 49 del regolamento 2016/679, 25 maggio 2018, consultabili al link: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_it.pdf.

⁴⁵⁸ Ibidem, p. 7.

⁴⁵⁹ Ibidem.

⁴⁶⁰ Ibidem, p. 8-10.

trasferimenti sistematici e su larga scala, tuttavia, il Comitato raccomanda a tutti gli esportatori di cercare adeguate garanzie ai sensi dell'articolo 46 per evitare trasferimenti sistematici, in ossequio al carattere di eccezionalità delle condizioni previste dall'articolo 49.⁴⁶¹

La lettera e), ammette il trasferimento quando questo sia necessario per «*accertare, esercitare o difendere un diritto in sede giudiziaria*», purché sia, a mente del Considerando 111 «*occasionale e necessario in relazione a un contratto o un'azione legale, che sia in sede giudiziale, amministrativa o stragiudiziale, compresi i procedimenti dinanzi alle autorità di regolamentazione*».

In caso di emergenza medica, quando la disponibilità di dati personali si presenta quale necessaria e fondamentale per la prestazione di trattamenti sanitari, il trasferimento è reso possibile dalla lettera f), che prevede questa possibilità quando detto trasferimento sia «*necessario per tutelare gli interessi vitali dell'interessato o di altre persone, qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso*». Il trattamento deve essere necessario ai fini di una diagnosi essenziale, pertanto, sottolinea l'EDPB, non è applicabile tale circostanza nel caso di una ricerca medica. Il soggetto deve trovarsi in una situazione in cui la facoltà decisionale è compromessa da un'incapacità fisica, mentale o giuridica, oppure deve trattarsi di un minore la cui incapacità va dimostrata e attestata con certificato medico.⁴⁶²

L'ultima condizione in cui è possibile il trasferimento transfrontaliero, pur in assenza di una decisione di adeguatezza o di una garanzia adeguata si ha quando

«il trasferimento sia effettuato a partire da un registro che, a norma del diritto dell'Unione o degli Stati membri, mira a fornire informazioni al pubblico e può esser consultato tanto dal pubblico in generale quanto da chiunque sia in grado di dimostrare un legittimo interesse, solo a condizione che sussistano i requisiti per la consultazione previsti dal diritto dell'Unione o degli Stati membri».

L'EDPB chiarisce che tale registro può essere tanto in formato cartaceo quanto in formato elettronico, e deve essere finalizzato alla trasmissione di informazioni al pubblico (come, ad esempio, il registro delle imprese), pertanto i registri privati sono esclusi dall'ambito di applicazione di questa deroga.⁴⁶³

L'articolo 49 procede al secondo comma del primo paragrafo statuendo che, se non è possibile avere una decisione di adeguatezza ai sensi dell'articolo 45, delle garanzie adeguate ai sensi dell'articolo 46, e non si presenta una delle condizioni appena citate, in via di *extrema ratio*,

«il trasferimento verso un paese terzo o un'organizzazione internazionale è ammesso soltanto se non è ripetitivo, riguarda un numero limitato di interessati, è necessario per il perseguimento degli interessi legittimi cogenti del titolare del trattamento, su cui non prevalgono gli interessi o i diritti e le libertà dell'interessato, e qualora il titolare e del trattamento abbia valutato tutte le circostanze relative al trasferimento e sulla base di tale valutazione

⁴⁶¹ Ibidem, p. 11.

⁴⁶² Ibidem, p. 13-14.

⁴⁶³ Ibidem, p. 14-15.

abbia fornito garanzie adeguate relativamente alla protezione dei dati personali. Il titolare del trattamento informa del trasferimento l'autorità di controllo. In aggiunta alla fornitura di informazioni di cui agli articoli 13 e 14, il titolare del trattamento informa l'interessato del trasferimento e degli interessi legittimi cogenti perseguiti».

Tale norma rappresenta un importante elemento di novità rispetto alla direttiva 95/46/CE⁴⁶⁴, tuttavia l'ambito di applicazione è particolarmente ristretto e subordinato a un ricco apparato di condizioni previste dalla legge. Come ribadito dal Considerando 113, «*tali trasferimenti dovrebbero essere ammessi soltanto nei casi residui in cui nessuno degli altri presupposti per il trasferimento è applicabile*».

Ad esempio, non bastano meri interessi legittimi del titolare del trattamento, ma è necessario che questi siano «cogenti», ovvero essenziali per il titolare del trattamento, come, a titolo esemplificativo, nel caso in cui sia necessario per proteggere la propria organizzazione da un danno grave o immediato. Tali interessi legittimi del titolare devono peraltro superare un giudizio di bilanciamento con gli interessi, i diritti e le libertà dell'interessato, tenendo in considerazione tutti i rischi del trasferimento. L'esportatore dovrà comunque in ogni caso applicare misure supplementari per ridurre al minimo i rischi prospettati, da stabilire caso per caso.⁴⁶⁵

Il trasferimento non deve essere ripetitivo e deve riguardare un numero limitato di interessati, che nella pratica varia a seconda dei singoli casi.⁴⁶⁶

3.4.2 Il trasferimento negli Stati Uniti: il *Datagate*

Al fine di illustrare le criticità collegate al trattamento dei dati personali durante la didattica a distanza, si ritiene necessario descrivere l'evoluzione della disciplina del trasferimento transfrontaliero verso gli Stati Uniti. Prima di analizzare le decisioni di adeguatezza della Commissione e le sentenze della Corte di Giustizia dell'Unione europea, occorre gettare luce sulla tutela della privacy e dei dati personali in ambito statunitense e sullo scandalo del *datagate*, data la sua forte influenza sull'intera disciplina del trasferimento.

Una data spartiacque in materia di tutela della privacy negli Stati Uniti è l'11 settembre del 2001. Negli anni precedenti il tragico attentato alle World Trade Center, la Federal Trade Commission (FTC) aveva in realtà messo in atto una serie di iniziative finalizzate a una regolamentazione della privacy online, che, laddove fossero state effettivamente approvate, avrebbero probabilmente stroncato sul nascere il capitalismo della sorveglianza di Google.⁴⁶⁷

Tuttavia, dopo l'11 settembre, le esigenze di sicurezza fecero sì che tutte le perplessità legate alla privacy passassero in sordina.⁴⁶⁸ Peraltro, si segnala che questo generale clima di timore legato agli attentati terroristici rappresentò terreno fertile per

⁴⁶⁴ Ibidem, p. 15.

⁴⁶⁵ Ibidem.

⁴⁶⁶ Ibidem, p.16.

⁴⁶⁷ Così S. Zuboff, «Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri», p. 123 e ss.

⁴⁶⁸ Ibidem.

le lobby del mondo di internet intenzionate a bloccare ogni tipo di regolamentazione.⁴⁶⁹ Secondo Zuboff, l'11 settembre 2001 determinò la nascita di una vera e propria alleanza tra Governo statunitense e Google, dal momento che CIA e National Security Agency (NSA) – ma in realtà qualsiasi agenzia governativa che si occupasse di sicurezza interna – necessitavano dell'*expertise* di Google per lavorare con i dati non strutturati che avevano a disposizione. Nacque così un vero e proprio asse Pentagono – Silicon Valley, che – come già esaminato – minaccia tutt'ora la democrazia stessa.

In questa cornice di eventi si colloca lo scandalo *Datagate*: al centro ci sono le dichiarazioni dell'ormai celeberrimo Edward Snowden, impiegato presso un'azienda di tecnologia consulente della NSA, riguardanti operazioni di sorveglianza di massa perpetrate da quest'ultima e dalla CIA. Si comprendono le intenzioni del *whistleblower* dal celebre incipit del suo libro pubblicato nel 2019 – «*Errore di sistema*» – in cui afferma di aver lavorato per trent'anni per il governo, ma di aver scelto adesso di lavorare per le persone e di aver capito solo dopo tempo la differenza tra i due concetti.

Snowden, infatti, tra il 2012 e 2013 consegnò circa ventimila documenti top secret ai giornali *The Guardian* e *The Washington Post*, gettando luce sulla pervasiva attività di spionaggio a danno di cittadini americani e non, a partire dall'intercettazione del traffico telefonico e servendosi dell'ausilio di quelli che, qualche anno più tardi, Shoshana Zuboff chiamerà capitalisti della sorveglianza.

Snowden, ad esempio, nelle sue dichiarazioni del 2011, denunciava l'utilizzo del programma di sorveglianza «*PRISM*». Tale programma, nato come di massima segretezza, sarebbe in grado di ottenere dati afferenti, per esempio, alla posta elettronica, chat, videochat e foto, grazie alla collaborazione di *content* e *service provider* come Microsoft, Skype, Apple e altri. Dalle denunce di Snowden alle testate giornalistiche, molte sono state le inchieste finalizzate a conoscere il raggio effettivo di pervasività di programmi come PRISM.

Ciò che in questa sede preme particolarmente sottolineare, anche alla luce delle finalità del presente lavoro, è che tale attività di spionaggio di massa era comunque condotta non solo nei confronti dei cittadini americani, ma a danno potenzialmente dell'intera popolazione mondiale, anche grazie alla collaborazione di varie agenzie straniere.⁴⁷⁰

3.4.3 La decisione di adeguatezza *Safe Harbor* e la pronuncia *Schrems I*

Le dichiarazioni di Snowden gettano luce per la prima volta sui problemi di sorveglianza di massa e determinano una serie di conseguenze a livello europeo. In particolare, si deve al giovane attivista austriaco Maximilian Schrems l'attenzione verso le criticità legate al trasferimento dei dati personali negli Stati Uniti.

All'epoca della decisione della Corte di Giustizia del 2014, nota come decisione *Schrems I*, il trasferimento dei dati personali verso gli Stati Uniti avveniva grazie alla

⁴⁶⁹ Ibidem.

⁴⁷⁰ Si v. E. Snowden, «*Errore di sistema*», Milano, Longanesi, 2019.

decisione di adeguatezza denominata «*Safe Harbor*» (Decisione 520/2000/CE)⁴⁷¹. A mente di tale decisione, le organizzazioni che si fossero conformate ai «*Safe Harbor Privacy Principles*» avrebbero potuto beneficiare del trasferimento dei dati personali negli Stati Uniti registrandosi per la qualificazione di «approdo sicuro» in un apposito sito. Tramite la registrazione, le organizzazioni dichiaravano di rispettare i principi sanciti dall'Allegato I della decisione, vale a dire notifica, scelta, trasferimento successivo, sicurezza, integrità dei dati, accesso e garanzie dell'applicazione.

La decisione di un'organizzazione di qualificarsi per l'approdo sicuro era da considerarsi puramente volontaria, e le organizzazioni intenzionate ad aderire a tali principi erano chiamate a dichiarare pubblicamente il loro impegno in tal senso. Le organizzazioni erano libere di sviluppare proprie politiche in fatto di riservatezza dei dati personali, purché queste fossero conformi ai principi indicati. Il mancato rispetto dei principi era perseguibile in forza delle disposizioni contenute nella sezione 5 del Federal Trade Commission Act, che proibisce atti sleali e ingannevoli, oppure in forza di disposizioni analoghe che proibiscono tali atti. Il risultato era un sistema di presunzione di adeguatezza dell'organizzazione che dichiarasse di sottostare ai principi del Safe Harbor.

Dopo un'esperienza di studio presso la Santa Clara University, nel cuore della Silicon Valley, in cui ebbe occasione di conoscere la diversa prospettiva statunitense in materia di privacy grazie all'incontro con uno dei legali di Facebook,⁴⁷² Schrems fondava nel 2011 un gruppo di attivisti chiamato «*Europe v. Facebook*».⁴⁷³

Il 25 giugno 2013, Schrems cominciava la sua battaglia contro Facebook, presentando un reclamo presso l'autorità di controllo preposta alla protezione dei dati personali in Irlanda (il «Commissario»), Paese europeo in cui ancora oggi il social network californiano detiene uno stabilimento. Il reclamo conteneva una richiesta di vietare a Facebook Ireland il trasferimento negli Stati Uniti, ritenendo che l'ordinamento statunitense non offrisse un livello di protezione adeguato e coerente con la Direttiva 95/46/CE, anche alla luce delle rivelazioni di Snowden.

Dopo un primo rigetto da parte del Commissario, in cui si sottolineava la vincolatività della decisione Safe Harbor, la Corte d'Appello, innanzi cui Schrems ricorreva, riconosceva «*un serio dubbio*» circa l'adeguatezza della protezione dei dati personali da parte dell'ordinamento statunitense. Più nello specifico, dal momento che la Costituzione irlandese tutela il rispetto della vita privata e familiare e l'invulnerabilità del domicilio, essa implica che qualsiasi ingerenza in tali diritti sia proporzionata e conforme ai requisiti previsti dalla legge. Secondo la Corte d'Appello, «*l'accesso massiccio e indifferenziato a dati personali sarebbe manifestamente contrario al principio di proporzionalità e ai valori fondamentali protetti dalla costituzione irlandese*».⁴⁷⁴

⁴⁷¹ Commissione europea, Decisione 2000/520/CE, a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio sull'adeguatezza della protezione offerta dai principi di approdo sicuro, 26 luglio 2000, consultabile al link:

<https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32000D0520>.

⁴⁷² P. Guarda, G. Binoletto, «Diritto comparato della privacy e della protezione dei dati personali», p.135.

⁴⁷³ Il gruppo non è più attivo, si v. <http://www.europe-v-facebook.org/>.

⁴⁷⁴ Corte di Giustizia dell'Unione europea, Sentenza della Corte (Grande Sezione), 6 ottobre 2015, Maximilian Schrems contro Data Protection Commissioner, causa C-362/14, d'ora in avanti, Schrems I, par. 33, disponibile al link:

La Corte d'Appello riconosceva la rilevanza europea della questione:

*«il diritto al rispetto della vita privata, garantito dall'articolo 7 della Carta e dai valori fondamentali comuni alle tradizioni degli Stati membri, sarebbe svuotato di significato qualora i pubblici poteri fossero autorizzati ad accedere alle comunicazioni elettroniche su base casuale e generalizzata, senza alcuna giustificazione oggettiva fondata su motivi di sicurezza nazionale o di prevenzione della criminalità, specificamente riguardanti i singoli interessati, e senza che tali pratiche siano accompagnate da garanzie adeguate e verificabili».*⁴⁷⁵

Per tali motivi, la Corte d'Appello irlandese presentava un rinvio pregiudiziale alla Corte di Giustizia dell'Unione Europea, in particolar modo chiedendo se l'autorità nazionale preposta alla tutela dei dati personali fosse vincolata alla decisione di adeguatezza o se, al contrario, fosse per questa possibile condurre un'indagine propria circa il livello di protezione offerto dal paese terzo, sulla base dei principi sanciti dalla Carta dei diritti fondamentali dell'Unione Europea (anche "la Carta").⁴⁷⁶

Con la causa C-362/14 «*Maximillian Schrems v. Data Protection Commissioner*»⁴⁷⁷, la Corte di Giustizia invalidava la decisione di adeguatezza Safe Harbor. La Corte, dopo aver puntualmente sottolineato la centralità della tutela dei diritti fondamentali al rispetto della vita privata e alla tutela dei dati personali, spostava la sua analisi sui poteri di cui dispongono le autorità di controllo nazionali, così come disciplinati dall'articolo 28 della direttiva 95/46. Pur potendosi evincere che i poteri – investigativi e di intervento – riguardassero i trattamenti di dati personali effettuati nel territorio dello Stato membro, la Corte precisava che, in ogni caso, il trasferimento di dati personali andasse inteso come trattamento di dati personali ai sensi dell'articolo 2, lett. b) della direttiva 95/46. Tale ragionamento implica dunque che

*«poiché le autorità nazionali di controllo sono incaricate, ai sensi dell'articolo 8, paragrafo 3, della Carta e dell'articolo 28 della direttiva 95/46, di sorvegliare il rispetto delle norme dell'Unione relative alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, ciascuna di esse è quindi investita della competenza a verificare se un trasferimento di dati personali dal proprio Stato membro verso un paese terzo rispetti i requisiti fissati dalla direttiva 95/46».*⁴⁷⁸

<https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:62014CJ0362>.

⁴⁷⁵ Ibidem, par. 34.

⁴⁷⁶ «1) Se, nel decidere in merito a una denuncia presentata a un'autorità indipendente investita per legge delle funzioni di gestione e di applicazione della legislazione sulla protezione dei dati, secondo cui i dati personali sono trasferiti a un paese terzo (nel caso di specie, gli Stati Uniti d'America) il cui diritto e la cui prassi si sostiene non prevedano adeguate tutele per i soggetti interessati, tale autorità sia assolutamente vincolata dalla constatazione in senso contrario dell'Unione contenuta nella decisione 2000/520, tenuto conto degli articoli 7, 8 e 47 della Carta, nonostante le disposizioni dell'articolo 25, paragrafo 6, della direttiva 95/46.

2) Oppure, in alternativa, se detta autorità possa e/o debba condurre una propria indagine sulla questione alla luce degli sviluppi verificatisi nel frattempo, successivamente alla prima pubblicazione della decisione 2000/520».

⁴⁷⁷ Per una descrizione degli eventi, si v. par 25-36.

⁴⁷⁸ Schrems I, par. 47.

La Corte, riconoscendo che il compito di emanare una decisione di adeguatezza circa il livello di tutela dei dati personali offerto da parte di paesi terzi spettasse alla Commissione, escludeva che, fintantoché tale decisione non fosse stata dichiarata invalida dalla Corte, le autorità di controllo indipendenti, ma in generale gli Stati membri o i loro organi, potessero adottare misure contrarie a tale decisione. Ciò, tuttavia, non escludeva che le persone i cui dati personali fossero stati trasferiti in un paese terzo potessero investire le autorità di controllo di una domanda volta a conoscere la protezione dei diritti e libertà con riguardo al trattamento dei dati personali. Tale possibilità trovava infatti un preciso riferimento normativo all'articolo 28, paragrafo 4, che non riconosceva la presenza di una decisione di adeguatezza quale limite alla possibilità di presentare una domanda alle autorità nazionali di controllo. Le autorità nazionali di controllo dovevano quindi poter verificare, in piena indipendenza, se il trasferimento di tali dati rispettasse o meno i requisiti fissati dalla direttiva.⁴⁷⁹

I giudici di Lussemburgo sottolineavano la loro competenza esclusiva a dichiarare l'invalidità di un atto dell'Unione, come ad esempio una decisione della Commissione, dal momento che, trattandosi questa di un atto delle istituzioni europee, è soggetta al controllo della sua conformità ai Trattati e ai principi generali del diritto nonché ai diritti fondamentali.⁴⁸⁰

Invece, nel caso in cui una persona, i cui dati personali erano stati trasferiti verso un paese terzo nei confronti del quale esisteva una decisione di adeguatezza emanata dalla Commissione, avesse proposto una domanda all'autorità nazionale di controllo, quest'ultima sarebbe stata tenuta a esaminarla con tutta la diligenza richiesta e, nel caso in cui avesse ritenuto tale domanda infondata, il soggetto avrebbe comunque potuto impugnare detta decisione davanti ai giudici nazionali. Laddove questi avessero ritenuto uno o più elementi sollevati fondati, avrebbero dovuto sospendere la decisione e investire la Corte di un procedimento pregiudiziale. In ogni caso, l'ultima parola sarebbe spettata sempre alla Corte di Giustizia: veniva infatti detto che il legislatore era tenuto a prevedere mezzi di ricorso che consentissero all'autorità di far valere le censure ritenute fondate davanti ai giudici nazionali, affinché questi potessero operare un rinvio pregiudiziale.⁴⁸¹

Pronunciandosi sulla validità della decisione Safe Harbor, la Corte sottolineava che il significato di «*livello di protezione adeguato*» previsto dall'articolo 25 della direttiva non fosse da intendere come livello di protezione identico a quello dell'Unione, ma andasse piuttosto inquadrato nella necessità di verificare che il paese terzo offra un livello di protezione «*sostanzialmente equivalente*» a quello offerto dall'Unione in forza della direttiva, interpretata alla luce della Carta.⁴⁸² La Commissione, dopo aver verificato il livello di protezione offerto da un paese terzo tenendo presenti le condizioni di cui all'articolo 25, era inoltre chiamata a verificare periodicamente che il livello di protezione assicurato non fosse cambiato.

Dal momento che l'allegato I, quarto comma, della decisione 2000/520 disponeva che l'applicabilità dei principi Safe Harbor potesse essere limitata

⁴⁷⁹ Ibidem, par. 53-60.

⁴⁸⁰ Ibidem, par. 61.

⁴⁸¹ Ibidem, par. 63-65.

⁴⁸² Ibidem, par. 73-74.

«se ed in quanto necessario per soddisfare esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia [degli Stati Uniti]», nonché da «disposizioni legislative o regolamentari ovvero decisioni giurisdizionali quando tali fonti comportino obblighi contrastanti od autorizzazioni esplicite, purché nell'avvalersi di un'autorizzazione siffatta un'organizzazione possa dimostrare che il mancato rispetto dei principi da parte sua si limita a quanto strettamente necessario per soddisfare i legittimi interessi d'ordine superiore tutelati da detta autorizzazione»,⁴⁸³

la Corte riteneva che fosse in ultima istanza sancito il primato delle esigenze di sicurezza nazionale, interesse pubblico e amministrazione della giustizia sui principi posti a tutela dei dati personali. Erano pertanto possibili ingerenze nei diritti fondamentali delle persone i cui dati personali erano stati trasferiti dall'Unione verso gli Stati Uniti, che erano peraltro sprovviste di una tutela giuridica o giurisdizionale efficace.⁴⁸⁴

Secondo la Corte, l'ingerenza nei diritti fondamentali avrebbe dovuto prevedere regole chiare e precise, che permettessero di proteggere efficacemente i dati personali da eventuali abusi e usi illeciti, ed era inoltre necessario che le deroghe e le restrizioni alla tutela dei dati personali, qualificandosi quest'ultima come diritto fondamentale, operassero entro i limiti dello stretto necessario.⁴⁸⁵

La normativa in esame non era, secondo la Corte, limitata allo stretto necessario, perché autorizzava

«in maniera generale la conservazione di tutti i dati personali di tutte le persone i cui dati sono stati trasferiti dall'Unione verso gli Stati Uniti senza alcuna distinzione, limitazione o eccezione a seconda dell'obiettivo perseguito e senza che sia previsto alcun criterio oggettivo che permetta di delimitare l'accesso delle autorità pubbliche ai dati e il loro uso ulteriore a fini precisi, rigorosamente ristretti ed idonei a giustificare l'ingerenza che sia l'accesso sia l'utilizzazione di tali dati comporta».⁴⁸⁶

I giudici di Lussemburgo rilevavano così che gli Stati Uniti d'America non garantissero un livello di protezione adeguato in considerazione della loro legislazione nazionale e dei loro impegni internazionali.⁴⁸⁷

Per queste ragioni, la decisione Safe Harbor era da considerarsi invalida.⁴⁸⁸

3.4.4 La decisione Privacy Shield e Schrems II

L'indagine del Commissario irlandese rivelava che Facebook, già nelle more della decisione Schrems I, aveva iniziato a operare il trasferimento dei dati personali da

⁴⁸³ Ibidem, par. 84.

⁴⁸⁴ Ibidem, par. 85-86.

⁴⁸⁵ Ibidem par. 91-92.

⁴⁸⁶ Ibidem, par. 93.

⁴⁸⁷ Ibidem, par. 103.

⁴⁸⁸ Per un'analisi della decisione, si v. T. Schulz, «Schrems v. Data Protection Commissioner (C.J.E.U.)», *International Legal Materials*, 56(2), 2017, pp. 245-272. doi:10.1017/ilm.2017.8.

Facebook Ireland a Facebook Inc. nella Silicon Valley servendosi della base giuridica delle clausole contrattuali tipo, sicché nel 2015, dopo una nuova denuncia dell'austriaco all'autorità irlandese, la Corte d'Appello si rivolse nuovamente alla Corte di Giustizia dell'Unione europea con un nuovo rinvio pregiudiziale nei confronti della decisione 2010/87/UE⁴⁸⁹ in materia di clausole contrattuali tipo, dal momento che i dati personali continuavano ad essere alla mercé delle autorità statunitensi.

Il quadro si complicò per due eventi: l'emanazione, a opera della Commissione, della decisione 2016/1250, detta «Privacy Shield»⁴⁹⁰ e l'abrogazione della Direttiva 95/46/CE a seguito dell'emanazione del GDPR, la cui disciplina – precedentemente illustrata – assume rilievo ai fini della pronuncia C-311/18, nota oggi come Schrems II.⁴⁹¹

Prima di illustrare la pronuncia della Corte, occorre chiarire le peculiarità della nuova decisione di adeguatezza. Al centro della nuova decisione vi era l'impegno del governo statunitense a implementare un meccanismo di vigilanza, chiamato «*Mediatore dello scudo*», sulle ingerenze delle autorità pubbliche per motivi di sicurezza nazionale. Le società statunitensi che avessero aderito ai principi dello scudo⁴⁹² sarebbero state soggette a uno specifico accreditamento e inserimento in un apposito registro, permettendo il trasferimento. Pur presentandosi la possibilità di limitare il rispetto di tali principi per finalità di sicurezza nazionale, interesse pubblico e amministrazione della giustizia degli Stati Uniti, l'ambito di applicazione di tali limitazioni era maggiormente circoscritto grazie al controllo da parte del Mediatore dello scudo, chiamato a verificare le concrete finalità perseguite.⁴⁹³

Nella causa Schrems II vennero sottoposte alla Corte di Giustizia dell'Unione europea ben undici questioni pregiudiziali.⁴⁹⁴ Ai fini del presente lavoro, sono in primo luogo rilevanti le questioni numero sette e undici, con cui si interrogava la Corte di Giustizia circa la validità della decisione 2010/87/UE. Il giudice del rinvio poneva l'accento sul fatto che le clausole contrattuali tipo, avendo appunto valore contrattuale, non vincolassero le autorità del paese terzo, ma solo le parti che le avessero sottoscritte.

⁴⁸⁹ Commissione europea, Decisione 2010/87, relativa alle clausole contrattuali tipo per il trasferimento di dati personali e incaricati al trattamento stabiliti in paesi terzi a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio, 5 febbraio 2010. Si ricordi che la decisione 2010/87/UE è stata abrogata, con effetto a decorrere dal 27 settembre 2021, dalla decisione di esecuzione 2021/914/UE della Commissione europea.

⁴⁹⁰ Commissione europea, Decisione di esecuzione (UE) 2016/1250, a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio, sull'adeguatezza della protezione offerta dal regime dello scudo UE-USA per la privacy, 12 luglio 2016 (d'ora in avanti Privacy Shield), consultabile al link: <https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32016D1250>.

⁴⁹¹ Corte di Giustizia dell'Unione europea, Sentenza della Corte (Grande Sezione), 16 luglio 2020, Data Protection Commissioner contro Facebook Ireland Limited e Maximilian Schrems, Causa C-311/18, consultabile al link:

<https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A62018CJ0311>.

D'ora in avanti, Schrems II.

⁴⁹² Principio sull'informativa, principio sull'integrità dei dati e sulla limitazione della finalità, principio sulla scelta, principio sulla sicurezza, principio sull'accesso, principio su ricorso, controllo e responsabilità: si v. paragrafi 19-29 dell'introduzione al Privacy Shield.

⁴⁹³ Si v. par. 64-90 dell'introduzione al Privacy Shield.

⁴⁹⁴ Per un'analisi della decisione Schrems II, si v. S. Alistair, «Schrems II: Commission 0», 41, *Business Law Review*, Issue 6, 2019, pp.257-259. Si v. anche P. Guarda, G. Bincoletto, «Diritto comparato della privacy e della protezione dei dati personali», p.138 e ss.

La Corte, dopo un'approfondita analisi della decisione in materia di clausole contrattuali tipo, non riconosceva alcun elemento che potesse inficiare la validità. In ogni caso, la Corte statuiva la necessità di una valutazione caso per caso finalizzata a verificare la sussistenza di idonee garanzie.⁴⁹⁵

Con le questioni quarta, quinta, nona e decima, i giudici di Lussemburgo erano chiamati a pronunciarsi sulla validità della decisione di adeguatezza Privacy Shield. Anche in tale decisione, la previsione di una possibilità di limitazione all'adesione ai principi per soddisfare esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia rendeva possibile ingerenze nei diritti fondamentali delle persone i cui dati personali erano stati trasferiti verso gli Stati Uniti. Per tale ragione, la Corte dubitava che il diritto degli Stati Uniti garantisse effettivamente un livello di protezione adeguato richiesto dall'articolo 45 del GDPR, letto alla luce dei diritti fondamentali previsti dalla Carta.

La comunicazione dei dati personali a un'autorità pubblica costituisce di per sé, infatti, un'ingerenza nei diritti fondamentali, indipendentemente da ogni qualsivoglia eventuale uso ulteriore dei dati.⁴⁹⁶ Eventuali limitazioni all'esercizio dei diritti e delle libertà fondamentali devono, ai sensi dell'articolo 52 della Carta, essere previsti dalla legge, devono rispettare il contenuto essenziale di detti diritti e libertà e devono soddisfare il requisito di proporzionalità.⁴⁹⁷ Le ingerenze del caso di specie potevano (e possono ancora oggi) declinarsi in veri e propri programmi di sorveglianza tramite il software PRISM o in generale tramite le diverse modalità disciplinate da norme statunitensi, quali l'articolo 702 Foreign Intelligence Surveillance Act (FISA), la Presidential Policy Directive 28 ovvero l'Executive Order 12333. La Corte esaminava tali disposizioni normative e riteneva che queste non corrispondessero ai requisiti minimi connessi, nel diritto europeo, al principio di proporzionalità, non prevedendo un controllo giudiziario all'accesso ai dati o garanzie per i cittadini stranieri potenzialmente soggetti a tali programmi.⁴⁹⁸

Secondo la Corte, inoltre, l'ordinamento statunitense non prevedeva garanzie necessarie né una tutela giurisdizionale effettiva nei confronti delle ingerenze da parte del governo, non potendosi qualificare il Mediatore dello scudo quale un giudice indipendente e imparziale, così come previsto dall'articolo 47 della Carta. Il Mediatore descritto dal Privacy Shield era, infatti, «*designato dal Segretario di Stato e costituiva parte integrante del Dipartimento di Stato degli Stati Uniti*»,⁴⁹⁹ pertanto non era possibile individuare presenti garanzie sostanzialmente equivalenti a quelle previste dall'articolo 47 della Carta.

La guerra di Schrems contro Facebook conosceva dunque un'ulteriore vittoria in battaglia: anche la decisione Privacy Shield è stata dichiarata invalida nel 2020, peraltro senza un «*grace period*» ai titolari del trattamento, chiamati a modificare la base

⁴⁹⁵ Schrems II, par. 122-149.

⁴⁹⁶ Ibidem, par. 171.

⁴⁹⁷ Ibidem, par. 174.

⁴⁹⁸ Ibidem, par. 185.

⁴⁹⁹ Ibidem, par. 195.

giuridica per le attività di trasferimento all'indomani della pubblicazione della pronuncia.⁵⁰⁰

3.4.5 Il trasferimento verso gli Stati Uniti dopo la pronuncia Schrems II: la decisione di adeguatezza Data Privacy Framework

I giudici di Lussemburgo, nella pronuncia Schrems II, hanno invalidato la decisione «Privacy Shield», facendo tuttavia salva la decisione 2010/87/UE in materia di clausole contrattuali tipo. Tale decisione è stata recentemente abrogata a opera della decisione di esecuzione 2021/914 della Commissione europea. La novità principale di dette clausole è un approccio modulare – sono infatti previsti quattro moduli⁵⁰¹ – caratterizzato da una serie di disposizioni generali.

Dopo poche settimane dalla pronuncia Schrems II, l'associazione senza scopo di lucro Noyb aveva richiesto a ben trentatré aziende note per il trasferimento dei dati personali verso gli Stati Uniti quale fosse la base giuridica adottata per tale trasferimento in seguito all'invalidazione della decisione di adeguatezza.⁵⁰² A titolo di esempio, Google, Microsoft, Apple e Zoom avevano riportato l'intenzione di fare affidamento sulle clausole contrattuali tipo, mentre le piattaforme dell'universo *Meta* Facebook e Instagram si erano limitate a riportare riferimenti all'informativa sulla privacy, affermando che altre domande esulassero dal campo di applicazione del GDPR. Amazon, invece, non aveva fornito risposte univoche, mentre Coinbase rispondeva molto dettagliatamente, allegando copia delle clausole contrattuali tipo implementate.

Nel 2022, l'autorità garante irlandese, nell'ambito della procedura di cooperazione ai sensi dell'articolo 60 del GDPR, aveva condiviso con alcune autorità di controllo europee interessate il proprio progetto di decisione rispetto ad un'indagine circa il trasferimento dei dati personali al di fuori dello Spazio economico europeo effettuati da Meta sulla base di clausole contrattuali standard. In seguito a pareri discordanti delle autorità coinvolte, l'autorità garante irlandese aveva avviato la procedura di risoluzione delle controversie ai sensi dell'articolo 65, paragrafo 1, lettera a) del GDPR, con cui il Comitato europeo per la protezione dei dati viene chiamato a pronunciarsi con una decisione vincolante sulle controversie relative al trattamento dei dati transfrontaliero per garantire un'applicazione corretta e coerente del GDPR. L'autorità garante irlandese, in particolare, chiedeva all'EDPB di esaminare la legittimità del trasferimento dei dati personali verso gli Stati Uniti sulla base di clausole contrattuali effettuato da Meta. Il 12 maggio del 2023, l'autorità garante irlandese, sulla base della decisione vincolante dell'EDPB numero 1 del 2023⁵⁰³, ha sanzionato Meta, ai sensi degli

⁵⁰⁰ P. Guarda, G. Bincoletto, «Diritto comparato della privacy e della protezione dei dati personali», p. 145.

⁵⁰¹ 1) da titolare a titolare; 2) da titolare a responsabile; 3) da responsabile a responsabile; 4) da responsabile a titolare.

⁵⁰² Noyb, «Opening Pandora Box, how companies addressed our questions about their international data transfers after the CJEU's ruling in C-311/18 - Schrems II», 25 settembre 2020, Consultabile al link: https://noyb.eu/sites/default/files/2021-10/Replies_from_controllers_on_EU-US_transfers.pdf.

⁵⁰³ European Data Protection Board, binding decision 1/2023 on the dispute submitted by the Irish SA on data transfers by Meta Platforms Limited for its Facebook Services, 13 aprile 2023, consultabile al link: https://edpb.europa.eu/our-work-tools/consistency-findings/binding-decisions_it.

articoli 58 paragrafo 2, lettera i) del GDPR, per 1.2 miliardi di euro.⁵⁰⁴ Più nello specifico, l'autorità irlandese ha ritenuto che l'ordinamento statunitense non fornisca un livello di protezione sostanzialmente equivalente a quello europeo,⁵⁰⁵ dal momento che il colosso della Silicon Valley è soggetto alle leggi di sorveglianza statunitense.⁵⁰⁶ Inoltre, nella decisione si legge che le clausole contrattuali standard sono ritenute inadeguate a colmare tale divario nella tutela,⁵⁰⁷ e che Meta non ha in atto delle misure che possano compensare il livello di protezione dei dati personali inadeguato offerto dagli Stati Uniti.⁵⁰⁸ L'autorità irlandese ha inoltre ordinato, ai sensi dell'articolo 58, comma 2 lettera j) del GDPR, la sospensione del trasferimento dei dati personali.⁵⁰⁹

Nonostante l'ennesimo riconoscimento della pervasività delle leggi di sorveglianza statunitense, i negoziati finalizzati alla semplificazione del processo di trasferimento di dati personali dall'Europa agli Stati Uniti hanno conosciuto un importante punto di svolta già nel marzo 2022, quando il Presidente degli Stati Uniti Joe Biden e la Presidente della Commissione europea Ursula Von der Leyen hanno annunciato la volontà di ripristinare il flusso di dati dal vecchio al nuovo continente sulla base di una decisione di adeguatezza. Il Presidente Biden, in data 7 ottobre 2022, ha dunque emanato l'Executive Order (EO) 14086⁵¹⁰ in attuazione dell'accordo con la Presidente della Commissione.

L'EO si apre con una dichiarazione di intenti da parte di Biden di limitare l'attività di intelligence al fine di garantire una maggiore attenzione al rispetto della dignità della persona. Il testo recita infatti:

*«Gli Stati Uniti riconoscono che le attività di intelligence devono tenere conto del fatto che tutte le persone dovrebbero essere trattate con dignità e rispetto, indipendentemente dalla loro nazionalità e ovunque risiedano, e che tutte le persone hanno legittimi interessi alla privacy nella gestione delle loro informazioni personali. Pertanto, questo ordine stabilisce salvaguardie per tali attività di intelligence basate sulla raccolta dei dati».*⁵¹¹

⁵⁰⁴ Data Protection Commission irlandese, Decision of the Data Protection Commission made pursuant to Section 111 of the Data Protection Act, 2018 and Articles 60 and 65 of the General Data Protection Regulation, 12 maggio 2023, consultabile al link: https://edpb.europa.eu/system/files/2023-05/final_for_issue_ov_transfers_decision_12-05-23.pdf, si v. par. 10.3.

⁵⁰⁵ Si v. par. 7.46 e ss.

⁵⁰⁶ Si v. par. 7.51 e ss.

⁵⁰⁷ Si v. par. 7.155 e ss.

⁵⁰⁸ Si v. par. 7.175 e ss.

⁵⁰⁹ Si v. par. 10.3, 10.4: «*Timeline for compliance with the suspension order*»: «*For the purpose of this Section 10, "the Commencement Date" shall be understood as meaning the date corresponding to the later in time of the following events: (i) the date on which the period allowed for an appeal against this Decision under Section 150 of the 2018 Act expires; and (ii) the date on which the period allowed for the bringing of an application for annulment of the Article 65 Decision under Article 243 TFEU expires*»; si v. anche par. 10.5: «*The Suspension Order will take effect on a date 12 (twelve) weeks from the Commencement Date*».

⁵¹⁰ Presidente degli Stati Uniti d'America, Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities, 7 ottobre 2022, consultabile al link: <https://www.whitehouse.gov/briefing-room/presidential-actions/2022/10/07/executive-order-on-enhancing-safeguards-for-united-states-signals-intelligence-activities/>.

⁵¹¹ Traduzione dell'Autorità Garante per la protezione dei dati personali.

Di primo acchito, l'EO sembrerebbe far propri i concetti chiave della disciplina europea in materia di protezione dei dati personali: figurano infatti, ad esempio, richiami ai principi di minimizzazione e liceità del trattamento dei dati personali.⁵¹²

L'EO permette lo svolgimento di attività di intelligence solamente per dodici obiettivi legittimi,⁵¹³ con un espresso riferimento alla necessità del rispetto dei requisiti di necessità e proporzionalità, esortando le agenzie di intelligence ad adattare le loro operazioni, tenendo conto della possibilità di utilizzare fonti meno invasive.⁵¹⁴

Il 13 dicembre del 2022, sulla base dell'EO, è stata pubblicata dalla Commissione europea una bozza di una nuova decisione di adeguatezza, denominata «*Data Privacy Framework*».⁵¹⁵

Due mesi dopo, il 14 febbraio 2023, il Parlamento europeo ha pubblicato un parere, chiamato «*Draft motion for a resolution*»,⁵¹⁶ in cui ha escluso che il livello di protezione dei dati personali offerto dagli Stati Uniti fosse sufficiente, esortando la Commissione a non adottare la decisione di adeguatezza.

Il Parlamento, pur riconoscendo gli sforzi dell'EO nel limitare le attività di intelligence in ossequio ai principi di proporzionalità e necessità, ha sottolineato che tali principi, così come espressi nell'EO, non sono in linea con la definizione del diritto dell'UE e la loro interpretazione da parte della Corte di Giustizia.⁵¹⁷

Le altre criticità sollevate riguardano, *ex multis*, la mancanza di una legge federale sulla protezione dei dati personali, la possibilità che l'EO venga in qualsiasi momento emendato dal Presidente e l'inapplicabilità di quest'ultimo al Cloud Act o al Patriot Act.

Dopo due settimane, il 28 febbraio del 2023, l'EDPB ha pubblicato il parere 5/2023 sul *Data Privacy Framework*⁵¹⁸. L'EDPB ha rilevato che alcuni dei principi sanciti dalla nuova bozza di decisione di adeguatezza sono corrispondenti a principi già enunciati dal Privacy Shield, pertanto permangono le precedenti perplessità.⁵¹⁹ Pur riconoscendo i passi in avanti compiuti dalle novità introdotte nell'EO (in particolare, si sottolinea che il sistema di ricorso giudiziario offra più garanzie della precedente figura del Mediatore

⁵¹² G. Scorza, «Executive order di Biden, ecco i punti critici, quelli positivi e quelli da chiarire», Autorità Garante per la protezione dei dati personali per Agenda Digitale, 10 ottobre 2022, consultabile al link: <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9813161>.

⁵¹³ Presidente degli Stati Uniti d'America, Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities, Section I b(i)(A)(11).

⁵¹⁴ Ibidem, Section II c(i)(A) e (B).

⁵¹⁵ Commissione europea, pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under EU-US Data Privacy Framework, consultabile al link:

[/https://commission.europa.eu/system/files/2022/12/Draft%20adequacy%20decision%20on%20EU-US%20Data%20Privacy%20Framework_0.pdf](https://commission.europa.eu/system/files/2022/12/Draft%20adequacy%20decision%20on%20EU-US%20Data%20Privacy%20Framework_0.pdf).

⁵¹⁶ Parlamento europeo, Draft motion for a resolution to wind up the debate on the statement by the Commission, pursuant to rule 132(2) of the Rules of Procedure on the adequacy of the protection afforded by the EU-US Data Privacy Framework, 2023/2501(RSP), consultabile al link:

https://www.europarl.europa.eu/doceo/document/LIBE-RD-740749_EN.pdf.

⁵¹⁷ Si v. lett. j, par. 2 del parere.

⁵¹⁸ European Data Protection Board, Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-UE Data Privacy Framework, 28 Febbraio 2023, consultabili al link:

https://edpb.europa.eu/system/files/2023-02/edpb_opinion52023_eu-us_dpf_en.pdf.

⁵¹⁹ Si v. par. 12 del parere.

dello scudo),⁵²⁰ l'EDPB ha riconosciuto alcuni punti di criticità che emergono da una lettura olistica dell'intera disciplina.

Il sistema di ricorso giudiziario ha destato alcune perplessità per quanto riguarda l'inappellabilità della notifica al querelante che neghi l'esistenza di violazioni, esortando dunque la Commissione a monitorare nello specifico tale meccanismo.⁵²¹

Inoltre, l'EDPB ha ritenuto necessari ulteriori chiarimenti circa la possibilità, a opera delle autorità statunitensi, di effettuare una raccolta temporanea di dati in blocco, dal momento che tali raccolte di dati in massa non prevedono né l'obbligo di autorizzazione preventiva da parte di un'autorità indipendente, né una revisione *ex post* da parte di un tribunale o di un organo equivalente indipendente.⁵²²

Nonostante le criticità segnalate e la Risoluzione non vincolante del Parlamento Europeo contraria all'adozione del DPF⁵²³, il 10 luglio 2023 la Commissione europea ha emanato la decisione di adeguatezza Data Privacy Framework.⁵²⁴ La Commissione ribadisce infatti la possibilità che il trasferimento avvenga nei confronti di un paese terzo

⁵²⁰ Ibidem, par. 34.

⁵²¹ Ibidem, p. 5: «*the EDPB is nevertheless concerned about the general application of the standard response of the DPRC notifying the complainant that either no covered violations were identified or a determination requiring appropriate remediation was issued, and its non-appealability, taken together*».

⁵²² Ibidem, «*As a deficit in the current framework, the EDPB has in particular identified that the U.S. legal framework, when allowing for the collection of bulk data under Executive Order 12333, lacks the requirement of prior 116mericana116ion by an independent authority, as required in the most recent jurisprudence of the EctHR, nor does it provide for a systematic independent review ex post by a court or an equivalently independent body*».

⁵²³ Si v. Parlamento europeo, Risoluzione dell'11 maggio 2023 sull'adeguatezza della protezione offerta dal UE-U.S. Data Privacy Framework, 11 maggio 2023, consultabile al link: https://www.europarl.europa.eu/doceo/document/TA-9-2023-0204_IT.html.

In particolare, «*osserva che i principi del quadro in materia di privacy dei dati del Dipartimento del commercio degli Stati Uniti non hanno subito modifiche sufficienti, rispetto a quelle previste dallo scudo per la privacy, al fine di fornire una protezione sostanzialmente equivalente a quella prevista dal RGPD;(...)*osserva che, mentre gli Stati Uniti stanno assumendo un impegno importante per migliorare l'accesso ai mezzi di ricorso e alle norme sul trattamento dei dati da parte delle autorità pubbliche, la comunità dell'intelligence statunitense ha tempo fino a ottobre 2023 per aggiornare le proprie politiche e pratiche in linea con l'impegno dell'ordinanza esecutiva n. 14086, e che l'Advocate General degli Stati Uniti non ha ancora definito l'UE e i suoi Stati membri come paesi che soddisfano i requisiti per poter accedere ai mezzi di ricorso disponibili dinanzi al Tribunale; sottolinea che ciò significa che la Commissione non è stata in grado di valutare "in pratica" l'efficacia dei mezzi di ricorso delle misure proposti in materia di accesso ai dati; conclude, pertanto, che la Commissione può solamente procedere con la fase successiva di una decisione di adeguatezza una volta che tali scadenze e obiettivi fondamentali siano soddisfatti dagli Stati Uniti per garantire che gli impegni siano rispettati nella pratica;(...) conclude che il quadro UE-USA in materia di privacy dei dati non crea un'equivalenza essenziale del livello di protezione; invita la Commissione a proseguire i negoziati con le sue controparti statunitensi al fine di creare un meccanismo che garantisca tale equivalenza, nonché l'adeguato livello di protezione richiesto dal diritto dell'Unione in materia di protezione dei dati e dalla Carta secondo l'interpretazione della CGUE; invita la Commissione a non adottare la decisione di adeguatezza fino a quando non saranno pienamente attuate tutte le raccomandazioni formulate nella presente risoluzione e nel parere del comitato europeo per la protezione dei dati».

⁵²⁴ Commissione europea, implementing decision of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the UE-UE Data Privacy Framework, 10 luglio 2023, consultabile al link: https://commission.europa.eu/system/files/2023-07/Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework_en.pdf.

il cui livello di protezione dei dati personali sia assimilabile, ma non identico, a quello europeo.

Analizzando il quadro normativo statunitense, in particolare l'EO 14086, la Commissione afferma che gli Stati Uniti assicurano un livello adeguato di protezione dei dati. Tale decisione di adeguatezza prevede, al pari del Safe Harbor e del Privacy Shield, un sistema di certificazione, per cui i titolari e i responsabili del trattamento potranno autocertificare la loro adesione a una serie di principi al fine di poter ricevere e trattare i dati provenienti dall'UE.⁵²⁵ Solo una volta che l'organizzazione intenzionata a certificarsi abbia adempiuto tutti gli obblighi previsti dalla decisione sarà possibile effettuare il trasferimento, inoltre la Federal Trade Commission renderà disponibile una lista, denominata «Data Privacy Framework List», in cui saranno riportate le organizzazioni che decideranno di adeguarsi alle prescrizioni previste dal DPF.⁵²⁶ Le organizzazioni sono chiamate a ripresentare annualmente una richiesta di certificazione al DPF, e la FTC avrà dunque inoltre il compito di rimuovere dalla lista sia le organizzazioni che non procederanno al meccanismo di ricertificazione annuale, sia quelle che «*have persistently failed to comply with the Principles*». Per queste ultime è preclusa la possibilità di beneficiare nuovamente della decisione DPF, sicché saranno chiamate a restituire o eliminare i dati ricevuti nell'ambito del DPF e saranno inserite in un'apposita lista mantenuta dalla FTC.⁵²⁷ Questo meccanismo di autocertificazione risulta pertanto invariato rispetto alla formulazione del Privacy Shield.⁵²⁸

I principi a cui le organizzazioni sono chiamate ad aderire per poter procedere al meccanismo di autocertificazione sono descritti dall'allegato I alla decisione, dove sono allegati i sette «principi originali»⁵²⁹, ovvero: i) notice; ii) choice; iii) accountability for onward transfer; iv) security; v) data integrity and purpose limitation; vi) access, vii) recourse, enforcement and liability. La formulazione di molti di questi principi è molto simile a quella contenuta nel Privacy Shield, ma sono presenti riferimenti espressi alle norme del GDPR rilevanti, rendendo dunque tale formulazione generalmente più

⁵²⁵ M. Giacalone, «Verso Schrems III? Analisi del nuovo EU-US Data Privacy Framework», European papers, quaderni europei, 14 giugno 2023, consultabile al link: <https://www.europeanpapers.eu/en/europeanforum/verso-schrems-iii-analisi-nuovo-eu-us-data-privacy-framework->

⁵²⁶ A. Titone, «EU-US. Data Privacy Framework: è (finalmente) realtà!», Medialaws, 2023, consultabile al link: <https://www.medialaws.eu/eu-u-s-data-privacy-framework-e-finalmente-realta/>, cfr. Considerando 52.

⁵²⁷ Ibidem.

⁵²⁸ L. Drechsler, A. Elbi, E. Kindt, E. Kun, J. Meszaros, K. Vranckaert, «Third Time Is the Charm? The Draft Data Privacy Framework for International Personal Data Transfers From the European Union to the United States», CiTiP Working Paper, giugno 2023, p. 20. <http://dx.doi.org/10.2139/ssrn.4477120>.

⁵²⁹ Ibidem, p. 9.

ampia.⁵³⁰ Accanto a questi principi la decisione riporta quindici principi supplementari⁵³¹, rimasti invariati rispetto al Privacy Shield, salvo per alcuni minori aggiornamenti.⁵³²

Ai sensi del Considerando 5 dell'allegato I, il rispetto di tali principi può essere limitato dalla normativa statunitense:

«(a) to the extent necessary to comply with a court order or meet public interest, law enforcement, or national security requirements, including where statute or government regulation create conflicting obligations; (b) by statute, court order, or government regulation that creates explicit authorizations, provided that, in exercising any such authorization, an organization can demonstrate that its non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorization; or (c) if the effect of the GDPR is to allow exceptions or derogations, under the conditions set out therein, provided such exceptions or derogations are applied in comparable contexts».

Il DPF si concentra soprattutto sull'analisi della possibilità di accesso ai dati per finalità di sicurezza nazionale, che viene descritta in maniera più completa rispetto alla formulazione del Privacy Shield.⁵³³ In generale, è possibile affermare che il maggiore cambiamento rispetto alla disciplina del Privacy Shield si legge nell'intenzione di fornire un apparato di norme più completo in materia di limitazioni all'accesso ai dati da parte del governo statunitense.⁵³⁴

A mente dell'EO, il US Foreign Intelligence Surveillance Court (FISC), tribunale indipendente e istituito per legge, sorveglia la raccolta di informazioni sulle comunicazioni elettroniche secondo la Sezione 702 del Foreign Intelligence Surveillance Act, mentre il Privacy and Civil Liberties Oversight Board si occupa di mantenere un equilibrio tra gli sforzi del governo federale per prevenire il terrorismo e la protezione della privacy e degli altri diritti fondamentali, svolgendo un ruolo di supervisore per quanto riguarda l'attuazione dell'EO 14086.⁵³⁵ Nonostante l'indipendenza di questi organi, desta particolare preoccupazione la previsione di meccanismi di sorveglianza interna da parte di funzionari legali, di controllo e di conformità appartenenti all'intelligence stessa, dunque difficilmente considerabili indipendenti.⁵³⁶

Inoltre, viene istituito un sistema di ricorso giudiziario a doppio livello per i cittadini europei: un Civil Liberties Protection Officer (CLPO) le cui decisioni sono impugnabili davanti alla Data Protection Review Court (DPRC), composta da tre giudici.

⁵³⁰ Ibidem.

⁵³¹ i) sensitive data; ii) journalistic exceptions; iii) secondary liability; iv) performing due diligence and conducting audits; v) the role of data protection authorities; vi) self-certification; vii) verification; viii) access; ix) human resources data; x) obligatory contracts for onward transfers; xi) dispute resolution and enforcement; xii) choice – timing of opt out; xiii) travel information; xiv) pharmaceutical and medical products; xv) public record and publicly available information.

⁵³² L. Drechsler, A. Elbi, E. Kindt, E. Kun, J. Meszaros, K. Vranckaert, «Third Time Is the Charm? The Draft Data Privacy Framework for International Personal Data Transfers From the European Union to the United States», p. 15.

⁵³³ Ibidem, p. 16.

⁵³⁴ Ibidem, p. 20.

⁵³⁵ Ibidem, p. 32.

⁵³⁶ Ibidem.

Se da un lato la garanzia dell'inamovibilità dei componenti sembra avvicinare queste autorità alle autorità indipendenti europee, dall'altro non si può non sottolineare che il CLPO è nominato dal Direttore dell'Intelligence Nazionale e il DPRC da un organismo del governo: desta dunque sospetto la compatibilità di detta previsione con il principio di indipendenza del giudice.⁵³⁷ In via di rimedio residuale, è infine prevista per il cittadino europeo la possibilità invocare la procedura di arbitrato vincolante condotta dall' «EU-U.S. Data Privacy Framework Panel», composto da almeno dieci arbitri scelti dal Dipartimento del Commercio e dalla Commissione.⁵³⁸

Per le criticità descritte e evidenziate dall'EDPB e dal Parlamento europeo, non mancano voci in dottrina che escludono che il nuovo EO doti la legislazione statunitense di un livello di tutela dei dati personali sostanzialmente equivalente a quello previsto dal GDPR.⁵³⁹ In particolare, sebbene l'EO insista sulla necessità che l'eventuale disapplicazione dell'accordo per esigenze di sicurezza nazionale avvenga esclusivamente in ossequio ai principi di proporzionalità e necessità, si dubita che tale disposizione sia coerente con la lettura da parte dei giudici di Lussemburgo dell'articolo 52 della Carta, per cui l'esercizio dei diritti e delle libertà possono essere limitati solamente da una legge che preveda tali limitazioni in modo chiaro, preciso e prevedibile, rispettando il loro contenuto essenziale.⁵⁴⁰ Nell'EO, infatti, gli obiettivi legittimi che permettono le attività di intelligence sono formulati in maniera generica e, peraltro, non sono soggetti ad un'interpretazione prevedibile, dal momento che permangono in capo al Presidente degli Stati Uniti la possibilità di modificarli in caso di minaccia nazionale.⁵⁴¹ Si guarda inoltre con criticità la scelta dello strumento normativo effettuata: l'executive order non ha rango legislativo, sicché non interviene sulle altre leggi che garantiscono una pervasiva attività di sorveglianza di massa⁵⁴², già censurate dalla Corte di Giustizia.⁵⁴³ Peraltro, il giudici di Lussemburgo hanno chiarito nella sentenza Schrems I che il fatto stesso che una normativa consenta all'autorità pubblica di accedere in modo generalizzato al contenuto delle comunicazioni elettroniche compromette l'essenza del diritto fondamentale al rispetto della vita privata.⁵⁴⁴ Dal momento che l'EO permette, in determinate circostanze, la raccolta in massa di dati personali, ci si chiede come questo possa garantire la sostanziale equivalenza rispetto al diritto europeo.⁵⁴⁵

In ogni caso, sarà senza dubbio interessante assistere ai prossimi sviluppi, in particolare, non è chiaro come l'approvazione di una nuova decisione di adeguatezza

⁵³⁷ G. Scorza, «Executive order di Biden, ecco i punti critici, quelli positivi e quelli da chiarire».

⁵³⁸ Commissione europea, implementing decision of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the UE-UE Data Privacy Framework, si v. par. 65-86.

⁵³⁹ Si v. L. Drechsler, A. Elbi, E. Kindt, E. Kun, J. Meszaros, K. Vranckaert, «Third Time Is the Charm? The Draft Data Privacy Framework for International Personal Data Transfers From the European Union to the United States».

⁵⁴⁰ M. Giacalone, «Verso Schrems III? Analisi del nuovo EU-US Data Privacy Framework».

⁵⁴¹ Ibidem.

⁵⁴² G. Scorza, «Executive order di Biden, ecco i punti critici, quelli positivi e quelli da chiarire».

⁵⁴³ M. Giacalone, «Verso Schrems III? Analisi del nuovo EU-US Data Privacy Framework».

⁵⁴⁴ Si v. Schrems I, par. 94-95.

⁵⁴⁵ Si v. M. Giacalone, «Verso Schrems III? Analisi del nuovo EU-US Data Privacy Framework».

possa coordinarsi con la decisione della autorità garante irlandese contro Meta prima descritta.⁵⁴⁶

3.4.6 Il trasferimento dei dati personali della didattica a distanza dopo Schrems II

In Italia, durante il mese di settembre 2020, a poche settimane dalla data del 16 luglio, in cui la Corte di Giustizia dell'Unione europea invalidava la decisione di adeguatezza Privacy Shield, le esigenze di contenimento del virus determinavano una ripresa delle attività didattiche per l'anno scolastico 2020-21 ancora caratterizzata dall'ausilio delle piattaforme, verso una nuova didattica digitale definita «integrata» o «*blended*»⁵⁴⁷, ovvero caratterizzata da una commistione tra didattica tradizionale e strumenti tecnologici.⁵⁴⁸

Le piattaforme dell'*emergency remote teaching*, non potendo più trasferire i dati personali negli Stati Uniti sulla base di una decisione di adeguatezza, hanno dovuto cercare una nuova base giuridica del trattamento tra quelle previste dagli articoli 46 e 29 del GDPR.

Lo strumento preferibile, ovvero le clausole contrattuali, si dimostrava tuttavia inidoneo a permettere il trasferimento di dati personali verso gli Stati Uniti nel contesto della didattica a distanza. Infatti, qualificandosi questi strumenti come contratti, essi vincolano solamente le parti e dunque non precludono a eventuali soggetti terzi, come le autorità statali, di accedere a tali dati. Da ciò derivava la necessità che l'Università o l'istituto scolastico, in forza del suo ruolo di titolare del trattamento, operassero delle valutazioni caso per caso per verificare la sussistenza di idonee garanzie circa il livello di protezione dei dati personali offerto nel paese terzo. Tali valutazioni e verifiche si declinano, tuttavia, quali troppo onerose in termini di tempo e denaro per il mondo dell'istruzione.⁵⁴⁹

Le norme vincolanti di impresa (articolo 46, lettera b) GDPR), che spesso riguardano grandi aziende e società, non erano compatibili con il mondo della didattica a distanza, dove l'utilizzo di piattaforme di piccole società quasi sconosciute (come Jitsi e Discord) è rapidamente incrementato durante la pandemia.⁵⁵⁰

Anche il trasferimento dei dati personali sulla base di codici di condotta o meccanismi di certificazione (articolo 46, lettere e) e f) GDPR) richiede che il titolare o il responsabile del trattamento implementino misure di sicurezza appropriate, dunque la vaghezza di tale disposizione non si coordinava con l'universo ERT.⁵⁵¹

⁵⁴⁶ A. Titone, «EU-US. Data Privacy Framework: è (finalmente) realtà!».

⁵⁴⁷ Si v. il Decreto del Ministero dell'Istruzione n.89 del 7 agosto 2020, consultabile al link:

<https://www.miur.gov.it/-/scuola-pubblicate-le-linee-guida-per-la-didattica-digitale-integrata>

⁵⁴⁸ Per un approfondimento, si v. M.B. Ligorio, S. Cacciamani, D. Cesareni, «Didattica blended. Teorie, metodi ed esperienze», Milano, Mondadori Education, 2022.

Per una lettura critica, si v. V. Pinto, «Didattica blended: una tappa verso l'università delle piattaforme?», Roars, 24 giugno 2020, al link: <https://www.roars.it/didattica-blended-una-tappa-verso-luniversita-delle-piattaforme/>.

⁵⁴⁹ C. Angiolini, R. Ducato, A. Giannopoulou, G. Schneider, «Remote Teaching During the Emergency and Beyond: Four Open Privacy and Data Protection Issues of 'Platformised' Education», p. 59.

⁵⁵⁰ Ibidem.

⁵⁵¹ Ibidem, p.60.

Tra le condizioni descritte dall'articolo 49 del GDPR, in materia di didattica a distanza, sarebbero state potenzialmente idonee a permettere il trasferimento dei dati personali verso gli Stati Uniti il consenso esplicito dell'interessato ai sensi della lettera a) dello stesso articolo, tuttavia, i titolari del trattamento avrebbero dovuto, a mente della stessa disposizione, prioritariamente informare gli interessati dei possibili rischi derivanti dal trasferimento dei dati personali in paesi sprovvisti di una decisione di adeguatezza o garanzie adeguate. Ciò avrebbe provocato, probabilmente, numerose richieste di cancellazione dei dati raccolti da parte degli utenti.⁵⁵²

Il trasferimento sarebbe potuto anche avvenire perché necessario per l'esecuzione di un contratto ai sensi della lettera b) dell'articolo 49, tuttavia, come già illustrato, detto trasferimento avrebbe dovuto essere occasionale e obiettivamente necessario e le piattaforme utilizzate per la DaD avrebbero dovuto dare prova del rispetto di tali requisiti.⁵⁵³ In generale, tali deroghe, in conformità alla loro natura, vanno interpretate in senso restrittivo, onde evitare che sia persa la loro natura di eccezionalità.⁵⁵⁴

Si comprendono dunque le difficoltà che gli istituti scolastici e universitari erano chiamati a fronteggiare: in qualità di titolari del trattamento dovevano selezionare responsabili del trattamento che presentassero garanzie sufficienti idonee a dimostrare che il trattamento fosse in linea con i requisiti del GDPR e che garantisse la tutela dei diritti dell'interessato (articolo 28). Ciò significa che le scuole e le università avrebbero dovuto conoscere la struttura organizzativa della piattaforma, con particolare attenzione alla base giuridica che permetteva il trasferimento dei dati personali fuori dall'UE e alla finalità del trattamento.⁵⁵⁵

Dopo Schrems II, i titolari del trattamento del mondo dell'istruzione erano stati dunque chiamati a rinegoziare i termini contrattuali con le piattaforme. Ad oggi, questo problema può ritenersi superato in forza della decisione di adeguatezza DPF, tuttavia Noyb, l'associazione di Maximilian Schrems, ha già annunciato l'intenzione di presentare ricorso contro questa decisione.⁵⁵⁶ Alla luce dunque del potenziale rischio di annullamento di questa decisione o di decisioni future, onde evitare il ripresentarsi delle criticità appena descritte, si ritiene necessario armare il mondo dell'istruzione di un maggiore potere contrattuale: ad esempio, una soluzione prospettabile potrebbe essere l'implementazione di associazioni di Università per gestire e regolamentare collettivamente il trasferimento dei dati personali, oppure si potrebbe incoraggiare un

⁵⁵² Ibidem.

⁵⁵³ Ibidem.

⁵⁵⁴ European Data Protection Board, Initial Legal Assessment of the Impact of the US Cloud Act on the EU Legal Framework for the Protection of Personal Data and the Negotiations of an EU-US Agreement on Close Border Access to Electronic Evidence, luglio 2019, consultabile al link: https://edpb.europa.eu/sites/default/files/files/file2/edpb_edps_joint_response_us_cloudact_annex.pdf.

⁵⁵⁵ C. Angiolini, R. Ducato, A. Giannopoulou, G. Schneider, «Remote Teaching During the Emergency and Beyond: Four Open Privacy and Data Protection Issues of 'Platformised' Education», p.61.

⁵⁵⁶ Si v. Noyb, «Il nuovo quadro transatlantico sulla privacy dei dati è in gran parte una copia del "Privacy Shield"». Noyb impugnerà la decisione», 10 luglio 2023, consultabile al link: <https://noyb.eu/it/european-commission-gives-eu-us-data-transfers-third-round-cjeu>.

maggior dialogo tra data protection officer dei singoli istituti e autorità nazionali di controllo.⁵⁵⁷

3.5. La compatibilità al GDPR dei software di *e-proctoring*

3.5.1 La decisione dell’Autorità Garante per la protezione dei dati personali italiana

L’utilizzo durante l’*emergency remote teaching* di software di *e-proctoring* al fine di garantire un corretto e onesto svolgimento degli esami a distanza solleva alcune criticità con riferimento alla compatibilità di tali strumenti con la disciplina del GDPR.

L’utilizzo del software di *e-proctoring Respondus* è stato infatti al centro in una decisione dell’Autorità Garante per la protezione dei dati personali (anche comunemente chiamato Garante Privacy) italiana del 16 settembre 2021. Con tale decisione è stata pronunciata un’ordinanza di ingiunzione nei confronti dell’Università Commerciale “Luigi Bocconi”, condannandola ad una sanzione pecuniaria di euro 200.000.⁵⁵⁸ La vicenda è iniziata da un reclamo formale da parte di uno studente della medesima università, in cui veniva messa in dubbio la compatibilità dell’utilizzo di Respondus con la disciplina della protezione dei dati personali prevista dal GDPR.⁵⁵⁹

Il reclamo dello studente si basa sul fatto che l’Università avrebbe obbligatoriamente raccolto dati cosiddetti *biometrici*⁵⁶⁰ sulla base giuridica del consenso degli studenti, pena l’impossibilità di svolgimento dei cd. esami «*core*» ovvero «*finalizzati al conseguimento di un titolo con valore legale*». ⁵⁶¹ Infatti, recita l’informativa del 24 aprile dell’Università: «*l’eventuale rifiuto di prestare il consenso per il trattamento dei dati biometrici [...] comporterà l’impossibilità di sostenere l’esame in modalità online e a distanza. Potrai, pertanto, sostenere la prova d’esame unicamente dal vivo, alla presenza reale e non virtuale del docente di riferimento, presso le sedi dell’Università*». ⁵⁶²

Il Garante Privacy, nonostante riconosca la natura di libera Università o Università privata dell’Ateneo milanese, sottolinea che il quadro normativo previsto dal GDPR non prevede un diverso regime applicabile a seconda che il soggetto sia pubblico o privato, ma insiste, piuttosto, sul profilo funzionale del trattamento dei dati. Per l’Autorità Garante, le Università, tanto pubbliche quanto private, perseguono il medesimo interesse pubblico, pertanto vi saranno peculiarità con riferimento alla base giuridica

⁵⁵⁷ Ibidem, p.62.

⁵⁵⁸ Autorità Garante per la protezione dei dati personali, Ordinanza ingiunzione nei confronti di Università Commerciale ‘Luigi Bocconi’ di Milano – 16 settembre 2021 [doc. web. N. 9703988], pubblicata in Registro dei provvedimenti n. 317 del 16 settembre 2021, consultabile al link: <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9703988>.

⁵⁵⁹ G. Bincoletto, «Italy - E-Proctoring During Students’ Exams: Emergency Remote Teaching at Stake», *European Data Protection Law Review* 7, fasc. 4, 2021, pp. 586–91, <https://doi.org/10.21552/edpl/2021/4/15>.

⁵⁶⁰ Articolo 6 n. 14 GDPR: «i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l’identificazione univoca, quali l’immagine facciale o i dati dattiloscopici».

⁵⁶¹ Si v. par. 2 della decisione.

⁵⁶² Ibidem.

necessaria per il trattamento.⁵⁶³ In particolar modo, la base giuridica varia a seconda che si processino dati personali o categorie particolari di dati ai sensi dell'articolo 9 GDPR tra cui rientrano anche, appunto, i «*dati biometrici intesi a identificare in modo univoco una persona fisica*». Dunque, sarà possibile trattare i dati personali «*per adempiere un obbligo legale al quale è soggetto il titolare del trattamento*» o «*per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri*» ai sensi dell'articolo 6, paragrafo 1, lett. c) ed e) del GDPR.

Con riferimento alle categorie particolari di dati, invece, la questione si complica: come già visto, l'articolo 9 del Regolamento, nel dettare al primo paragrafo un generale divieto di trattamento delle categorie particolari di dati, prevede al secondo paragrafo una serie di eccezioni a tale divieto. Nel caso di specie, assume rilievo l'eccezione di cui alla lett. g) del Regolamento: «*necessità per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati Membri*». L'articolo, però, postula anche la necessità che il trattamento sia proporzionato alla finalità perseguita, rispetti l'essenza del diritto alla protezione dei dati e preveda misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

L'Università Bocconi si è difesa allegando di non trattare dati biometrici, essendo preponderante una tecnologia di rilevamento facciale non comportante alcun tipo di estrazione di dato biometrico. Tuttavia, secondo il Garante, il software

*«effettua un trattamento tecnico specifico di una caratteristica fisica degli interessati per confermare la presenza e la coincidenza dell'interessato per tutta la durata della prova. Seppur il sistema non comporta l'identificazione del candidato – nonostante fra le azioni preliminari di LockDown Browser sia previsto che lo studente scatti una propria foto con le funzionalità interne a LockDown Browser ed esibisca un documento e non confronti l'immagine del volto con altre immagini presenti in propri database e in database esterni, ovvero non effettui una identificazione (1 a molti) o verifica biometrica (uno a uno), il sistema effettua comunque un trattamento di dati biometrici che consiste nella raccolta, elaborazione e analisi del video prodotto dal software tramite un algoritmo di intelligenza artificiale al fine di produrre i 'flag'».*⁵⁶⁴

Dunque, l'Ateneo milanese non avrebbe potuto raccogliere determinati dati sulla base giuridica del consenso, che non potrebbe peraltro qualificarsi come «*manifestazione di volontà libera*», visto lo squilibrio della posizione degli studenti rispetto al titolare del trattamento. L'alternativa di svolgere l'esame in presenza avrebbe infatti innescato, secondo il Garante, sia maggiori rischi per la salute tanto dello studente quanto del docente, sia «*il timore di subire ripercussioni negative, anche indirette, da parte dei docenti come conseguenza del rifiuto*».⁵⁶⁵

L'Ateneo milanese avrebbe dovuto effettuare il trattamento di dati biometrici sulla base giuridica della «*necessità per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati Membri*», ovvero, ai sensi dall'articolo 2 *sexies* del Codice in materia di protezione dei dati personali in presenza di «*disposizioni di legge (...) che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il*

⁵⁶³ Si v. par. 3.1 della decisione.

⁵⁶⁴ Si v. par. 3.4 decisione.

⁵⁶⁵ Ibidem.

motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato», laddove esistenti. Non essendo possibile rinvenire una normativa che espressamente autorizzi il trattamento dei dati biometrici, si deve quindi desumere che il trattamento di detti dati sia avvenuto in assenza di base giuridica.

Nel mirino dell'Autorità Garante finisce anche l'informativa privacy fornita dall'Università agli studenti. Secondo il garante, infatti

«l'informativa sul trattamento dei dati personali fornita agli studenti, non riporta tutte le informazioni richieste dal Regolamento per assicurare un trattamento corretto e trasparente. Il documento, che fa riferimento al trattamento dei dati biometrici e di alcuni altri dati degli studenti (nome, cognome e data di nascita), solo 'a titolo esemplificativo e non esaustivo', non menziona invece gli ulteriori specifici trattamenti posti in essere mediante il sistema 'Respondus', quali il tracciamento del comportamento dello studente durante la prova (posizione del viso; disconnessioni dalla rete Internet; tentativi di utilizzare il mouse o il trackpad per passare da un'applicazione all'altra o per uscire dal sistema; applicazioni in uso), le successive elaborazioni mediante profilazione, la registrazione audio-video della prova. Né vi è menzione della fotografia scattata dal sistema all'inizio della prova allo studente, cui viene chiesto di esibire un documento di identità e di effettuare una ripresa panoramica dell'ambiente circostante. (...) inoltre, sono omessi gli specifici tempi di conservazione dei dati personali, limitandosi a prevedere, in modo generico, che 'i dati verranno conservati per il periodo strettamente necessario al perseguimento delle finalità indicate [...] e] per un periodo ulteriore in caso emergano necessità di gestire eventuali contestazioni o contenziosi». ⁵⁶⁶

Inoltre, manca una spiegazione del funzionamento del sistema di supervisione e del funzionamento del sistema di segnalazione di eventuali anomalie.⁵⁶⁷

Peraltro, per il Garante, le informazioni di per sé estremamente scarse, sono state fornite agli studenti in maniera frammentaria e disorganica.

Alla luce di ciò, dunque, il trattamento posto in essere dell'Ateneo milanese è contrario ai principi dell'articolo 5 GDPR di liceità, trasparenza e correttezza.

Secondo l'Autorità Garante, il software di *Respondus Monitor* determina una «profilazione», ovvero un «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»,⁵⁶⁸ dal momento che il software è dotato della tipica funzionalità in grado di generare segnali di allarme per rilevare comportamenti sospetti o anomali durante lo svolgimento dell'esame. Tale profilazione comporta una serie di rischi quando svolta nell'ambito dell'esercizio di compiti di interesse pubblico, consistenti in conseguenze pregiudizievoli per l'interessato, che nel caso di specie si qualificano

⁵⁶⁶ Si v. par. 3.3 decisione.

⁵⁶⁷ Ibidem.

⁵⁶⁸ Si v. art. 4, n.4) GDPR.

nell'annullamento della prova d'esame. Non solo, nel caso dell'Università Bocconi, detto trattamento non viene chiaramente descritto agli interessati, e dovrebbe peraltro avvenire, secondo il combinato disposto dell'articolo 6 par.1 lett. e) del GDPR e dell'art. 2-ter del Codice in materia di protezione di dati personali per «l'esecuzione di un compito di interesse pubblico» previsto da una norma di legge o da un regolamento, non sussistenti nel caso di specie.⁵⁶⁹

Il Garante Privacy ha inoltre sottolineato la necessità di implementare misure di *data protection by design* e *data protection by default* ai sensi dell'articolo 25 GDPR⁵⁷⁰, rilevando come il software *Respondus* collezioni molti più dati rispetto a quelli necessari alle finalità del controllo della validità dell'esame, violando il principio di minimizzazione del trattamento dei dati. In questa cornice, si colloca anche il rilievo per cui il periodo di conservazione di cinque anni per i video registrati dal software risulta sproporzionato alle finalità del trattamento.⁵⁷¹

Desta inoltre criticità il fatto che l'informativa si limiti a menzionare la possibilità che i dati siano trasferiti in territori all'esterno dell'Unione europea, senza però specificare l'esistenza della possibilità di un trasferimento anche negli Stati Uniti d'America ai sensi della decisione di adeguatezza ex articolo 44 del GDPR *Privacy Shield*, al tempo dei fatti in un primo momento ancora in vigore. Successivamente alla decisione della Corte di Giustizia dell'Unione Europea sul caso *Shrems II*, l'Università avrebbe stipulato delle clausole contrattuali tipo con *Respondus*, tuttavia senza prevedere l'adozione di misure supplementari affinché fosse garantita una tutela di dati personali adeguata, quindi non rispettando quanto stabilito dagli articoli 44 e 46 del GDPR.⁵⁷²

Infine, il Garante ha ritenuto in più parti la valutazione di impatto sulla protezione dei dati personali particolarmente lacunosa e inadeguata rispetto a quanto richiesto dall'art. 35 del GDPR. Manca, infatti, una

«puntuale valutazione 'della necessità e proporzionalità dei trattamenti in relazione alla finalità' e 'dei rischi per i diritti e le libertà degli interessati' (art. 35, par. 7, lett. b) e c)), anche in termini di possibile condizionamento o

⁵⁶⁹ Si v. par. 3.5 decisione.

⁵⁷⁰ «Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, 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 presente regolamento e tutelare i diritti degli interessati. 2. Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica».

⁵⁷¹ Si v. par. 3.6.

⁵⁷² Si v. par. 3.7.

*pressioni indirette nei confronti degli studenti, riportando giudizi di adeguatezza estremamente sintetici, privi di idonea motivazione».*⁵⁷³

Ex multis, il Garante ha rilevato che l'Università non ha illustrato le valutazioni compiute circa la necessità di utilizzare un software che raccoglie dati biometrici, così come non ha preso in considerazione strumenti alternativi meno intrusivi.⁵⁷⁴

3.5.2 Spunti comparatistici

Casi simili sono giunti davanti alle Autorità per la protezione dei dati personali di altri Paesi dell'UE e extra UE, con esiti non sempre scontati.⁵⁷⁵

Ad esempio, la Commissione Nazionale per la protezione dei dati Portoghese (CNPD), con Delibera 2021/662⁵⁷⁶ ha censurato, con rilievi simili a quelli della decisione dell'omologa autorità italiana, il software *Respondus*, disponendo inoltre la cancellazione dei dati nel frattempo raccolti nell'ambito della prima sperimentazione del software. In particolare, il CNPD ha rinvenuto, *ex multis*, che il consenso fosse, in realtà, imposto *de facto*, e dunque incompatibile con le disposizioni del GDPR. Il trattamento coinvolgeva una massiccia raccolta di dati per scopi di profilazione e monitoraggio degli studenti, senza tuttavia effettuare una valutazione sull'appropriatezza, necessità e proporzionalità di tale trattamento rispetto alla finalità generale di garantire l'integrità degli esami, non rispettando il principio di minimizzazione dei dati.⁵⁷⁷

La questione è stata invece risolta diversamente dal Tribunale di Amsterdam. In questa vicenda, gli studenti dell'Università olandese hanno lamentato la contrarietà dell'utilizzo del software di e-proctoring *Proctorio* al GDPR. L'Università di Amsterdam, nelle sue memorie difensive, ha sottolineato che i video raccolti dal software sono stati utilizzati solamente per controllare eventuali irregolarità durante lo svolgimento dell'esame, e sono accessibili solamente allo staff dell'Ateneo. Tutti i dati vengono criptati, conservati solamente all'interno del territorio UE e cancellati automaticamente dopo 30 giorni. Inoltre, gli studenti sono ben informati circa il trattamento dei dati personali, che avviene coerentemente con il GDPR in forza di un contratto stipulato tra l'Università olandese e Proctorio Inc. La corte olandese ha ritenuto, al pari del Garante italiano, che la base giuridica del trattamento dovesse collocarsi nell'interesse pubblico ex articolo 6, lettera e) del GDPR, ma ha riconosciuto detto interesse sussistente, dal momento che l'emergenza pandemica non permetteva lo svolgimento dell'esame con

⁵⁷³ Ibidem.

⁵⁷⁴ Si v. par. 3.8.

⁵⁷⁵ Per un'analisi comparata delle decisioni in materia di *e-proctoring* in Danimarca, Germania, Islanda, Italia, Olanda e Portogallo, si v. A. Giannopoulou, R. Ducato, C. Angiolini, G. Schneider, «From data subjects to data suspects : challenging e-proctoring systems as a university practice».

⁵⁷⁶ CNPD, Deliberação/2021/622:

<https://www.cnpd.pt/comunicacao-publica/noticias/aplicacoes-respondus-violam-rgpd/>.

⁵⁷⁷ A. Giannopoulou, R. Ducato, C. Angiolini, G. Schneider, «From data subjects to data suspects: challenging e-proctoring systems as a university practice», p. 289, cfr. CNPD, Deliberação/2021/622, par.53-54.

modalità tradizionali, salvando quindi l'utilizzo di *Proctorio*.⁵⁷⁸ In Olanda, la decisione del Tribunale è stata impugnata davanti alla Corte d'Appello di Amsterdam, che ha escluso che le immagini del volto contenute nei documenti identificativi potessero rientrare nelle categorie particolari di dati ai sensi del GDPR, ritenendo peraltro improbabile una discriminazione degli studenti sulla base di tali attributi.⁵⁷⁹

Anche oltreoceano, negli Stati Uniti, si è sentita la necessità di fare chiarezza su questi strumenti di sorveglianza durante lo svolgimento di esami online.⁵⁸⁰ In particolare, il merito di ciò si deve al gruppo di ricerca pubblico statunitense Electronic Privacy Information Center (EPIC). EPIC è stato fondato nel 1994 e la sua missione è così riassunta: «*to focus public attention on emerging privacy and civil liberties issues and to protect privacy, freedom of expression, and democratic values in the information age*».⁵⁸¹

Nel dicembre del 2020, EPIC ha presentato un reclamo⁵⁸² al Procuratore Generale del Distretto di Columbia, lamentando un'eccessiva raccolta di dati personali degli studenti, nonché l'utilizzo di algoritmi segreti per segnalare comportamenti sospetti, determinando pratiche commerciali ingannevoli contrarie al D.C Consumer Protection Procedure Act. Nel mirino di EPIC ci sono cinque software: i già noti *Proctorio* e *Respondus*, nonché *ProctorU*⁵⁸³, *Examity* e *Honorlock*⁵⁸⁴. Secondo EPIC, questi software raccolgono una grande quantità di dati sensibili (quelli che il GDPR «categorie particolari di dati»), tra cui dati biometrici, in maniera ingiustificata, eccessiva e dannosa per gli studenti, che non hanno la possibilità di scegliere di non acconsentire al trattamento di detti dati,⁵⁸⁵ peraltro senza allegare una ragionevole motivazione per la quale risulti necessaria una tale raccolta di dati. Il trattamento di questo enorme quantitativo di dati «*deprives students of control over their data; can reveal sensitive details about a student's physical features, behaviors, disabilities, family members, and home; and can induce undue stress in test-takers that undermines the integrity of their exam sessions*».⁵⁸⁶

EPIC lamenta inoltre che i software di intelligenza artificiale finalizzati a rinvenire alcuni comportamenti sospetti non rispettano i principi di trasparenza, riservatezza e non discriminazione sanciti dai principi per l'intelligenza artificiale dell'Organization for

⁵⁷⁸ Rechtback Amsterdam, 11 giugno 2020, C/13/684665 / KG ZA 20-481, consulabile al link: <https://uitspraken.rechtspraak.nl/#!/details?id=ECLI:NL:RBAMS:2020:2917>

⁵⁷⁹ Gerechtshof Amsterdam – 200.280.852/01, par. 3.3.7.

⁵⁸⁰ Per un approfondimento sulle criticità dei software di *e-proctoring* con riferimento alla normativa statunitense, si v. L. Barrett, «Rejecting Test Surveillance in Higher Education», 1 Mich. St. L. Ver, July 29, 2021, <https://ssrn.com/abstract=3871423>.

⁵⁸¹ «About Us», EPIC - Electronic Privacy Information Center (blog), <https://epic.org/about/>.

⁵⁸² EPIC, In re Online Test Proctoring Companies, 2020, consulabile al link: [https://epic.org/documents/in-re-online-test-proctoring-companies/#:~:text=On%20December%209%2C%202020%2C%20EPIC,Act%20\(DCCPPA\)%20and%20the%20Federal.](https://epic.org/documents/in-re-online-test-proctoring-companies/#:~:text=On%20December%209%2C%202020%2C%20EPIC,Act%20(DCCPPA)%20and%20the%20Federal.)

⁵⁸³ <https://www.proctoru.com/>.

⁵⁸⁴ <https://honorlock.com/>.

⁵⁸⁵ Si v. par. 20 del reclamo.

⁵⁸⁶ Si v. par. 109 del reclamo.

Economic Cooperation and Development. Il sistema di segnalazione di eventuali irregolarità può comportare conseguenze importanti nella vita degli studenti, senza che però questi possano accedere ai dati eventualmente raccolti per confutarli o contraddirli.⁵⁸⁷

Le società proprietarie di detti software, poi, non hanno condiviso le logiche di funzionamento degli stessi: ciò significa che gli studenti non sanno come i loro dati personali sono utilizzati e quindi, in ultima istanza, non possono prestare un informato consenso al trattamento.⁵⁸⁸ Inoltre, l'idea per cui tali strumenti dovrebbero garantire processi decisionali imparziali è smentita dall'esperienza: molto spesso si registrano casi in cui l'algoritmo ha difficoltà ad individuare volti non caucasici, così come si registrano episodi di discriminazione nei confronti di soggetti di sesso femminile.⁵⁸⁹

Tali algoritmi, poi, risultano estremamente discriminatori nei confronti dei soggetti affetti da disabilità da vario tipo: molti dei comportamenti derivanti da eventuali patologie o disabilità vengono segnalati come atipici e quindi sospetti ai fini della validità dell'esame.⁵⁹⁰ Con questo reclamo, EPIC chiede formalmente al Procuratore Generale che sia condotta un'indagine su questi cinque software.

Il reclamo presentato da EPIC ha il merito di aver comportato il divieto temporaneo di tecnologie per il riconoscimento facciale nelle scuole dello stato di New York.⁵⁹¹

Il reclamo di EPIC getta luce su alcuni seri rischi di discriminazione derivanti dall'uso dei sistemi di riconoscimento facciale di *e-proctoring* che necessitano di una particolare attenzione; tuttavia, occorre notare che nel panorama europeo la sola applicazione del GDPR da parte delle autorità garanti per la protezione dei dati personali non rappresenta un rimedio sufficiente dinanzi a tali eventi discriminatori. Se da un lato l'applicazione dei principi fondamentali di correttezza, integrità, proporzionalità e necessità può svolgere un ruolo significativo nella valutazione dei rischi di discriminazione, sarà anche la cornice normativa delle disposizioni anti-discriminazione ad aiutare le Università nella scelta di piattaforme che non discriminino intere categorie di studenti.⁵⁹²

L'attenzione verso la scelta di piattaforme non discriminatorie non deve riguardare solo eventuali discriminazioni perpetrate per motivi razziali, ma anche quelle derivanti da diverse situazioni socio-economiche che limitano o impediscono l'accesso

⁵⁸⁷ Si v. par. 50 del reclamo.

⁵⁸⁸ Si v. par. 114 del reclamo.

⁵⁸⁹ J. Dastin, «Amazon Scraps Secret AI Recruiting Tool That Showed Bias against Women», Reuters, ottobre 2018, <https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G>.

⁵⁹⁰ Si v. paragrafo 54 del reclamo.

⁵⁹¹ Harvard Kennedy School, Belfer Center for science and international affair «Tech Spotlight Casebook, spring 2021», 2021, disponibile al link: <https://hks-spotlight.netlify.app/assets/tech-spotlight-casebook-2021.pdf>.

⁵⁹² A. Giannopoulou, R. Ducato, C. Angiolini, G. Schneider, «From data subjects to data suspects: challenging e-proctoring systems as a university practice», p. 298.

agli strumenti di *e-proctoring*,⁵⁹³ come ad esempio nel caso di studenti *care-giver* o che non dispongano di un ambiente proprio in cui poter svolgere il test.⁵⁹⁴

Anche in questo caso, l'Università che scelga di utilizzare dei sistemi di *e-proctoring* deve effettuare una valutazione accurata delle caratteristiche del software e, in quanto titolare del trattamento, è chiamata a verificare che le finalità del trattamento perseguite dalle piattaforme di *e-proctoring* siano in linea con gli obiettivi istituzionali dell'Ateneo.⁵⁹⁵

3.6 La tutela dei dati personali di bambini e minori

Il repentino passaggio alla didattica a distanza a marzo del 2020 e la ripresa delle attività didattiche in modalità *blended* a settembre 2021 ha riguardato, soprattutto, milioni di bambini e minori. Le criticità evidenziate relative allo svolgimento delle attività didattiche online desta ancora maggiori perplessità quando l'attenzione si sposta sui minori.

Il fanciullo gode di uno speciale livello di protezione grazie alle norme internazionali: gli articoli 8 e 16 della Convenzione di New York sui diritti del fanciullo del 1989, ratificata dall'Italia con legge 17 maggio 1991, numero 179, riconosce il diritto all'identità personale e il diritto alla riservatezza e al rispetto della vita privata. Anche per il minore, la protezione della riservatezza e dei dati personali permette una maggiore tutela della libertà e della vita stessa.⁵⁹⁶ Tutelare i dati di un minore significa proteggere il minore stesso, la sua la sua autodeterminazione e dignità.⁵⁹⁷

Il GDPR considera i minori come persone vulnerabili. Il Considerando 38 recita infatti:

«I minori meritano una specifica protezione relativamente ai loro dati personali, in quanto possono essere meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia interessate nonché dei loro diritti in relazione al trattamento dei dati personali. Tale specifica protezione dovrebbe, in particolare, riguardare l'utilizzo dei dati personali dei minori a fini di marketing o di creazione di profili di personalità o di utente e la raccolta di dati personali relativi ai minori all'atto dell'utilizzo di servizi forniti direttamente a un minore. Il consenso del titolare della responsabilità

⁵⁹³ Ibidem, p. 301.

⁵⁹⁴ Si v. T. Scassa, «The Surveillant University: Remote Proctoring, AI, and Human Rights», 8 The Canadian Journal of Comparative and Contemporary Law, 2022, pp. 271-312.

⁵⁹⁵ A. Giannopoulou, R. Ducato, C. Angiolini, G. Schneider, «From data subjects to data suspects: challenging e-proctoring systems as a university practice», p. 301.

⁵⁹⁶ A. Soro, «Liberi e connessi», Torino, codice edizioni, 2016.

⁵⁹⁷ Consiglio d'Europa, Consultative committee of the convention for the protection of individuals with regard to automatic processing of personal data, Convention 108, Children's Data Protection in Education Systems: Challenges and Possible Remedies, p. 11. In questo senso, si v. anche Consiglio d'Europa, Children's data protection in an education setting, guidelines, dicembre 2020, p. 23: «*The right to privacy and data protection are enabling rights for the protection of further rights and of the child. The right to non-discrimination, the right to development, the right to freedom of expression, the right to play and the right to protection from economic exploitation might also be at stake*», consultabile al link: <https://rm.coe.int/prems-001721-gbr-2051-convention-108-txt-a5-web-web-9-/1680a9c562>.

genitoriale non dovrebbe essere necessario nel quadro dei servizi di prevenzione o di consulenza forniti direttamente a un minore».

Il GDPR prevede inoltre all'articolo 8 delle diverse condizioni per il consenso dei minori: in particolare, solo il minore che abbia compiuto 16 anni può prestare il consenso al trattamento dei dati personali, mentre, ove il minore abbia un'età inferiore ai 16 anni «*tale trattamento è lecito soltanto se e nella misura in cui tale consenso è prestato o autorizzato dal titolare della responsabilità genitoriale*».

Tale disposizione non è esente da critiche, *in primis* dal momento che il GDPR opera una presunzione di capacità di poter comprendere le finalità del trattamento all'età di 16 anni, senza riportare elementi a sostegno di tale presunzione.⁵⁹⁸ È inoltre possibile che i singoli Stati membri stabiliscano un'età inferiore, purché non inferiore ai 13 anni.

La possibilità di prestare un consenso libero, specifico, informato e inequivocabile si scontra non solo con la mancanza di trasparenza delle privacy policy, ma anche con una scarsa educazione e formazione dei minori in termini di comprensione dell'ambiente digitale.⁵⁹⁹ Inoltre, il consenso non rappresenta un'ideale base giuridica per il trattamento dei dati nel caso in cui una scuola imponga l'utilizzo di strumenti di *e-learning*: esso non sarebbe infatti libero;⁶⁰⁰ la scuola dovrebbe dunque offrire una valida alternativa che non arrechi alcun pregiudizio al minore.⁶⁰¹

Nel tentativo di realizzare la finalità prospettata dal Considerando 38 di fornire ai minori una specifica protezione, è stata ipotizzata⁶⁰² la possibilità di applicare alcune previsioni generali del GDPR, come i principi di *data protection by design e by default* (disciplinati dall'articolo 25)⁶⁰³, al contesto dei bambini e minori.

In materia di articolo 25, una soluzione per la protezione dei dati fin dalla progettazione dovrebbe integrare il rispetto del principio di trasparenza. Quando si opera con i dati personali di bambini e minori, è infatti necessario coordinare il principio di trasparenza con le esigenze specifiche dei bambini, tenendo conto delle loro percezioni, esperienze e aspettative, considerando le diverse fasce d'età e il fatto che si trovino ancora in un'età di sviluppo.⁶⁰⁴

La *privacy by design* potrebbe rappresentare uno strumento con cui vietare la profilazione dei dati personali relativi a persone di età inferiore ad anni diciotto, obbligando i titolari del trattamento a distinguere tra bambini e adulti. Infatti, il

⁵⁹⁸ S. van der Hof, E. Lievens, «The importance of privacy by design and data protection impact assessment in strengthening protection of children's personal data under the GDPR», *Communications Law*, Vol. 23, No.1, 2018, p.3.

<https://ssrn.com/abstract=3107660>.

⁵⁹⁹ *Ibidem*, p. 5.

⁶⁰⁰ Consiglio d'Europa, *Children's data protection in an education setting, guidelines*, dicembre 2020, par. 3.5.3.

⁶⁰¹ *Ibidem*, par. 7.1.9.

⁶⁰² S. van der Hof, E. Lievens, «The importance of privacy by design and data protection impact assessment in strengthening protection of children's personal data under the GDPR», p.5.

⁶⁰³ Per un approfondimento sul concetto di *privacy by design*, si v. G. Bincoletto «La *privacy by design*: un'analisi comparata nell'era digitale», *Privacy e innovazione*, Vol. 2, Giugno 2020.

⁶⁰⁴ S. van der Hof, E. Lievens, «The importance of privacy by design and data protection impact assessment in strengthening protection of children's personal data under the GDPR», p. 12.

Considerando 71 specifica che i minori non dovrebbero essere sottoposti a un trattamento automatizzato che produca effetti giuridici che lo riguardino, compresa la profilazione.⁶⁰⁵

La privacy by design dovrebbe anche incorporare una particolare attenzione per il «diritto all'oblio», ovvero il diritto riconosciuto al soggetto di poter richiedere la cancellazione dei propri dati personali, che nei minori assume carattere centrale in forza della vulnerabilità di questi ultimi. Recita infatti il Considerando 65:

«Tale diritto è in particolare rilevante se l'interessato ha prestato il proprio consenso quando era minore, e quindi non pienamente consapevole dei rischi derivanti dal trattamento, e vuole successivamente eliminare tale tipo di dati personali, in particolare da internet. L'interessato dovrebbe poter esercitare tale diritto indipendentemente dal fatto che non sia più un minore».

Al momento, la cancellazione dei dati avviene previa richiesta dell'interessato, ma potrebbe evolversi in un ulteriore elemento di una tutela della privacy del minore by design.⁶⁰⁶ Non sono mancati tentativi di istituire una funzionalità predefinita – di *default* – di cancellazione dei dati al raggiungimento della maggiore età, salvo il consenso dell'interessato alla conservazione dei dati.⁶⁰⁷ I bambini, infatti, dovrebbero avere il diritto di condurre la propria vita adulta senza il peso degli errori commessi durante l'infanzia.⁶⁰⁸ Come già sottolineato dal Gruppo di Lavoro ex articolo 29, *«because children are developing, the data relating to them change, and can quickly become outdated and irrelevant to the original purpose of collection. Data should not be kept after this happens»*.⁶⁰⁹

Nella nota dell'Autorità Garante per la protezione dei dati personali, diffusa a marzo 2020⁶¹⁰, si legge che

«Spetta in primo luogo alle scuole e alle università- quali titolari del trattamento - la scelta e la regolamentazione, anche sulle base delle indicazioni fornite dalle autorità competenti, degli strumenti più utili per la realizzazione della didattica a distanza (cfr. anche, ove applicabile, art. 39 del Regolamento (UE) 2016/679, infra: "Regolamento").

Tali scelte dovranno conformarsi ai principi di privacy by design e by default, tenendo conto, in particolare, del contesto e delle finalità del trattamento,

⁶⁰⁵ Ibidem, p. 13.

⁶⁰⁶ Ibidem, p.14.

⁶⁰⁷ Public Interest Advocacy Center Submission to the Governor Consultation on a Digital Economy Strategy for Canada, 2010, consultabile al link:

<https://www.piac.ca/research-reports/piac-submission-to-the-government-consultation-on-a-digital-economy-strategy-for-canada/>.

⁶⁰⁸ S. van der Hof, E. Lievens, «The importance of privacy by design and data protection impact assessment in strengthening protection of children's personal data under the GDPR», p.14.

⁶⁰⁹ Gruppo di Lavoro ex articolo 29, Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools), 11 febbraio 2009, p.8, consultabile al link: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp160_en.pdf.

⁶¹⁰ Autorità Garante per la protezione dei dati personali, didattica a distanza, prime indicazioni.

nonché dei rischi per i diritti e le libertà degli interessati (artt. 24 e 25 del Regolamento). (...)

Tra i criteri che devono orientare la scelta degli strumenti da utilizzare è, dunque, opportuno includere, oltre all'adeguatezza rispetto alle competenze e capacità cognitive di alunni e studenti, anche le garanzie offerte sul piano della protezione dei dati personali (artt. 5 e ss. del Regolamento)».

Il Garante, dunque, pur raccomandando una scelta di piattaforme per lo svolgimento delle attività didattiche che rispettino i principi di privacy by design e by default, non fornisce indicazioni più dettagliate, né particolari accorgimenti nel caso di minori.

Un ulteriore strumento potrebbe essere la valutazione d'impatto sulla protezione dei dati personali (DPIA),⁶¹¹ disciplinata dall'articolo 35⁶¹².

La DPIA non è obbligatoria, ma va effettuata allorché si preveda che l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche. Essa è richiesta i) nei casi di una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche, ii) nel caso in cui vi sia il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10, ovvero vi sia la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Ebbene, pur mancando nel testo dell'articolo 35 un riferimento alla necessità di effettuare una DPIA in caso di trattamento di dati personali dei minori, il Gruppo di Lavoro ex articolo 29⁶¹³ ha ritenuto necessario condurre una DPIA nel caso in cui si effettui il trattamento di dati personali di soggetti vulnerabili o nel caso in cui vi sia uno squilibrio di potere tra interessato e responsabile del trattamento. Stando alla *littera legis* del Considerando 38, che considera i minori come soggetti vulnerabili, si ritiene dunque opportuno che gli istituti scolastici effettuino una DPIA quando ci sia il trattamento di dati personali di minori.⁶¹⁴

Tale valutazione dovrebbe tenere conto dell'intera gamma dei diritti dei minori in gioco, quali la libertà di parola e di pensiero, il diritto alla non discriminazione e il diritto alla libertà,⁶¹⁵ alla luce delle considerazioni svolte in materia di rischi per il diritto all'autodeterminazione e all'identità personale, che, nel caso dei fanciulli, è ancora un *work in progress* e dunque particolarmente a rischio.

⁶¹¹ S. van der Hof, E. Lievens, «The importance of privacy by design and data protection impact assessment in strengthening protection of children's personal data under the GDPR», p. 16.

⁶¹² Per un approfondimento, si v. G.M. Riccio, G. Scorza, E. Bellisario, «GDPR e normativa privacy, commentario».

⁶¹³ Gruppo di Lavoro ex articolo 29, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, 4 aprile 2018, consultabile al link: <https://ec.europa.eu/newsroom/article29/items/611236>.

⁶¹⁴ S. van der Hof, E. Lievens, «The importance of privacy by design and data protection impact assessment in strengthening protection of children's personal data under the GDPR», p.19.

⁶¹⁵ Ibidem.

Anche in questo caso, tuttavia, la valutazione del Garante, nella nota precedentemente citata, circa la necessità di un effettuare una DPIA dei dati personali trattati durante la didattica a distanza, non è particolarmente dettagliata.

Si dice infatti:⁶¹⁶

«La valutazione di impatto, che l'art. 35 del Regolamento richiede per i casi di rischi elevati, non è necessaria se il trattamento effettuato dalle istituzioni scolastiche e universitarie, ancorché relativo a soggetti in condizioni peculiari quali minorenni e lavoratori, non presenta ulteriori caratteristiche suscettibili di aggravarne i rischi per i diritti e le libertà degli interessati. Ad esempio, non è richiesta la valutazione di impatto per il trattamento effettuato da una singola scuola (non, quindi, su larga scala) nell'ambito dell'utilizzo di un servizio on line di videoconferenza o di una piattaforma che non consente il monitoraggio sistematico degli utenti o comunque non ricorre a nuove soluzioni tecnologiche particolarmente invasive (quali, tra le altre, quelle che comportano nuove forme di utilizzo dei dati di geolocalizzazione o biometrici)».

3.7 Nuove sfide per il mondo dell'istruzione

La tutela dei dati personali e il mondo dell'istruzione oggi conoscono un'ulteriore sfida in comune: l'intelligenza artificiale applicata all'istruzione.

In particolare, da ultimo ha suscitato l'attenzione del Garante Privacy il chatbot ChatGPT, software che sfrutta l'intelligenza artificiale generativa e l'apprendimento automatico per dialogare con gli utenti, fornendo risposte ad un numero elevatissimo di quesiti.

ChatGPT è stato sviluppato da OpenAI, la società di AlphaFold e GPT-3, previo finanziamento di 2 miliardi di dollari da parte di Microsoft tra il 2019 e il 2021.⁶¹⁷ Il software permette di porre delle domande a cui l'intelligenza artificiale risponde con frasi formulate in italiano corretto e fluente, emulando conversazioni umane.

ChatGPT può avere interessanti utilizzi anche nell'ambito del mondo dell'istruzione: interrogato su come possa essere utilizzato a fini scolastici e accademici, la risposta ottenuta è stata la seguente:

⁶¹⁶ Autorità Garante per la protezione dei dati personali, didattica a distanza, prime indicazioni.

⁶¹⁷ M. Castigli, «ChatGPT: cos'è, come si usa e cosa può fare», Agenda Digitale, 19 aprile 2023, <https://www.agendadigitale.eu/cultura-digitale/introduzione-a-chatgpt-cose-come-si-usa-e-cosa-puo-fare/>.



Ci sono diverse modalità per utilizzare ChatGPT a fini didattici. Ecco alcune idee:

1. Supporto agli studenti: Gli insegnanti possono incorporare ChatGPT in una piattaforma o un sistema di chat per fornire supporto immediato agli studenti. Gli studenti possono porre domande su concetti difficili, richiedere spiegazioni o chiedere chiarimenti. ChatGPT può fornire risposte immediate e aiutare gli studenti a superare eventuali difficoltà.
2. Esercitazioni e quiz: ChatGPT può essere utilizzato per creare esercitazioni o quiz interattivi. Gli studenti possono rispondere alle domande e ChatGPT può fornire feedback immediato sulle risposte. Questo può essere un modo efficace per consentire agli studenti di esercitarsi e verificare la loro comprensione di concetti specifici.
3. Scrittura collaborativa: Gli insegnanti possono coinvolgere gli studenti in attività di scrittura collaborativa utilizzando ChatGPT. Gli studenti possono interagire con ChatGPT per ottenere suggerimenti di scrittura, feedback sulla struttura del testo o supporto nella revisione e correzione grammaticale.
4. Generazione di contenuti: ChatGPT può essere utilizzato per generare contenuti didattici, come risorse di studio, esempi di problemi o spiegazioni dettagliate di concetti complessi. Gli insegnanti possono utilizzare ChatGPT per creare materiale aggiuntivo per arricchire il processo di apprendimento degli studenti.
5. Lingue straniere: ChatGPT può essere utilizzato come assistente per lo studio delle lingue straniere. Gli studenti possono praticare conversazioni, fare esercizi di traduzione o chiedere spiegazioni grammaticali. ChatGPT può fornire feedback istantaneo e aiutare gli studenti a migliorare le loro competenze linguistiche.

È importante sottolineare che, quando si utilizza ChatGPT a fini didattici, è necessario avere un adeguato monitoraggio e supporto umano. ChatGPT è un modello di intelligenza artificiale e potrebbe non essere in grado di fornire risposte corrette o complete in tutte le situazioni. L'insegnante dovrebbe essere coinvolto per guidare l'esperienza di apprendimento e fornire spiegazioni aggiuntive quando necessario.

Le criticità sollevate con riferimento a tale strumento sono state numerose: mettendo da parte le perplessità legate alla possibilità che gli studenti copino durante lo svolgimento dei compiti e test, desta preoccupazione l'attendibilità e la correttezza delle risposte che vengono fornite⁶¹⁸ oppure l'impatto che tale strumento può avere sulla capacità di pensiero critico e di problem solving degli studenti. Per questo ordine

⁶¹⁸ Ad esempio, è stato segnalato che ChatGPT non dispone di informazioni corrette in materia di precedenti giurisprudenziali statunitensi. Si v. M. Basile, «New York, avvocato presenta una causa usando ChatGpt. Ed è un disastro», la Repubblica, 23 maggio 2023, https://www.repubblica.it/esteri/2023/05/29/news/chatgpt_avvocato_intelligenza_artificiale_avianca-402397182/#:~:text=Le%20scuse%20di%20Schwartz&text=Schwartz%20non%20era%20un%20avvocato%20prima%20volta%20il%20ChatGpt.

Per un approfondimento su alcune risposte errate fornite da ChatGPT, si v. J. Zhou, P. Ke, X. Qiu, et al., «ChatGPT: potential, prospects, and limitations», *Front Inform Technol Electron Eng*, 2023. <https://doi-org.ezp.biblio.unitn.it/10.1631/FITEE.2300089>.

di ragioni, il dipartimento dell'istruzione di New York, seguito poi da quello di Los Angeles e di Baltimora, ha scelto di bloccare il funzionamento di ChatGPT sui device scolastici.⁶¹⁹

Non è mancato chi ha ipotizzato un utilizzo virtuoso di tale strumento.⁶²⁰ Ad esempio, ChatGPT potrebbe rappresentare un importante sussidio per la didattica, assistendo i docenti nella preparazione delle lezioni, oppure potrebbe aiutare i ricercatori nell'analisi di grandi set di dati in maniera più celere. Il chatbot potrebbe inoltre essere in grado di implementare modalità di insegnamento personalizzate, creando metodi di valutazione "su misura", ovvero che tengano conto delle inclinazioni personali del singolo studente.⁶²¹

Le implicazioni a livello pedagogico sono senza dubbio numerose⁶²², tuttavia, anche in questo caso, le criticità legate alla tutela dei dati personali non possono essere ignorate.

Il Garante privacy italiano, il 31 marzo del 2023, ha disposto la limitazione provvisoria del trattamento dei dati personali degli utenti italiani, lasciando a OpenAI un termine di 20 giorni per comunicare le misure intraprese in attuazione delle indicazioni.⁶²³ È stato infatti rilevata la mancanza di un'informativa sulla privacy rivolta agli utenti, nonché una base giuridica che giustificasse la raccolta e la conservazione massiccia di dati personali. Inoltre, sebbene il software fosse rivolto a utenti di età superiore a 13 anni, mancava un filtro per la verifica dell'età degli utenti, con il rischio di esposizione dei minori a risposte assolutamente inadeguate rispetto al loro grado di sviluppo e autoconsapevolezza. OpenAI ha seguito le indicazioni del Garante e il chatbot ChatGPT è tornato a funzionare in Italia.

Preoccupazioni analoghe ci sono state anche all'estero: in Canada, ad esempio, l'Office of the Privacy Commissioner ha avviato un'indagine su ChatGPT.⁶²⁴

⁶¹⁹ Per maggior informazioni, si v. M. Elsen-Rooney, «NYC education department blocks ChatGPT on school devices, network», Chalkbeat New York, 4 gennaio 2023, <https://ny.chalkbeat.org/2023/1/3/23537987/nyc-schools-ban-chatgpt-writing-artificial-intelligence>.

⁶²⁰ Si v. A. Tlili, B. Shehata, M.A. Adarkwah et al. «What if the devil is my guardian angel: ChatGPT as a case study of using chatbots in education», Smart Learn. Environ. 10, 15, 2023. <https://doi-org.ezp.biblio.unitn.it/10.1186/s40561-023-00237-x>.

⁶²¹ Per un approfondimento, si v. S. Atlas, «ChatGPT for Higher Education and Professional Development: A Guide to Conversational AI», 2023.

⁶²² Si v., ad esempio, l'impatto sulla valutazione dell'apprendimento in F. Zehner, C. Hahnel, «Artificial intelligence on the advance to enhance educational assessment: Scientific clickbait or genuine gamechanger?», Journal of Computer Assisted Learning, volume 39, Issue 3, 2023, p.695-702, <https://doi-org.ezp.biblio.unitn.it/10.1111/jcal.12810>.

⁶²³ Autorità Garante per la protezione dei dati personali, «Intelligenza artificiale, il Garante blocca Chat GPT. Raccolta illecita di dati personali, assenza di sistemi per la verifica dell'età dei minori», 30 marzo 2023, consultabile al link: <https://www.gdpd.it/home/docweb/-/docweb-display/docweb/9870847>.

⁶²⁴ Si v. Office of the Privacy Commissioner of Canada, «Office of the Privacy Commissioner of Canada launches investigation into CHATGPT», 4 aprile 2023, consultabile al link: https://www.priv.gc.ca/en/opc-news/news-and-announcements/2023/an_230404/.

A livello europeo, i Garanti della privacy degli Stati membri, uniti del Comitato europeo per la protezione dei dati, hanno lanciato una task force su ChatGPT⁶²⁵.

Il quadro europeo in materia si arricchisce grazie all'approvazione della relazione ⁶²⁶ del Parlamento europeo sulla proposta di Regolamento (Artificial Intelligence Act) finalizzato a fissare un quadro normativo in materia di intelligenza artificiale. L'obiettivo è giungere a un Regolamento definitivo entro la primavera del 2024.

Con tale proposta, si intende «sviluppare un ecosistema di fiducia proponendo un quadro giuridico per un'IA affidabile». Infatti, pur riconoscendo i benefici che l'IA sarebbe in grado di offrire in numerosi settori, è necessario controllare i rischi associati all'intelligenza artificiale, quali la violazione della privacy, l'uso improprio dei dati personali o la discriminazione algoritmica. Ai sensi del Considerando 14, il legislatore europeo ha scelto di avvalersi un approccio basato sul rischio, che adatta la tipologia e il contenuto degli obblighi previsti dal Regolamento all'intensità e alla portata dei rischi che possono essere generati dai sistemi di IA. In forza di questa distinzione, l'attuale proposta di Regolamento distingue tra pratiche di intelligenza artificiale vietate (titolo II), sistemi di IA ad alto rischio (titolo III), e specifici obblighi di trasparenza per determinati sistemi di IA in ragione dei rischi specifici di manipolazione da essi derivanti (titolo IV).

Ai sensi dell'articolo 6 e del richiamo all'allegato III, numero 3, alla presente proposta di Regolamento, i sistemi di IA destinati a essere utilizzati al fine di determinare l'accesso o l'assegnazione di persone fisiche agli istituti di istruzione e formazione professionale, nonché quelli destinati alla valutazione degli studenti e dei partecipanti alle prove solitamente richieste per l'ammissione agli istituti di istruzione, devono essere considerati sistemi di IA ad alto rischio.

La proposta dell'IA Act sembra dunque riconoscere alcune delle criticità precedentemente descritte in materia di *e-proctoring*, recita infatti il Considerando 35:

«I sistemi di IA utilizzati nell'istruzione o nella formazione professionale, in particolare per determinare l'accesso o l'assegnazione di persone agli istituti di istruzione e formazione professionale o per valutare le persone che svolgono prove come parte o presupposto della loro istruzione, dovrebbero essere considerati ad alto rischio in quanto possono determinare il percorso d'istruzione e professionale della vita di una persona e quindi incidere sulla sua capacità di garantire il proprio sostentamento. Se progettati e utilizzati in modo inadeguato, tali sistemi possono violare il diritto all'istruzione e alla formazione, nonché il diritto alla non discriminazione, e perpetuare modelli storici di discriminazione».

⁶²⁵ Si v. European Data Protection Board, «EDPB resolves dispute on transfers by Meta and creates task force on Chat GPT», 13 aprile 2023, al link: https://edpb.europa.eu/news/news/2023/edpb-resolves-dispute-transfers-meta-and-creates-task-force-chat-gpt_en.

⁶²⁶ Commissione europea, proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'unione, consultabile al link: <https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52021PC0206>.

Gli orientamenti etici per gli educatori sull'uso dell'intelligenza artificiale e dei dati nell'insegnamento e nell'apprendimento, pubblicati dalla Commissione europea, riconoscono tuttavia utilizzi dell'IA nel settore dell'istruzione ulteriori rispetto alla mera valutazione degli studenti e accesso agli istituti di istruzione; tra gli utilizzi dell'AI descritti figurano la possibilità di i) creare servizi di orientamento sui percorsi di istruzione futuri; ii) programmare l'assegnazione delle risorse; o iii) utilizzare l'IA per diagnosticare difficoltà dell'apprendimento grazie all'analisi di competenze cognitive come lessico, ascolto, ragionamento spaziale, soluzioni di problemi e memoria.⁶²⁷

Peraltro, non sono mancate voci in dottrina contrarie a un approccio basato sul rischio, dal momento che questo, concentrandosi sui soli danni prevedibili, sembrerebbe sottovalutare le violazioni dei diritti individuali.⁶²⁸

3.8 Considerazioni di sintesi

Con la conclusione del terzo capitolo, si chiude la descrizione di come il fenomeno del capitalismo della sorveglianza abbia guadagnato terreno nel mondo dell'istruzione, tanto nel panorama universitario – peraltro valicando i limiti della dimensione prettamente didattica - quanto in quello scolastico. Gli attori pubblici non sono più gli unici governatori dell'istruzione, poiché la scelta sulla struttura degli strumenti per l'istruzione è ormai lasciata alle piattaforme digitali.⁶²⁹

La didattica a distanza, o *emergency remote teaching* che dir si voglia, altro non è che un altro passo «fuori dalla Silicon Valley» che i capitalisti della sorveglianza stanno compiendo, in risposta all'imperativo dell'estrazione del surplus comportamentale.

Questa raccolta di dati personali ha incontrato il favore del mondo dell'istruzione che, come illustrato nel secondo capitolo, salvo che in poche sparute occasioni, ha fatto affidamento alle piattaforme proprietarie, complice anche un atteggiamento deferente del Governo e del Garante.

La DaD, diventata poi didattica digitale integrata a settembre 2020, ha conosciuto una prima battuta di arresto con il decreto legge 24 marzo 2022 numero 24⁶³⁰, detto «Decreto riaperture», convertito in legge con legge 22 maggio 2022, numero 52. Tale decreto, infatti, limitava la DaD ai soli studenti in quarantena per positività al virus, determinando la continuazione delle normali attività didattiche in presenza.

Ad oggi, le attività didattiche sembrano essere tornate alle modalità tradizionali, ma le tecnologie care alla didattica a distanza, provate particolarmente utili a superare

⁶²⁷ Commissione europea, Direttorato generale per l'istruzione, della gioventù, dello sport e della cultura, Ethical guidelines on the use of artificial intelligence (AI) and data in teaching and learning for educators, p. 16.

⁶²⁸ Per un approfondimento, si v. M. Kaminski, «The developing law of AI Regulation: A Turn to Risk Regulation», The LawFare Institute, 2023: «Using risk regulation can deprioritize rights-based harms, such as those to dignity or autonomy, and harms that are otherwise harder to measure, such as emotional harms or harms to democratic society», p.14.

<https://www.lawfaremedia.org/article/the-developing-law-of-ai-regulation-a-turn-to-risk-regulation>.

⁶²⁹ E. Celeste, G. De Gregorio, «Towards a Right to Digital Education? Constitutional Challenges of Edtech», p. 246.

⁶³⁰ Decreto Legge 24 marzo 2022, n. 24, convertito con modificazioni dalla L. 9 maggio 2022, n.52, consultabile al link:

<https://www.gazzettaufficiale.it/eli/id/2022/03/24/22G00034/sg>.

le difficoltà logistiche, difficilmente cadranno nel dimenticatoio, con il rischio di un progressivo spostamento verso una «*platformised education*». ⁶³¹ In altre parole, è difficile che si torni alle modalità di svolgimento della didattica implementate prima della pandemia. ⁶³²

Uno dei rischi nascente dall'istruzione delle piattaforme, parte integrante del nostro futuro ⁶³³, è che si crei una vera e propria monocultura educativa globale. ⁶³⁴

L'autonomia del mondo dell'istruzione, riconosciuta quale valore fondamentale del nostro Paese, è messa a rischio dalle condizioni imposte dalle piattaforme, dotate di un potere contrattuale certamente maggiore. Si potrebbe ipotizzare una partecipazione inclusiva di rappresentanti delle parti coinvolte nel rapporto contrattuale, ovvero docenti, studenti e ricercatori, così da democratizzare la stesura delle condizioni tecniche e legali necessarie che le piattaforme devono garantire. ⁶³⁵ Dal momento che anche i sistemi di *e-proctoring* incidono sulle modalità di erogazione della didattica, con effetti sugli studenti e sulle istituzioni, sarebbe opportuno includere una partecipazione democratica nel procedimento di scelta di affidare lo svolgimento degli esami a tali piattaforme, così da ascoltare anche le voci delle minoranze. ⁶³⁶

Un'altra soluzione perseguibile per tutelare la libertà di insegnamento è quella già anticipata dal Politecnico di Torino, ovvero implementare un'infrastruttura digitale «in-house», libera da ogni qualsivoglia interferenza delle logiche commerciali proprie delle piattaforme dei capitalisti della sorveglianza.

Inoltre, alcuni in dottrina ⁶³⁷ hanno ipotizzato la possibilità di immaginare il mondo dell'istruzione online come un «*commons*» ⁶³⁸, che metta al centro l'azione collettiva, la fiducia e la cooperazione. L'obiettivo sarebbe quello di creare un «*data commons*» focalizzato sulla protezione dei dati, consentendo ai soggetti interessati al trattamento dei dati personali l'esercizio collettivo dei diritti derivanti dalla normativa posta a tutela

⁶³¹ V. Pinto, «Didattica blended: una tappa verso l'università delle piattaforme?».

⁶³² A. Giannopoulou, R. Ducato, C. Angiolini, G. Schneider, «From data subjects to data suspects: challenging e-proctoring systems as a university practice» p. 278.

⁶³³ Si v. Commissione europea, «Speech by Executive Vice-President Margrethe Vestager on a New Digital Education Action Plan 2021- 2027 and a New European Research Area», 30 September 2020, consultabile al link:

https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_20_1786.

⁶³⁴ C. Angiolini, R. Ducato, A. Giannopoulou, G. Schneider, «Remote Teaching During the Emergency and Beyond: Four Open Privacy and Data Protection Issues of 'Platformised' Education», p. 71: «*The circulation of cultural, educational, learning, and supervision models promoted through the structure of a specific platform could end up hurting the diversity of learning experiences guaranteed in different institutions. This standardization would potentially end up becoming the norm of an educational global monoculture*».

⁶³⁵ Ibidem, p. 70.

⁶³⁶ A. Giannopoulou, R. Ducato, C. Angiolini, G. Schneider, «From data subjects to data suspects: challenging e-proctoring systems as a university practice», p.302.

⁶³⁷ J. Wong, L. Racine, T. Henderson, K. Ball «Online Learning as Commons: supporting student's data protection preferences through a collaborative digital environment», JIPITEC, para 1, 14, 2023, pp. 251-277, <https://www.jipitec.eu/issues/jipitec-14-2-2023/5736>.

⁶³⁸ Il concetto è stato sviluppato da E. Ostrom, «Governing the Commons: The Evolution of Institutions for Collective Action», Cambridge University Press 1990.

dei dati personali.⁶³⁹ Secondo gli autori, il *commons* dovrebbe così funzionare: il soggetto interessato al trattamento specifica in che misura desidera che i suoi dati siano protetti, così da permettere un trattamento dei dati centrato sull'individuo, in cui gli interessi di quest'ultimo prevalgono sulle preferenze o politiche stabilite dagli altri *stakeholders*. Gli interessati possono poi aggiungere le loro esperienze al data *commons* e continuare a partecipare al processo di co-creazione.⁶⁴⁰

Tale *commons* permetterebbe agli studenti di meglio comprendere le indicazioni fornite dalle organizzazioni esterne circa la raccolta, elaborazione e condivisione dei dati afferenti all'apprendimento online. In questo modo, gli studenti sarebbero dotati di maggiore controllo sui propri dati, così da poter scegliere in base alle loro preferenze in materia di protezione dei dati personali in un'ottica tanto *ex ante* quanto *ex post*.⁶⁴¹ Si creerebbe così un ambiente di maggiore trasparenza tra studenti, istituzioni universitarie e piattaforme di apprendimento.⁶⁴² Tutto ciò non richiederebbe la creazione di un nuovo quadro giuridico, ma opererebbe all'interno del quadro giuridico e tecnologico attuale: la responsabilità di protezione dei dati non spetterebbe più all'individuo, ma alla conoscenza ed expertise di una data comunità.⁶⁴³

Attualmente, l'Autorità Garante per la protezione dei dati personali italiana, in data 15 maggio 2023, ha emanato un nuovo vademecum, «*la scuola a prova di privacy*»⁶⁴⁴, in cui si prende atto delle nuove sfide che l'era digitale pone al mondo dell'istruzione, che andranno affrontate con la guida delle norme del GDPR:

*«In un contesto in cui l'innovazione tecnologica rivoluziona i processi formativi – dall'uso del web ai tablet su cui consultare i libri, dai sistemi di messaggistica e i social media al registro elettronico – resta centrale la necessità di riaffermare quotidianamente, anche in ambito scolastico, quei principi di civiltà e rispetto, come la riservatezza e la dignità della persona, che devono sempre essere al centro della formazione di ogni cittadino di oggi e di domani».*⁶⁴⁵

Nella sezione dedicata alla didattica a distanza, il Garante non si discosta dalle indicazioni fornite durante la pandemia. Si legge infatti:

«Le scuole che utilizzano sistemi di didattica a distanza nell'ambito delle proprie finalità istituzionali non devono chiedere il consenso al trattamento dei dati di studenti, genitori e docenti. Le scuole sono però tenute ad assicurare la trasparenza del trattamento informando, con un linguaggio facilmente comprensibile anche dai minori, gli interessati (studenti, genitori e docenti) in merito, in particolare, alle caratteristiche essenziali del

⁶³⁹ J. Wong, L. Racine, T. Henderson, K. Ball, «Online Learning as a Commons: Supporting students' data protection preferences through a collaborative digital environment», p. 260.

⁶⁴⁰ Ibidem, p. 260.

⁶⁴¹ Ibidem, p. 273.

⁶⁴² Ibidem, p. 269.

⁶⁴³ Ibidem, p. 260.

⁶⁴⁴ Autorità Garante per la protezione dei dati personali, *La scuola a prova di privacy*. Vademecum ed. 2023, 15 maggio 2023, consultabile al link:

<https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9886884>.

⁶⁴⁵ Ibidem, p. 4.

*trattamento che viene effettuato specificando che le finalità perseguite sono limitate esclusivamente all'erogazione della didattica a distanza, sulla base dei medesimi presupposti e con garanzie analoghe a quelle della didattica tradizionale. Se la piattaforma prescelta per l'erogazione dell'attività didattica a distanza comporta il trattamento di dati personali di studenti, genitori, docenti o altro personale scolastico per conto della scuola, il rapporto con il fornitore dovrà essere regolato con contratto o altro atto giuridico e le istituzioni scolastiche dovranno assicurarsi che i dati trattati per loro conto siano utilizzati solo per finalità didattiche».*⁶⁴⁶

Le informative privacy delle piattaforme non «generaliste» più comunemente utilizzate a fini didattici, analizzate nei paragrafi precedenti, continuano a prevedere finalità del trattamento ulteriori rispetto a quelle didattiche, pertanto non dovrebbero essere utilizzate.⁶⁴⁷ Il Garante ha poi precluso la videoregistrazione delle lezioni, tipica della didattica a distanza «ibrida», laddove si manifestino le dinamiche di classe, anche nei casi di didattica a distanza.

Come è stato sottolineato⁶⁴⁸, un ruolo centrale nella risposta a tale fenomeno è ricoperto dal legislatore europeo, chiamato a determinare un quadro normativo più chiaro con riferimento alla tutela dei dati personali raccolti durante le attività didattiche, con speciale attenzione al trasferimento dei dati personali.

Un importante passo in questa direzione è stato compiuto grazie all'approvazione del Piano d'azione dell'Educazione Digitale 2021-2027 e dello spazio europeo dell'istruzione entro il 2025, che sembrerebbero aver innescato una "europeizzazione" del settore dell'istruzione.⁶⁴⁹ Tuttavia, tra gli obiettivi non rientra un maggiore controllo sull'influenza e sull'indirizzo delle infrastrutture digitali sul mondo dell'istruzione.⁶⁵⁰

La protezione dei dati personali, così come disciplinata dal GDPR, deve essere al centro della riflessione in merito alle nuove sfide causate dalla pandemia, dal momento che il diritto alla riservatezza e alla protezione dei dati personali è strumentale ad altri diritti di rango costituzionale, come alla libertà di espressione e di autodeterminazione.

Non vanno tuttavia trascurati ulteriori rischi emergenti, come le eventuali difficoltà di accesso all'istruzione «*platformised*» per studenti con disabilità fisiche o psicofisiche, spesso colpiti direttamente nel momento in cui i docenti o le istituzioni utilizzano come piattaforme a fini didattici piattaforme «generaliste», che non dispongono degli strumenti necessari per garantire l'accesso a fini didattici alle persone con disabilità.⁶⁵¹

⁶⁴⁶ Ibidem, p. 38.

⁶⁴⁷ Ad esempio, l'informativa privacy di Google Workspace for Education riporta che «*i dati dei servizi vengono utilizzati principalmente per erogare i servizi utilizzati dalle scuole e dagli studenti, ma sono usati anche per gestire e migliorare i servizi; consigliare modi per ottimizzarne l'utilizzo; fornire e migliorare altri servizi che richiedi; fornire assistenza; proteggere i nostri utenti, il pubblico e Google e ottemperare agli obblighi di legge*». La privacy policy è consultabile al link: https://workspace.google.com/terms/education_privacy.html#privacy-policy-revamp-your-info.

⁶⁴⁸ C. Angiolini, R. Ducato, A. Giannopoulou, G. Schneider, «Remote Teaching During the Emergency and Beyond: Four Open Privacy and Data Protection Issues of 'Platformised' Education», p. 62.

⁶⁴⁹ Ibidem, p. 63.

⁶⁵⁰ Ibidem, p. 72.

⁶⁵¹ Si v. R. Chugh, U. Ruhi, «Social Media for Tertiary Education» in Arthur Tatnall (ed), *Encyclopedia of Education and Information Technologies*, Springer International Publishing 2019.

Inoltre, lo svolgimento delle attività didattiche online presuppone la possibilità di accedere a Internet, e ciò non è sempre possibile, persino nei Paesi con sistemi consolidati di istruzione pubblica,⁶⁵² così come non va sottovalutato il problema del diverso grado di istruzione digitale delle diverse classi sociali.⁶⁵³

In ultima istanza, l'attenzione va mantenuta anche sul diritto fondamentale all'istruzione:⁶⁵⁴ la Corte europea dei diritti dell'uomo ha inoltre sottolineato il collegamento di tale diritto fondamentale al diritto al rispetto della vita privata e familiare⁶⁵⁵ e al diritto alla libertà di pensiero, coscienza e religione.⁶⁵⁶

https://doi.org/10.1007/978-3-319-60013-0_202-1.

⁶⁵² E. Celeste, G. De Gregorio, «Towards a Right to Digital Education? Constitutional Challenges of Edtech», p. 247.

⁶⁵³ C. Angiolini, R. Ducato, A. Giannopoulou, G. Schneider, «Remote Teaching During the Emergency and Beyond: Four Open Privacy and Data Protection Issues of 'Platformised' Education», p. 71.

⁶⁵⁴ Ibidem.

⁶⁵⁵ Si v. Corte europea dei diritti dell'uomo, *Catan and Others v. the Republic of Moldova and Russia* [GC], 19.10.2012, consultabile al link:

<https://hudoc.echr.coe.int/fre#%22itemid%22:%22002-7212%22>}}

⁶⁵⁶ Si v. Corte europea dei diritti dell'uomo, *Kjeldsen, Busk Madsen and Pedersen v. Denmark*, 7.12.1976, consultabile al link:

<https://hudoc.echr.coe.int/fre#%22itemid%22:%22001-57509%22>}}.

IV CAPITOLO

POSSIBILI SOLUZIONI: LA DISCIPLINA ANTITRUST E LA STRATEGIA EUROPEA DEI DATI

4.1 Il ruolo della normativa antitrust e l'ordine del ragionamento

Il fenomeno della *data driven economy* assume un ruolo sempre maggiore nel quadro economico europeo e globale. Basti pensare, infatti, che secondo una stima condotta dall'Unione europea, il valore dell'economia dei dati passerà da 301 miliardi nel 2018 a 829 miliardi nel 2025.⁶⁵⁷

Il dato assume il ruolo tradizionalmente svolto da capitale e lavoro, nella sua duplice veste, tuttavia, di risorsa economica e di oggetto di un diritto fondamentale.⁶⁵⁸

Se è vero che si può parlare dei dati personali come il nuovo petrolio, occorre tuttavia precisare che questi sono però dotati di caratteristiche strutturalmente differenti da quelle del petrolio: sono beni non rivali, ciò significa che l'utilizzo da parte di taluno non esclude la possibilità di godimento di altri, sono poi suscettibili di essere utilizzati e sfruttati contemporaneamente e in luoghi diversi da un numero illimitato di soggetti,⁶⁵⁹ non sono esauribili e vengono generati a un ritmo esponenziale.⁶⁶⁰

Ciò ha determinato un'attenzione crescente verso la dimensione "patrimoniale" dei dati, affiancando all'analisi della dimensione "morale" del dato una nuova indagine sulla possibilità di commercializzazione degli stessi. L'idea di fondo è quella di individuare nuove forme di tutela per il cittadino nel contesto digitale, che riveste, contemporaneamente, il ruolo di utente, consumatore e interessato al trattamento. Affiancando all'idea della protezione dei dati personali l'idea di una tutela di tipo negoziale, secondo alcuni meglio si potrebbe garantire una tutela dell'utente inteso quale *summa* di consumatore e soggetto interessato al trattamento.⁶⁶¹

Si è già visto come nell'ambito della *data driven economy* un ruolo centrale sia ricoperto dalle piattaforme GAFAM e non solo. Esse operano nei mercati bilaterali, caratterizzati da una tendenza connaturata al monopolio e famose sono diventate le loro attività di monopolizzazione degli utenti tramite operazioni di fusioni e acquisizioni

⁶⁵⁷ Privacy Network, «Il Mercato dei Dati», luglio 2021, consultabile al link: <https://www.privacynetwork.it/mercato-dei-dati/>, p. 2.

⁶⁵⁸ Autorità Garante per la Protezione dei Dati personali, Relazione annuale per il 2018, consultabile al link: <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9109211>.

⁶⁵⁹ Così A. La Bella, «Sfide, opportunità e minacce dell'economia data driven», in A. Morace Pinelli (a cura di), *La circolazione dei dati: persona, contratto e mercato*, Pisa, Pacini Giuridica, 2023.

⁶⁶⁰ Si stima che ognuno lasci una *footprint* digitale pari a 200 MB al giorno, si v. Basili, «Sistemi intelligenti e dati: opportunità e rischi etici».

⁶⁶¹ Per approfondire la commercializzazione dei dati personali, si v. G. D'Ippolito, «Commercializzazione dei dati personali: il dato personale tra approccio morale e negoziale», *Il diritto dell'informazione e dell'informatica*, n.3, 2020, pp. 634-674.

D'Ippolito ipotizza un riconoscimento, così come già avviene nell'ambito del diritto d'autore, di un diritto "morale" alla protezione dei dati personali, ma anche uno di "negoziale" che tutelerebbe il diritto di sfruttamento economico di tali dati personali.

di società concorrenti.⁶⁶² Inoltre, l'accumulo di dati personali da parte di aziende definite «*incumbent*» è stato gradualmente identificato come un ostacolo all'ingresso nel mercato per altre organizzazioni e un fattore determinante per l'aumento della concentrazione di potere di mercato nei mercati digitali.⁶⁶³

Se nel terzo capitolo si è effettuata una disamina delle criticità legate alla didattica a distanza con riferimento alla tutela dei dati personali, in questo capitolo si intende analizzare la possibilità di erodere l'attività delle piattaforme Big Tech non solo grazie alla disciplina del GDPR, ma servendosi dell'ausilio delle norme in materia di tutela della concorrenza, che hanno l'obiettivo di impedire la creazione di una concentrazione di potere eccessiva a vantaggio di un'impresa o un numero ristretto di imprese.⁶⁶⁴ Infatti, il valore monetario dei dati spinge le imprese ad acquistare e trattare un grande quantitativo di dati personali poiché questi ultimi vengono considerati fonte di potere di mercato. Si rende dunque necessario un approccio congiunto che tenga conto della natura di diritto fondamentale della tutela dei dati personali senza sottovalutarne il grande valore economico.⁶⁶⁵

Nel corso del presente capitolo si intende illustrare la possibile integrazione tra normativa in materia di protezione dei dati personali e antitrust, intese come normative idonee e tutelare la condizione di vulnerabilità di alcuni individui, tra cui i consumatori, tenendo a mente che i soggetti coinvolti nel fenomeno dell'istruzione delle piattaforme possono facilmente essere inclusi nella categoria di soggetti vulnerabili che nei prossimi paragrafi si cercherà di delineare.

Successivamente, si intende ricostruire l'evoluzione giurisprudenziale nel panorama europeo in materia di applicazione congiunta di normativa a tutela della concorrenza e protezione dei dati personali.

Infine, si esaminerà la strategia europea in materia di dati, con particolare attenzione al Digital Markets Act⁶⁶⁶ (DMA), Regolamento con cui l'Unione europea, riconoscendo le peculiarità dei mercati digitali, detta specifiche regole in materia di concorrenza rivolte ai grandi operatori di tale mercato, da applicare congiuntamente a

⁶⁶² Alcuni esempi di M&A a opera di Microsoft o Facebook sono stati riportati nel primo capitolo e si analizzeranno nei prossimi paragrafi.

⁶⁶³ J. Furman, «Unlocking Digital Competition, Report of the Digital Competition Expert Panel», UK Government, 2019, consultabile al link:
[/https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf).

⁶⁶⁴ A. Quarta, G. Smorto, «Diritto privato dei mercati digitali», p. 147.

⁶⁶⁵ In tal senso già nel 2014, si v. European Data Protection Supervisor, «Privacy e competitività nell'era dei Big Data», 26 marzo 2014: «*La raccolta e il controllo di enormi quantità di dati personali sono una fonte di potere di mercato per i maggiori operatori del mercato globale dei servizi Internet, ha dichiarato oggi il Garante europeo della protezione dei dati (EDPS). Le informazioni personali sono diventate una forma di valuta per pagare i cosiddetti servizi online "gratuiti" ed è un bene immateriale prezioso per un numero crescente di imprese che operano nell'UE. Ciò richiede una più stretta interazione tra i diversi regolatori*». Si v. il link;

https://edps.europa.eu/press-publications/press-news/press-releases/2014/privacy-and-competitiveness-age-big-data_en?etrans=it.

⁶⁶⁶ Regolamento (UE) 2022/1925 del Parlamento europeo e del Consiglio, 14 settembre 2022, relativo a mercati equi e contendibili nel settore digitale e che modifica la direttiva (UE) 2019/1937 e (UE) 2020/1828 (Regolamento sui mercati digitali), consultabile al link:
[/https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32022R1925&from=EN](https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32022R1925&from=EN).

quelle previste in materia di tutela della concorrenza in senso generale. Più nello specifico, i mercati digitali si caratterizzano per il coinvolgimento della comunità degli utenti nella produzione e nello scambio di beni o servizi, per la trasformazione dell'impresa secondo il modello di piattaforma, per la nascita di intermediari digitali per facilitare l'interazione degli utenti e per la centralità dell'informazione come risorsa fondamentale e fonte primaria di ricchezza.⁶⁶⁷ Il Regolamento riconosce il valore dei dati come *market asset* e la loro idoneità a determinare una posizione di vantaggio in termini concorrenziali.⁶⁶⁸ Seguirà una breve analisi delle altre norme rientranti nella strategia europea in materia di dati, ovvero il *Digital Services Act*⁶⁶⁹, il *Data Governance Act*⁶⁷⁰ e la proposta del *Data Act*⁶⁷¹ e dell'eventuale idoneità di queste ultime a rappresentare una soluzione per le criticità legate al fenomeno dell'«istruzione delle piattaforme».

4.1.1 Brevi cenni sulla normativa in materia di concorrenza e tutela del consumatore

In questa sede si cercherà di ricostruire il quadro normativo di riferimento in materia di tutela della concorrenza (tale disciplina prende sovente anche il nome di normativa antitrust) e tutela dei consumatori.

La legge di riferimento per l'ordinamento italiano in materia di tutela della concorrenza è la Legge numero 287 del 10 ottobre 1990.⁶⁷² I concetti al centro della normativa sono tre: intese restrittive della libera concorrenza (articolo 2), abuso di posizione dominante (articolo 3) e operazioni di concentrazione (articolo 5).

Più nello specifico, si hanno intese restrittive della libera concorrenza quando esse

⁶⁶⁷ A. Quarta, G. Smorto, «Diritto privato dei mercati digitali», p. 105.

⁶⁶⁸ Si v. l'articolo 5, paragrafo 2, lettera b) del DMA, che vieta la combinazione di «*dati personali provenienti dal pertinente servizio di piattaforma di base con dati personali provenienti da altri servizi di piattaforma di base o da eventuali servizi forniti dal gatekeeper o dati personali provenienti da servizi di terzi*». Tale disposizione segue un orientamento inaugurato dalla Commissione europea. Si v. par. 4.4.1 del presente lavoro oppure European Commission, imposing fines under Article 14(1) of Council Regulation (EC) No. 139/2004 for the supply by an undertaking of incorrect or misleading information, (Case No.M.8228 – Facebook/WhatsApp), decisione 17 maggio 2017, consultabile al link: https://ec.europa.eu/competition/mergers/cases/decisions/m8228_493_3.pdf.

⁶⁶⁹ Regolamento (UE), 2022/2065 del Parlamento Europeo e del Consiglio, 19 ottobre 2022, relativo al mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali) consultabile al link:

<https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32022R2065#d1e1509-1-1>.

⁶⁶⁹ «Il pacchetto della legge sui servizi digitali», sito web della Commissione europea, disponibile al link: <https://digital-strategy.ec.europa.eu/it/policies/digital-services-act-package>.

⁶⁷⁰ Regolamento (UE) 2022/868 del Parlamento europeo e del Consiglio, 30 maggio 2022, relativo alla governance europea dei dati, consultabile al link:

<https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32022R0868#d1e2972-1-1>.

⁶⁷¹ Proposta di Regolamento del Parlamento europeo e del Consiglio riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo (normativa sui dati), consultabile al link:

<https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52022PC0068>.

⁶⁷² Legge 10 ottobre 1990, n. 287, Norme per la tutela della concorrenza e del mercato, consultabile al link:

<https://www.agcm.it/chi-siamo/normativa/legge-10-ottobre-1990-n-287-norme-per-la-tutela-della-concorrenza-e-del-mercato>.

«abbiano per oggetto o per effetto di impedire, restringere o falsare in maniera consistente il gioco della concorrenza all'interno del mercato nazionale o in una sua parte rilevante, anche attraverso attività consistenti nel: a) fissare direttamente o indirettamente i prezzi d'acquisto o di vendita ovvero altre condizioni contrattuali; b) impedire o limitare la produzione, gli sbocchi o gli accessi al mercato, gli investimenti, lo sviluppo tecnico o il progresso tecnologico; c) ripartire i mercati o le fonti di approvvigionamento; d) applicare, nei rapporti commerciali con altri contraenti, condizioni oggettivamente diverse per prestazioni equivalenti, così da determinare per essi ingiustificati svantaggi nella concorrenza; e) subordinare la conclusione di contratti all'accettazione da parte degli altri contraenti di prestazioni supplementari che, per loro natura o secondo gli usi commerciali, non abbiano alcun rapporto con l'oggetto dei contratti stessi».

L'articolo 3, oltre a vietare la condotta di abuso di posizione dominante, vieta di:

«a) imporre direttamente o indirettamente prezzi di acquisto, di vendita o altre condizioni contrattuali ingiustificatamente gravose; b) impedire o limitare la produzione, gli sbocchi o gli accessi al mercato, lo sviluppo tecnico o il progresso tecnologico, a danno dei consumatori; c) applicare nei rapporti commerciali con altri contraenti condizioni oggettivamente diverse per prestazioni equivalenti, così da determinare per essi ingiustificati svantaggi nella concorrenza; d) subordinare la conclusione dei contratti all'accettazione da parte degli altri contraenti di prestazioni supplementari che, per loro natura e secondo gli usi commerciali, non abbiano alcuna connessione con l'oggetto dei contratti stessi».

Infine, l'operazione di concentrazione avviene quando:

«a) quando due o più imprese procedono a fusione; b) quando uno o più soggetti in posizione di controllo di almeno un'impresa ovvero una o più imprese acquisiscono direttamente od indirettamente, sia mediante acquisto di azioni o di elementi del patrimonio, sia mediante contratto o qualsiasi altro mezzo, il controllo dell'insieme o di parti di una o più imprese; c) quando due o più imprese procedono alla costituzione di un'impresa comune che esercita stabilmente tutte le funzioni di un'entità autonoma».

La legge antitrust italiana, inoltre, designa anche l'Autorità Garante della Concorrenza e del Mercato, dotata di, *ex multis*, poteri di indagine (articolo 12) e di emanare diffide e sanzioni (articolo 15).

In generale, si può dire che un mercato è concorrenziale quando gli operatori che vi partecipano non esercitano un potere sul prezzo di mercato, se esiste libertà di entrata e di uscita, se l'informazione è completa e distribuita simmetricamente tra le parti e non si verificano esternalità.⁶⁷³

Tali norme sono il precipitato della normativa europea in materia di concorrenza⁶⁷⁴, in particolare degli articoli 101 e 102 del Trattato sul Funzionamento

⁶⁷³ A. Quarta, G. Smorto, «Diritto privato dei mercati digitali», p. 146.

⁶⁷⁴ Per una visione d'insieme, si v. Parlamento europeo, «Note tematiche sull'Unione europea, politica della concorrenza» al link:
<https://www.europarl.europa.eu/factsheets/it/sheet/82/politica-della-concorrenza>.

dell'Unione europea (TFUE). Rispettivamente, infatti, essi vietano i) gli accordi tra imprese che possano pregiudicare il commercio tra Stati membri e che abbiano per oggetto o per effetto di impedire, restringere o falsare il gioco della concorrenza nel mercato nella concorrenza; ii) lo sfruttamento da parte di una o più imprese di una posizione dominante sul mercato interno. Tali norme rimangono applicabili ai mercati digitali anche dopo l'entrata in vigore del Digital Markets Act.⁶⁷⁵

La tutela del consumatore è invece affidata al decreto legislativo 6 settembre del 2005 numero 206, denominato «Codice del Consumo».⁶⁷⁶ Il consumatore è definito dall'articolo 18, lettera a) come «*qualsiasi persona fisica che agisce per fini che non rientrano nel quadro della sua attività commerciale, industriale, artigianale o professionale*». A livello europeo le norme più importanti del TFUE sono l'articolo 12, per cui «*nella definizione e nell'attuazione di altre politiche o attività dell'Unione sono prese in considerazione le esigenze inerenti alla protezione dei consumatori*» e l'articolo 169, in cui viene detto che

«al fine di promuovere gli interessi dei consumatori ed assicurare un livello elevato di protezione dei consumatori, l'Unione contribuisce a tutelare la salute, la sicurezza e gli interessi economici dei consumatori nonché a promuovere il loro diritto all'informazione, all'educazione e all'organizzazione per la salvaguardia dei propri interessi».

Accanto ad esse esistono poi numerose direttive finalizzate alla tutela del consumatore con un approccio di carattere spesso settoriale.⁶⁷⁷ *Ex multis*, si segnala la direttiva 2011/83/UE sui diritti dei consumatori.⁶⁷⁸

4.2 Data protection e antitrust: perché è necessario un approccio congiunto

⁶⁷⁵ Si v. il Considerando numero 10 del DMA «*il presente regolamento mira a integrare l'applicazione del diritto della concorrenza, esso dovrebbe applicarsi lasciando impregiudicati gli articoli 101 e 102 TFUE, le corrispondenti norme nazionali in materia di concorrenza e le altre norme nazionali in materia di concorrenza relative ai comportamenti unilaterali basati su una valutazione caso per caso delle posizioni e dei comportamenti di mercato, compresi i relativi effetti reali o potenziali e l'ambito di applicazione preciso del comportamento vietato, e che prevedono la possibilità per le imprese di invocare giustificazioni oggettive di efficienza rispetto al comportamento in questione, nonché le norme nazionali relative al controllo delle concentrazioni. Tuttavia, l'applicazione di queste norme non dovrebbe pregiudicare gli obblighi imposti ai gatekeeper a norma del presente regolamento e la loro applicazione uniforme ed effettiva nel mercato interno*».

⁶⁷⁶ Decreto legislativo 6 settembre 2005, n. 206, Codice del consumo.

<https://www.agcm.it/competenze/tutela-del-consumatore/pratiche-commerciali-scorrette/dettaglio?id=e020532b-9cea-46b8-b8f7-27a788825dd0>.

⁶⁷⁷ Per una visione d'insieme, si v. Parlamento europeo, «Note tematiche sull'Unione europea, misure di protezione dei consumatori» al link:

<https://www.europarl.europa.eu/factsheets/it/sheet/47/misure-di-protezione-dei-consumatori>.

⁶⁷⁸ Direttiva 2011/83/UE del Parlamento europeo e del Consiglio, 25 ottobre 2011, sui diritti dei consumatori, consultabile al link:

<https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32011L0083&from=FI>.

Si è argomentato⁶⁷⁹ che nell'ambito dei mercati digitali è possibile individuare due fallimenti di mercato, uno legato ai problemi in materia di concorrenza, l'altro derivante da problemi informativi e comportamentali che generano «asimmetrie informative», ovvero una circostanza in cui chi opera nel mercato non ha informazioni sufficienti per valutare correttamente le condizioni dello scambio.⁶⁸⁰ Ad ogni fallimento di mercato corrisponderebbe uno specifico insieme di norme in grado di porre rimedio a tali fallimenti: le questioni collegate alla concorrenza sarebbero risolvibili grazie all'ausilio della normativa vigente in materia, mentre sarebbero le norme a tutela dei dati personali e a tutela del consumatore a poter garantire una soluzione per quelli che sono i problemi informativi e comportamentali.⁶⁸¹

Questi due fallimenti di mercato spesso coesistono, pertanto l'utilizzo del tradizionale strumento impiegato per contrastare un fallimento di mercato non sarà sempre risolutivo, dal momento che gli effetti di tale strumento dipendono anche dall'entità degli altri fallimenti di mercato e dell'efficienza delle misure impiegate per contrastarli. Si rende dunque necessaria un'analisi che simultaneamente indaghi entrambi i fallimenti di mercato.⁶⁸²

Solitamente, le norme in materia di concorrenza e protezione dei dati personali sono intese quali norme che separatamente e rispettivamente risolvono i fallimenti di mercato ad esse attinenti, ma non si possono ignorare le interazioni possibili: le questioni attinenti alla concorrenza possono avere degli effetti negativi sulla privacy e protezione dei dati personali e viceversa, e al contempo anche l'insieme di norme poste a rimedio di uno o l'altro fallimento di mercato può determinare conseguenze che invadono il campo di applicazione di un altro insieme di norme.⁶⁸³ Gioverà in tal senso un esempio: le criticità precedentemente illustrate in materia di mancanza di trasparenza delle privacy policy determinano problemi comportamentali e informativi che, non permettendo ai consumatori di esprimere un consenso informato, costituiscono un fallimento di mercato. Ciò però crea delle conseguenze anche per quanto riguarda la tutela della concorrenza, perché i consumatori non possono confrontare le pratiche di raccolta dei dati delle imprese concorrenti, rafforzando il vantaggio competitivo di piattaforme digitali come Google e Facebook. Analogamente, la presenza di un effetto lock-in dei consumatori può essere un'efficace arma in mano

⁶⁷⁹ W. Kerber, K. Zolna, «The German Facebook Case: The Law and Economics of the Relationship between Competition and Data Protection Law», *European Journal of Law and Economics*, November 2021. <https://ssrn.com/abstract=3719098>.

⁶⁸⁰ A. Quarta, G. Smorto, «Diritto privato dei mercati digitali», p.67.

⁶⁸¹ W. Kerber, K. Zolna, «The German Facebook Case: The Law and Economics of the Relationship between Competition and Data Protection Law», p. 7: «*It is the task of consumer policy to protect consumers against the negative effects of market failures of information and behavioural problems. (...) If we interpret the EU data protection law from an economic standpoint, then it focuses on solving two different problems: on the one hand, it defines and assigns a bundle of rights on personal data to individual persons; on the other, it should help solving information and behavioural problems of these persons with regard to giving consent for allowing firms to process, collect, and use their personal data purposes. Therefore, both data protection law and consumer law can address the market failure "information and behavioural problems" with the respect to the collection and use of personal data*».

⁶⁸² Ibidem, p. 8.

⁶⁸³ Ibidem, p. 14.

alle piattaforme digitali, che potrebbero sfruttare tale circostanza per spingere gli utenti ad accettare politiche sul trattamento dei dati personali particolarmente pervasive.⁶⁸⁴

Tali interazioni tra due diversi settori del diritto rappresentano una novità che scaturisce dalla diffusione dell'utilizzo dei *Big Data*, e potrebbero suggerire la necessità di abbandonare un approccio a «compartimenti stagni», lasciando piuttosto spazio a un utilizzo congiunto delle norme in materia di dati personali e tutela della concorrenza.

La normativa posta a tutela della concorrenza può avere un ambito di applicazione molto ampio, dal momento che la raccolta di dati da parte delle piattaforme digitali può dare vita a una serie di conseguenze negative sulla concorrenza e quindi giustificare l'applicazione dei rimedi previsti. Ad esempio, il comportamento di collusione di più imprese che decidano di accordarsi circa il contenuto delle privacy policy può rappresentare una pratica contraria all'articolo 101 del TFUE poiché ostacolerebbe il gioco della concorrenza,⁶⁸⁵ fissando direttamente o indirettamente le condizioni di transazione. Questo porterebbe i consumatori a non poter scegliere tra diversi servizi con diversi gradi di tutela dei dati personali.⁶⁸⁶ In generale, qualsiasi condotta di raccolta o combinazione di dati in grado di creare barriere all'ingresso del mercato necessita l'applicazione della normativa antitrust.⁶⁸⁷

Più complesso è il discorso in materia di applicazione della tutela dei consumatori alle questioni attinenti alla tutela dei dati personali. Guardando alla privacy e alla tutela dei dati personali come un elemento attinente alla «qualità» di un servizio,⁶⁸⁸ si potrebbe argomentare che le criticità in materia di dati personali determinano una riduzione del benessere dei consumatori.⁶⁸⁹ Tuttavia, data la natura di dati personali quali beni non rivali, la raccolta dei dati personali non lascia i consumatori con meno dati disponibili, pertanto non sempre una massiccia raccolta di tali dati porta a una riduzione del benessere dei consumatori.⁶⁹⁰

Vi sono però situazioni in cui la tutela della dei dati personali si ricollega alla tutela del benessere del consumatore, come ad esempio nel caso in cui esistano clausole sulla tutela dei dati personali imposte da un'azienda dominante in maniera uniforme. In un mercato ben funzionante, infatti, esisterebbero aziende che offrono un livello di protezione dei dati personali diverso, finalizzato a incontrare le preferenze dei consumatori che sono, stando a studi empirici, eterogenee⁶⁹¹, così da garantire il benessere massimo del consumatore.⁶⁹² In altre parole, la possibilità di scegliere di far ricorso a piattaforme digitali con diversi gradi di tutela dei dati personali permetterebbe al consumatore di conseguire il benessere massimo: infatti, in base alle proprie

⁶⁸⁴ Ibidem.

⁶⁸⁵ Ibidem, p.13.

⁶⁸⁶ Ibidem, p. 10.

⁶⁸⁷ Ibidem, p. 13.

⁶⁸⁸ Si v. J. Hucap, «Data protection and Antitrust: new types of abuse cases? An economist view in light of the German Facebook Decision», CPI Antitrust Chronicle, febbraio 2019.

⁶⁸⁹ W. Kerber, K. Zolna, «The German Facebook Case: The Law and Economics of the Relationship between Competition and Data Protection Law», p.13-16.

⁶⁹⁰ Ibidem.

⁶⁹¹ Si v. A. Acquisti, C. Taylor, L. Wagman, «The Economics of Privacy» Journal of Economic Literature, 54(2),2016, pp. 442-492.

⁶⁹² W. Kerber, K. Zolna, «The German Facebook Case: The Law and Economics of the Relationship between Competition and Data Protection Law», p. 14.

preferenze, potrebbe scegliere un livello più o meno alto di tutela. Invece, se tale gamma di opzioni è limitata a causa di problemi di concorrenza, per esempio a causa di barriere all'entrata, il benessere dei consumatori è ridotto. Si potrebbe dunque argomentare che tanto la tutela dei dati personali quanto la tutela della concorrenza, quando mirano a fornire all'utente-consumatore il livello di tutela dei dati personali desiderato, condividano l'obiettivo comune di garantire il benessere del consumatore.⁶⁹³

Se l'applicazione delle norme poste a tutela della concorrenza riesce dunque a garantire risvolti positivi anche in materia di protezione dei dati personali, è stato argomentato che le norme in materia di protezione dei dati personali, e in particolar modo, dunque, il GDPR, non sono idonee a fornire soluzioni ai problemi relativi alla concorrenza. L'ostacolo maggiore è rappresentato dal fatto che il GDPR non differenzia, nel suo ambito di applicazione, le imprese a seconda del potere di mercato, prevedendo un'applicazione uniforme a tutte le imprese rientranti nell'ambito di applicazione, senza distinguere a seconda della presenza eventuali rischi per la concorrenza.⁶⁹⁴

4.3 La tutela della vulnerabilità dell'individuo tra data protection e antitrust

L'individuo, posto al centro dell'applicazione congiunta di tutela dei dati personali e tutela della concorrenza, può essere qualificato come consumatore o soggetto interessato al trattamento a seconda della normativa presa in considerazione. L'approccio perseguito dalle norme di riferimento è però differente: il GDPR, adottando un approccio interno o centrato sull'individuo, mira a preservare l'integrità delle decisioni individuali in materia di protezione dei dati personali, con lo scopo di proteggere un diritto fondamentale garantito dalle Carte, mentre la normativa antitrust, concentrandosi maggiormente sulle imprese, si pone l'obiettivo di proteggere il consumatore da eventuali abusi di mercato.⁶⁹⁵ Tali norme, pur adottando approcci diversi, si intersecano nel punto in cui mirano a ridurre la condizione di vulnerabilità dell'individuo derivante dallo squilibrio di potere tra l'individuo stesso e le piattaforme digitali.⁶⁹⁶

La vulnerabilità può manifestarsi durante il trattamento dei dati personali, in forza di presenza di privacy policy che ostano a una tutela dei diritti dell'interessato, o quale risultato del trattamento stesso in forza di pratiche di sorveglianza e manipolazione.⁶⁹⁷ Si noti come l'utilizzo di piattaforme proprietarie per la didattica a distanza desti preoccupazioni in materia di vulnerabilità dell'individuo in entrambi i sensi.

⁶⁹³ K. Jackwerth, «Great expectations: the Facebook case and subsequent legislative approaches to regulate large online platforms and digital markets», JIPITEC, 13, 2022, pp. 200-223, p.208. <https://www.jipitec.eu/issues/jipitec-13-3-2022/5556>.

⁶⁹⁴ W. Kerber, K. Zolna, «The German Facebook Case: The Law and Economics of the Relationship between Competition and Data Protection Law», p. 15-16.

⁶⁹⁵ Ibidem.

⁶⁹⁶ G. Malgieri, A. Davola, «Data Powerful, questioning the concept of power in digital markets», 5 febbraio 2022, p. 7.

<http://dx.doi.org/10.2139/ssrn.4027370>.

⁶⁹⁷ Ibidem.

La difficoltà è data dal fatto che il GDPR non prevede una definizione onnicomprensiva di soggetto vulnerabile. Solo il Considerando 75, nel tracciare le condizioni di rischio in presenza delle quali procedere a una DPIA, accenna alla condizione di vulnerabilità delle persone e in particolar modo dei minori, quali elementi da tenere in considerazione.

La condizione di vulnerabilità è tracciata con maggior precisione dal Gruppo di Lavoro ex articolo 29, che collega il concetto alla presenza di un significativo squilibrio di potere tra interessato al trattamento e titolare del trattamento. Più nello specifico, squilibrio di potere significa che l'individuo è «*unable to easily consent, or oppose, the processing of their data, or exercise their right*». ⁶⁹⁸

Si rende dunque necessario indagare il concetto di potere attraverso le lenti dell'antitrust, poiché nell'analisi del concetto di vulnerabilità è necessario un approccio multidisciplinare che coadiuvi la protezione dei dati personali e la tutela della concorrenza e che prenda in considerazione tanto il soggetto «*powerless*» quanto il soggetto «*powerful*». ⁶⁹⁹

Nella normativa posta a tutela della concorrenza, si parla infatti di potere di mercato, concetto coniato nel 1981 da Landes e Posner per descrivere «*the ability of a firm to raise prices above the competitive level without losing so many sales so rapidly that the price increase is unprofitable and must be rescinded*». ⁷⁰⁰ Nel tempo si sono susseguite diverse definizioni del concetto di potere mercato, ⁷⁰¹ ma in generale si registra una tendenza ad associare tale concetto con la presenza di una domanda inelastica, che permette alle imprese dotate di potere di mercato di non soffrire le conseguenze delle azioni che, in presenza di domanda elastica, cagionerebbero certamente una perdita di profitto. ⁷⁰²

Per indagare la presenza di potere di mercato, si è tradizionalmente postulata la necessità di individuare il mercato di riferimento, sia dal punto di vista geografico che del prodotto o servizio di riferimento, per poi comprendere se la quota di mercato detenuta da una singola impresa sia tale da rendere possibili comportamenti idonei a cagionare conseguenze dal punto di vista competitivo. ⁷⁰³

Ad oggi, il crescente sviluppo dei mercati digitali ha messo in crisi un tale approccio tradizionale, per lasciare spazio a quello che viene spesso definito come un «nuovo antitrust», ⁷⁰⁴ ambito del diritto che guarda ai dati come una fonte di potere di mercato in grado di determinare il successo delle aziende nel nuovo panorama digitale. ⁷⁰⁵

⁶⁹⁸ Gruppo di Lavoro ex art. 29, «Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679», 4 aprile 2018, consultabile al link: <https://ec.europa.eu/newsroom/article29/items/611236>.

⁶⁹⁹ G. Malgieri, A. Davola, «Data Powerful, questioning the concept of power in digital markets», p.7.

⁷⁰⁰ W.M. Landes, R.A. Posner, «Market Power in Antitrust Cases», Harvard Law Review 937, 1981, pp. 493-554.

⁷⁰¹ Si v. A. J. Daskin, L. Wu, «Observation on the Multiple Dimension of Market Power», American Bar Association 6,2005, pp. 53-58.

⁷⁰² G. Malgieri, A. Davola, «Data Powerful, questioning the concept of power in digital markets», p.9.

⁷⁰³ Ibidem.

⁷⁰⁴ F. Pasquale, M. Caderblom, «The New Antitrust: Realizing the Promise of Methodological Pluralism», 2022.

⁷⁰⁵ G. Malgieri, A. Davola, «Data Powerful, questioning the concept of power in digital markets», p.10-11.

Inoltre, taluni⁷⁰⁶ hanno persino cercato di dimostrare come le norme in materia di tutela dei dati personali e quelle poste a tutela del consumatore, come la direttiva 2011/83/UE sui diritti dei consumatori, adottino in realtà gli stessi strumenti, seppur con alcune differenze, per tutelare i soggetti deboli, prevedendo disposizioni ben specifiche in materia di informative da fornire agli utenti-consumatori, garantendo il diritto di revocare il consenso (al contratto per il consumatore o al trattamento per l'utente), oppure garantendo l'accesso alla tutela giurisdizionale dello Stato membro in cui essi abitualmente risiedono o hanno il domicilio.⁷⁰⁷ Questo sarebbe dovuto al fatto che l'utente e il consumatore, nell'ambito del commercio elettronico, si trovano in situazioni particolarmente simili: stipulano contratti con una controparte, si trovano in un ambiente digitale e non fisico, vi è una situazione di asimmetria informativa. In tali circostanze, «*the consumer and the data subject are indeed the same person*».⁷⁰⁸

4.4 L'evoluzione giurisprudenziale in materia

4.4.1 L'evoluzione nel panorama europeo

Il riconoscimento della necessità di considerare un'applicazione congiunta di tutela dei dati personali e disciplina a tutela della concorrenza non è stato immediato.

Nel 2008, la Commissione si è pronunciata in merito al progetto di concentrazione con cui Google ha acquisito l'impresa DoubleClick Inc. e alla compatibilità dell'operazione con la libera concorrenza nel mercato interno.⁷⁰⁹

In primis, la Commissione analizza la posizione delle parti nei mercati rilevanti: Google operava nel mercato della pubblicità online, mentre DoubleClick forniva tecnologie di collocamento di inserzioni pubblicitarie, qualificandosi quale operatore principale di tale mercato, ma dovendo comunque affrontare la concorrenza degli altri fornitori. La Commissione, esaminando una serie di preoccupazioni relative alla tutela della concorrenza che sarebbero potute derivare dall'operazione di acquisizione, riporta anche il rischio che la combinazione delle banche dati riguardo al comportamento in rete degli utenti potrebbe garantire all'impresa risultante dalla concentrazione una posizione ineguagliabile per i concorrenti, finendo per emarginarli.⁷¹⁰

Tale preoccupazione, però, non è considerata fondata, dal momento che

⁷⁰⁶ Per un approfondimento, si v. R. Mati, «Personal Data and Consumer Protection: What do they have in common?», in M. Bakhom et al., *Personal Data in Competition, Consumer Protection and Intellectual Property Law: Towards a Holistic Approach?*, Heidelberg, Springer Berlin, 2018.

⁷⁰⁷ Le norme di riferimento sarebbero: i) in materia di obblighi di informazione, gli articoli 13 e 14 del GDPR e gli articoli 6 e 8 della direttiva 2011/83/UE; ii) in materia di revoca del consenso, gli articoli 14 del GDPR e l'articolo 9 della suddetta direttiva; iii) in materia di tutela giurisdizionale, l'articolo 79 paragrafo 2, mentre per i consumatori, gli articoli 17-19 del Regolamento 1215/2012 concernente la competenza giurisdizionale, il riconoscimento e l'esecuzione delle decisioni in materia civile e commerciale.

⁷⁰⁸ R. Mati, «Personal Data and Consumer Protection: What do they have in common?», p. 378.

⁷⁰⁹ Commissione europea, caso COMP/M.4731 – Google/DoubleClick, 11 marzo 2008. La sintesi è liberamente consultabile al link:

[https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52008XC0722\(03\)](https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52008XC0722(03)).

⁷¹⁰ *Ibidem*, par. 25.

*«i contratti di DoubleClick con gli inserzionisti e gli editori consentono attualmente a DoubleClick di utilizzare i dati creati mediante la sua tecnologia di collocamento di inserzioni pubblicitarie solo a vantaggio del cliente in questione. Non vi è indicazione che l'impresa risultante dalla concentrazione sarebbe in grado di imporre ai suoi clienti variazioni delle condizioni contrattuali che permettano in futuro l'utilizzo incrociato dei loro dati».*⁷¹¹

Analogamente, nel 2014 la Commissione è chiamata a pronunciarsi sull'operazione di fusione tra Facebook e WhatsApp.⁷¹² Anche in questo caso, l'autorità autorizza senza condizioni l'operazione di concentrazione, non rilevando criticità dal punto di vista della concorrenza, dal momento che Facebook e WhatsApp non erano concorrenti diretti e che anche un'eventuale integrazione tra i due servizi non avrebbe comportato una riduzione della concorrenza in quanto la base di utenti era sostanzialmente la medesima.⁷¹³ La Commissione analizza inoltre la potenziale concentrazione dei dati per quanto riguarda il rafforzamento della posizione di Facebook nel mercato della pubblicità online, e ritiene che eventuali preoccupazioni in tema di privacy e dati personali non rientrino nell'ambito di applicazione delle norme in materia di concorrenza⁷¹⁴. Peraltro, dal momento che Whatsapp non raccoglie dati utili per scopi pubblicitari, l'operazione non aumenterebbe la quantità di dati potenzialmente disponibili a Facebook per finalità di carattere pubblicitario.⁷¹⁵

La Commissione, in ogni caso, riconosce due potenziali rischi successivi all'operazione di fusione. *In primis*, si ipotizza l'introduzione di servizi pubblicitari su WhatsApp, rischio che però viene ridimensionato dalla stessa autorità, in forza della presenza di un numero sufficiente di imprese concorrenti tale da evitare conseguenze dal punto di vista della concorrenza.⁷¹⁶ Il secondo rischio evidenziato attiene alla possibilità che Facebook utilizzi WhatsApp come fonte di dati relativi agli utenti per migliorare l'attività di pubblicità della piattaforma. Secondo la Commissione, questo sarebbe possibile solamente dopo una modifica delle privacy policy e dopo un abbinamento del profilo WhatsApp con il profilo Facebook, con notevoli difficoltà tecniche. Tale possibilità, comunque, non cagionerebbe problemi dal punto di vista concorrenziale, dal momento che, a mente del ragionamento della Commissione, nel mercato ci sarebbero comunque fornitori alternativi di servizi di pubblicità online.⁷¹⁷

Tali osservazioni si sono rivelate in qualche modo scorrette: nel 2017, infatti, la Commissione ha sanzionato Facebook per 110 milioni di dollari⁷¹⁸ per aver collegato,

⁷¹¹ Ibidem, par. 26.

⁷¹² Commissione europea, caso COMP/M.7217 – Facebook/Whatsapp, 3 ottobre 2012, consultabile al link: https://ec.europa.eu/competition/mergers/cases/decisions/m7217_20141003_20310_3962132_EN.pdf.

⁷¹³ Ibidem, par. 153-158.

⁷¹⁴ Ibidem, par. 164.

⁷¹⁵ Ibidem, par. 71.

⁷¹⁶ Ibidem, par. 168-179.

⁷¹⁷ Ibidem, par. 180 e ss.

⁷¹⁸ Commissione europea, imposing fines under Article 14(1) of Council Regulation (EC) No. 139/2004 for the supply by an undertaking of incorrect or misleading information, (Case No.M.8228 – Facebook/Whatsapp), decisione 17 maggio 2017, consultabile al link: https://ec.europa.eu/competition/mergers/cases/decisions/m8228_493_3.pdf.

modificando le privacy policy, i profili degli utenti di Facebook ai relativi profili di WhatsApp.⁷¹⁹

Un primo punto di svolta si è avuto nel 2016, quando la Commissione ha espresso il proprio parere sull'operazione di acquisizione di Microsoft del social network LinkedIn.⁷²⁰ Per la prima volta, la Commissione sottolinea come il controllo e lo sfruttamento di un'ampia categoria di dati riguardanti il comportamento degli utenti e la tutela dei dati personali possano avere conseguenze sulla valutazione di compatibilità delle concentrazioni con le regole in materia di concorrenza.⁷²¹

In ogni caso, la Commissione non ha ritenuto questa concentrazione di dati in un unico soggetto potesse creare effetti pregiudizievoli per la concorrenza grazie alla presenza delle norme a tutela dei dati personali,⁷²² autorizzando quindi l'operazione di acquisizione.

Si noti dunque come in un primo momento la Commissione, pur riconoscendo che i dati possano essere presi come parametro rilevante per la concorrenza, riteneva che l'obbligo delle imprese al rispetto delle norme europee in materia di protezione dei dati personali potesse limitare il peso che il trattamento dei dati ha sul mercato concorrenziale.⁷²³

4.4.2 Il *Bundeskartellamt* tedesco contro Facebook

Il caso del *Bunderkartellamt*⁷²⁴ tedesco (d'ora in avanti, Autorità Garante per la concorrenza tedesca o autorità antitrust) è divenuto celebre perché rappresenta un importante punto di svolta: per la prima volta, nel panorama europeo, una piattaforma digitale è stata ritenuta colpevole di aver sfruttato la sua posizione di dominio sul mercato per ottenere vantaggi ingiusti o per danneggiare i consumatori; peraltro, è stata anche la prima volta che un'azienda è stata accusata di sfruttare i consumatori attraverso una raccolta eccessiva di dati.⁷²⁵ L'innovazione della decisione si legge inoltre nel fatto che l'Autorità tedesca ha ricollegato il comportamento anticoncorrenziale alla violazione da parte di Facebook del GDPR.⁷²⁶

Le criticità rinvenute dall'Autorità riguardavano l'utilizzo da parte di piattaforme e siti internet terzi del «*Facebook Business Tools*». Più nello specifico, i servizi e gli strumenti in esso inclusi erano messi gratuitamente a disposizione per sviluppatori,

⁷¹⁹ Per un resoconto dei fatti, si v. La Repubblica «Maxi multa UE a Facebook per aver collegato gli account di whatsapp:110 milioni», 18 maggio 2017, consultabile al link:

https://www.repubblica.it/economia/finanza/2017/05/18/news/maxi-multa_ue_a_facebook_per_aver_collegato_gli_account_di_whatsapp-165722348/.

⁷²⁰ Commissione europea, Regulation (EC) NO 138/2004 merger procedure, case M.8124-Microsoft/LinkedIn, 6 dicembre 2016, consultabile al link:

https://ec.europa.eu/competition/mergers/cases/decisions/m8124_1349_5.pdf.

⁷²¹ Ibidem, par. 179.

⁷²² Ibidem, par. 255.

⁷²³ A. Quarta, G. Smorto, «Diritto privato dei mercati digitali», p. 156.

⁷²⁴ Bundeskartellamt, 6th Decision Division, decisione n. B6-22/16, 6 Febbraio 2019.

⁷²⁵ A.C. Witt, «Excessive Data Collection as a Form of Anticompetitive Conduct – The German Facebook Case», 66(2) Antitrust Bulletin, Jean Monnet Working Paper 1/20, 2021, pp. 276–307, p.9.

<https://ssrn.com/abstract=3671445>.

⁷²⁶ Ibidem.

inserzionisti di siti web e altre aziende terze. A mente di quanto riportato dall’Autorità, al tempo dei fatti, milioni di aziende utilizzavano i servizi di «*Facebook Business Tools*», ma i termini e le condizioni del social network non riportavano un elenco di tali aziende terze, impedendo dunque agli utenti di conoscere se un sito web avesse avuto accesso ai loro dati. Tale pratica ha permesso a Facebook di raccogliere un enorme quantitativo di dati con i quali ha costruito un database di profili utente altamente dettagliato, rendendolo in grado di offrire servizi di pubblicità mirata alle aziende.

L’Autorità Garante per la concorrenza tedesca ha avviato il procedimento a marzo del 2016, giungendo a una decisione il 6 febbraio 2019: Facebook ha abusato della sua posizione dominante.

Al cuore della decisione dell’Autorità Garante⁷²⁷ vi è l’analisi della condotta di abuso di posizione dominante di Facebook. Il *Bunderkartellamt* applica gli articoli 19(1) e 19(2) della legge tedesca in materia di concorrenza (*Gesetz gegen Wettbewerbsbeschränkung*, GWB) rifacendosi a una lettura inaugurata dalla Corte Federale di giustizia tedesca secondo cui costituisce abuso di posizione dominante l’imposizione di clausole contrattuali ai consumatori incompatibili con i diritti fondamentali. Nel caso di specie, le clausole contrattuali imposte da Facebook erano incompatibili con il diritto all’autodeterminazione e alla privacy sancito dalla legge costituzionale tedesca e con l’articolo 8 comma 2 della Carta di Nizza. Secondo l’Autorità Garante, tali diritti fondamentali sono stati riuniti sotto l’applicazione GDPR, che, intenzionato a far venir meno le asimmetrie di potere tra aziende e individui, ha reso possibile far rientrare dette questioni nel diritto commerciale.

Si comprende dunque che la base concettuale di tale decisione è rinvenibile nella lettura dei *Big Data* quali *market asset*: il fatto che Facebook sia stato in grado di ottenere dagli utenti un enorme quantitativo di dati personali è una manifestazione del potere monopolistico del social network, dal momento che tale profitto è stato reso possibile grazie alla posizione dominante sul mercato tedesco dei social network.⁷²⁸ La decisione dell’Autorità Garante sembra dunque suggerire che il rispetto della privacy e dei dati personali degli utenti sia essenziale per favorire la concorrenza nel mercato dei social network.⁷²⁹

Tra le molte argomentazioni di difesa proposte da Facebook, in questa sede si sceglie di riportare quella relativa al consenso. Più nello specifico, secondo Facebook, la sua condotta non sarebbe illecita dal momento che gli utenti avevano prestato il consenso ai termini e le condizioni previste dalla privacy policy. L’Autorità Garante ha tuttavia ritenuto che tale consenso non fosse liberamente fornito ai sensi del GDPR, dal momento che lo squilibrio di potere tra titolare del trattamento e interessato impediva un consenso libero ai sensi dell’articolo 4, numero 11 del GDPR. A sostegno di tale lettura, si ricordi anche il Considerando 43, per cui il consenso non costituisce un valido presupposto per il trattamento dei dati personali «*qualora esista un evidente squilibrio tra l’interessato e il titolare del trattamento*». Lo squilibrio di potere, a mente dell’autorità antitrust, era da collegarsi al fatto che Facebook, all’epoca della decisione, detenesse oltre il 90% della quota di mercato dei social network, ove era assente una

⁷²⁷ Per una sintesi dettagliata in lingua inglese, si v. *ibidem*.

⁷²⁸ G. Malgieri, A. Davola, «Data Powerful, questioning the concept of power in digital markets», p.15.

⁷²⁹ *Ibidem*.

vera impresa concorrente anche alla luce dell'esistenza di barriere all'entrata del mercato: gli individui che avessero voluto utilizzare un social network non avrebbero avuto nessuna scelta se non acconsentire alle privacy policy di Facebook. Alcuni⁷³⁰ hanno letto tale fenomeno di squilibrio di potere come una situazione in cui l'utente si trova in una situazione di lock-in, vale a dire una situazione in cui, pur di poter utilizzare il social network, presterebbe il consenso a privacy policy non gradite.

In seguito, il social network californiano ha impugnato tale decisione davanti al Tribunale superiore del Land Düsseldorf in Germania che ha ricorso alla Corte di Giustizia dell'Unione europea con una domanda di pronuncia pregiudiziale.⁷³¹ Ai Giudici di Lussemburgo, viene chiesto, *ex multis*, di stabilire se un'autorità nazionale garante della concorrenza possa esaminare, in via principale o incidentale, i comportamenti di un'impresa alla luce della normativa del GDPR e se, il fatto che l'operatore occupi una posizione dominante nel mercato dei social network online possa ostare a un consenso libero, specifico, informato e inequivocabile, così come disciplinato dall'articolo 4, punto 11 del GDPR.

I giudici di Lussemburgo rilevano che la conformità o la non conformità alle disposizioni del GDPR può costituire un elemento che l'autorità garante della concorrenza deve esaminare per verificare la presenza di un eventuale abuso di posizione dominante del mercato,⁷³² dal momento che l'accesso e lo sfruttamento dei dati personali rivestono «un'importanza fondamentale nell'ambito dell'economia digitale»⁷³³, diventando

*«un parametro significativo della concorrenza fra imprese dell'economia digitale. Pertanto, escludere le norme in materia di protezione dei dati personali dal contesto giuridico che le autorità garanti della concorrenza devono prendere in considerazione in sede di esame di un abuso di posizione dominante ignorerebbe la realtà di tale evoluzione economica e potrebbe pregiudicare l'effettività del diritto della concorrenza all'interno dell'Unione».*⁷³⁴

La Corte precisa che le autorità di controllo del GDPR e l'autorità garante della concorrenza nazionale esercitano funzioni diverse e perseguono obiettivi e compiti ad esse propri.⁷³⁵ Nella pratica, ciò significa che, in forza del principio di leale cooperazione, se l'autorità garante della concorrenza ritenga necessario esaminare la conformità di un comportamento di un'impresa al GDPR, questa debba seguire quanto già deciso dall'autorità nazionale di controllo competente o dalla Corte, non potendo discostarsene e potendo solo trarre le proprie conclusioni circa l'applicazione del diritto

⁷³⁰ Ibidem, p. 18.

⁷³¹ Corte di Giustizia dell'Unione europea, Sentenza della Corte (Grande Sezione), 4 luglio 2023, Causa 252/21, Meta Platforms, già Facebook Inc., Meta Platforms Ireland Ltd, già Facebook Ireland Ltd, Facebook Deutschland GmbH contro Bundeskartellamt, consultabile al link: <https://curia.europa.eu/juris/document/document.jsf?jsessionid=D79FF609E07A861EB91C4BE8B5B19882?text=&docid=275125&pageIndex=0&doclang=IT&mode=req&dir=&occ=first&part=1&cid=154729>.

⁷³² Ibidem, par. 48.

⁷³³ Ibidem par. 50.

⁷³⁴ Ibidem, par. 51.

⁷³⁵ Ibidem, par. 44.

della concorrenza.⁷³⁶ In caso di dubbi sulla decisione dell'autorità di controllo competente o nel caso in cui ritenga necessaria una pronuncia della stessa in forza di una violazione del GDPR, deve consultare l'autorità competente,⁷³⁷ che deve rispondere entro un termine ragionevole.⁷³⁸

Con riferimento al consenso, la Corte sottolinea che il semplice fatto che l'operatore di un social network online, in quanto titolare del trattamento, operi in una posizione dominante sul mercato, non osta di per sé a che gli utenti possano prestare un consenso libero, specifico, informato e inequivocabile.⁷³⁹ In ogni caso, la presenza di una posizione dominante sul mercato deve essere tenuta in considerazione nella valutazione della validità del consenso prestato, poiché l'utente potrebbe essere posto nella condizioni di non poter rifiutare o revocare il suo consenso senza subire pregiudizio.⁷⁴⁰ Gli utenti, inoltre, dovrebbero essere in grado di rifiutare individualmente, nell'ambito della procedura contrattuale, di prestare il loro consenso a operazioni particolari di trattamento non necessarie all'esecuzione del contratto, senza dover necessariamente rinunciare integralmente alla fruizione del servizio.⁷⁴¹ La Corte ritiene che nel caso di specie non risulta che il trattamento effettuato dal «*Facebook Business Tools*» sia necessario all'esecuzione del contratto tra Meta e gli utenti del social network Facebook.⁷⁴²

Questa vicenda giudiziaria, terminata con il sostanziale riconoscimento della necessità di un approccio congiunto di normativa antitrust e a tutela dei dati personali, in ragione del fatto che il trattamento e la pratica di accumulazione di questi ultimi riveste un ruolo centrale nella nuova economia digitale, sembra dunque inaugurare una nuova era di rimedi contro i grandi capitalisti della sorveglianza e contro la loro progressiva opera di creazione di monopoli e sfruttamento del surplus comportamentale degli utenti.

4.4.3 L'esperienza italiana

Anche in Italia l'Autorità Garante per la Concorrenza e il Mercato (d'ora in avanti AGCM o il Garante per la concorrenza) ha inglobato, nella sua attività di tutela del consumatore e della concorrenza, l'attenzione alla normativa in materia di protezione dei dati personali, seguendo un trend di convergenza dei due sistemi normativi già sviluppatosi nel panorama europeo e americano.⁷⁴³

⁷³⁶ Ibidem, par. 56.

⁷³⁷ Ibidem, par. 57.

⁷³⁸ Ibidem, par. 58.

⁷³⁹ Ibidem, par. 147.

⁷⁴⁰ Ibidem, par. 148.

⁷⁴¹ Ibidem, par. 150.

⁷⁴² Ibidem, par. 149.

⁷⁴³ G. D'Ippolito, «Commercializzazione dei dati personali: il dato personale tra approccio morale e negoziale», p.652.

Per un approfondimento sull'evoluzione americana, si v. M.K. Ohlhausen, A. P. Okuliar, «Competition, Consumer Protection and the right (approach) to privacy», *Antitrust Law Journal*, 2015, <https://ssrn.com/abstract=2561563>.

Più nello specifico, si segnala il provvedimento del 29 novembre 2018,⁷⁴⁴ con cui l'AGCM sanziona, in seguito a pratiche commerciali scorrette, la società capogruppo Facebook Inc. e la società operativa a livello europeo Facebook Ireland per un importo complessivo di 10 milioni di euro.

Le pratiche commerciali esaminate e sanzionate sono due. In primo luogo, l'attenzione è posta sul fatto che l'utente, all'epoca dei fatti, nel momento della registrazione sulla piattaforma, avrebbe letto una clausola sulla gratuità del servizio che recitava: «*Iscriviti, è gratis e lo sarà sempre*». Tale clausola, secondo l'autorità antitrust, avrebbe violato la disciplina in materia di Codice del consumo poiché non informava adeguatamente gli utenti sul fatto che il social network avrebbe utilizzato i loro dati personali per finalità commerciali.⁷⁴⁵ In altre parole, gli utenti si sarebbero trovati nella cosiddetta «*trappola del dono*» o «*Internet cost trap*»: se il servizio o il bene offerto è gratuito, allora il prodotto venduto è l'utente stesso.⁷⁴⁶ In fase istruttoria, infatti, l'AGCM conferma il business model del gruppo Facebook, basato sulla raccolta e sfruttamento dei dati degli utenti a fini remunerativi. Tali dati, quindi, avrebbero potuto essere intesi come contro-prestazione del servizio offerto dal social network.⁷⁴⁷

La seconda pratica sanzionata, invece, consiste nella trasmissione dei dati dei consumatori registrati da Facebook a soggetti terzi per finalità commerciali senza il loro espresso e preventivo consenso e lasciando loro solo la possibilità di de-selezionare tale trattamento attraverso un meccanismo di *opt-out*.

Dopo tale provvedimento, il social network californiano ha proposto ricorso amministrativo presso il TAR Lazio.⁷⁴⁸ I giudici del TAR Lazio hanno annullato la sanzione per la seconda condotta, sottolineando «*l'assenza di elementi sufficienti a dimostrare l'esistenza di una condotta idonea a condizionare le scelte del consumatore*»⁷⁴⁹, ma hanno confermato la sanzione per la prima condotta, stabilendo che

*«il valore economico dei dati dell'utente impone al professionista di comunicare al consumatore che le informazioni ricavabili da tali dati saranno usate per finalità commerciali che vanno al di là della utilizzazione del social network: in assenza di adeguate informazioni, ovvero nel caso di informazioni fuorvianti, la pratica posta in essere può quindi qualificarsi come ingannevole».*⁷⁵⁰

La sentenza del TAR Lazio, che brilla per chiarezza espositiva, merita di essere riprodotta nelle sue parti più importanti ai fini del presente lavoro:

«A fronte della tutela del dato personale quale espressione di un diritto della personalità dell'individuo, e come tale soggetto a specifiche e non rinunciabili

⁷⁴⁴ Autorità Garante della Concorrenza e del Mercato, provvedimento n. 27432 del 29 novembre 2018, consultabile al link:

www.agcm.it/dotcmsdoc/allegati-news/PS11112_scorr_sanz.pdf.

⁷⁴⁵ Si v. par 18-21 della decisione.

⁷⁴⁶ A. De Franceschi, «Il "pagamento" mediante dati personali», in V. Cuffaro, V. D'Orazio, V. Ricciuto (a cura di), I dati personali nel diritto europeo, Torino, Giappichelli, 2019, p. 1397.

⁷⁴⁷ Ibidem.

⁷⁴⁸ TAR Lazio, sez. I, 10 gennaio 2020 n. 261.

⁷⁴⁹ Ibidem, par. 17 della parte in diritto.

⁷⁵⁰ Ibidem, par. 10 della parte in diritto.

*forme di protezione, quali il diritto di revoca del consenso, di accesso, rettifica, oblio, sussiste pure un diverso campo di protezione del dato stesso, inteso quale possibile oggetto di una compravendita, posta in essere sia tra gli operatori del mercato che tra questi e i soggetti interessati. Il fenomeno della "patrimonializzazione" del dato personale, tipico delle nuove economie dei mercati digitali, impone agli operatori di rispettare, nelle relative transazioni commerciali, quegli obblighi di chiarezza, completezza e non ingannevolezza delle informazioni previsti dalla legislazione a protezione del consumatore, che deve essere reso edotto dello scambio di prestazioni che è sotteso alla adesione ad un contratto per la fruizione di un servizio, quale è quello di utilizzo di un "social network"».*⁷⁵¹

*«Non sussiste, nel caso di specie, alcuna incompatibilità o antinomia tra le previsioni del "Regolamento privacy" e quelle in materia di protezione del consumatore, in quanto le stesse si pongono in termini di complementarietà, imponendo, in relazione ai rispettivi fini di tutela, obblighi informativi specifici, in un caso funzionali alla protezione del dato personale, inteso quale diritto fondamentale della personalità, e nell'altro alla corretta informazione da fornire al consumatore al fine di fargli assumere una scelta economica consapevole».*⁷⁵²

Così facendo, il TAR sembrerebbe aver riconosciuto all'AGCM la vigilanza sugli aspetti negoziali inerenti al trattamento dei dati personali, lasciando al Garante Privacy la tutela degli aspetti morali.⁷⁵³

La decisione del TAR è stata confermata anche dal Consiglio di Stato, nella sentenza numero 2631 del 2021.⁷⁵⁴ In particolare, pronunciandosi rispetto al rapporto esistente tra norme in materia di protezione dei dati personali e poste a tutela della concorrenza, i giudici di Palazzo Spada affermano che esse

«vanno interpretate non nel senso della creazione di "compartimenti stagni di tutela" ma della esigenza di garantire "tutele multilivello" che possano amplificare il livello di garanzia dei diritti delle persone fisiche, anche quando un diritto personalissimo sia "sfruttato" a fini commerciali, indipendentemente dalla volontà dell'interessato-utente-consumatore. Nell'appena descritta accezione non viene in emersione la commercializzazione del dato personale da parte dell'interessato, ma lo sfruttamento del dato personale reso disponibile dall'interessato in favore di un terzo soggetto che lo utilizzerà a fini commerciali, senza che di tale destino l'interessato conosca in modo compiuto le dinamiche, fuorviato peraltro

⁷⁵¹ Ibidem, par. 6 della parte in diritto.

⁷⁵² Ibidem, par. 8 della parte in diritto.

⁷⁵³ G. D'Ippolito, «Commercializzazione dei dati personali: il dato personale tra approccio morale e negoziale», p.654.

⁷⁵⁴ Consiglio di Stato, sezione VI, 29 marzo 2021, n. 2631, consultabile al link:

https://www.giustizia-amministrativa.it/portale/pages/istituzionale/visualizza/?nodeRef=&schema=cds&nrg=202001825&noMeFile=202102631_11.html&subDir=Provvedimenti.

dalle indicazioni che derivano dalla lettura delle condizioni di utilizzo (come nel caso di specie) di una “piattaforma informatica” ». ⁷⁵⁵

Nel novembre del 2021, il Garante per la concorrenza italiano è tornato a pronunciarsi in materia di pratiche commerciali scorrette alla luce di trattamenti di dati personali non conformi al GDPR, sanzionando Apple⁷⁵⁶ e Google⁷⁵⁷ per 10 milioni di euro.

La condotta di Apple è contestata nella parte in cui prevede l’obbligo di creare un ID Apple al fine di accedere all’Apple Store e ad altri servizi collegati ad Apple, non informando i consumatori del fatto che i dati forniti con il loro ID Apple sarebbero stati utilizzati a scopi commerciali e trasmessi a terzi, dunque integrando una pratica commerciale ingannevole. Inoltre, si contesta il fatto che l’attività promozionale è svolta in assenza di una concreta possibilità per il consumatore di effettuare una scelta preventiva ed espressa sulla condivisione dei dati, in forza di un’architettura di acquisizione che non rende possibile per il consumatore esprimere la sua propria sull’utilizzo a fini commerciali dei propri dati.

Google, invece, è stato condannato per aver previsto, in sede di creazione di un ID Google, un meccanismo di *opt-out* per il consenso al trattamento per fini commerciali dei dati personali, dal momento che, a mente dell’AGCM, tale condotta avrebbe compromesso l’autodeterminazione e la libertà di scelta dei consumatori. ⁷⁵⁸

Entrambe le piattaforme hanno proposto ricorso amministrativo davanti al TAR Lazio, che ha confermato la sanzione per Google⁷⁵⁹ ma annullato quella per Apple.⁷⁶⁰ In particolare, secondo il TAR Lazio, mancherebbe un uso diretto del dato fornito dall’utente, in quanto la mera personalizzazione dello *store* non equivale a uno sfruttamento immediato delle informazioni raccolte: il profitto di Apple deriva dall’eventuale futuro acquisto degli utenti. La pratica, inoltre, non sarebbe ingannevole perché il consumatore, trovandosi in uno *store*, ovvero in un negozio virtuale, è consapevole della natura commerciale delle transazioni eseguite al suo interno.

⁷⁵⁵ Ibidem, par. 8

⁷⁵⁶ Autorità Garante della Concorrenza e del Mercato, provvedimento n. 29888 del 9 novembre 2021, consultabile al link:

https://www.agcm.it/dotcmsdoc/allegati-news/PS11150%20prov%20chiusura_estratto.pdf.

⁷⁵⁷ Autorità Garante della Concorrenza e del Mercato, provvedimento n. 29890 del 16 novembre 2021, consultabile al link:

https://www.agcm.it/dotcmsdoc/allegati-news/PS11147%20chiusura_estratto.pdf.

⁷⁵⁸ Per una sintesi del contenuto di entrambi i provvedimenti, si v. Autorità Garante della Concorrenza e del Mercato, «Sanzioni per 20 milioni a Google e Apple per uso dei dati degli utenti a fini commerciali», 26 novembre 2021, consultabile al link:

<https://www.agcm.it/media/comunicati-stampa/2021/11/PS11147-PS11150>.

⁷⁵⁹ TAR Lazio, sezione I, 18 novembre 2022, n. 15326, consultabile al link:

https://www.giustizia-amministrativa.it/portale/pages/istituzionale/visualizza?nodeRef=&schema=tar_rm&nrg=202113870&nomeFile=202215326_01.html&subDir=Provvedimenti.

⁷⁶⁰ TAR Lazio, sezione I, 18 novembre 2022, n. 15317, consultabile al link:

https://www.giustizia-amministrativa.it/portale/pages/istituzionale/visualizza?nodeRef=&schema=tar_rm&nrg=202113949&nomeFile=202215317_01.html&subDir=Provvedimenti.

Da ultimo, a maggio 2023, l’Autorità Garante della Concorrenza e del Mercato ha avviato un’istruttoria⁷⁶¹ nei confronti delle società Apple Inc., Apple Distribution International Ltd, Apple Italia S.r.l per accertare l’esistenza di un presunto abuso di posizione dominante nel mercato delle piattaforme per la distribuzione di app per utenti del sistema operativo iOS. Secondo l’AGCM, a partire da aprile 2021, Apple avrebbe adottato per i soli sviluppatori terzi di app una politica sulla privacy più restrittiva rispetto a quella applicata a sé stessa.

Dal momento che la redditività degli spazi pubblicitari venduti dagli sviluppatori di app dipende dalla disponibilità di dati raccolti in base alla profilazione – nel rispetto delle prescrizioni del GDPR - la condotta discriminatoria di Apple potrebbe causare un calo dei proventi della pubblicità degli inserzionisti di app di terze parti, a vantaggio delle proprie.

Le decisioni dell’AGCM sopra riportate dimostrano ormai la sempre crescente tendenza, anche a livello nazionale, di riconoscere i *Big Data* quali importanti *market asset*, in grado di impattare profondamente «*on the micro, meso, and macroscopic power relationships in the digital environment*».⁷⁶²

Gli studenti, ma in generale i soggetti coinvolti nella didattica a distanza, si trovano in una condizione di vulnerabilità che li rende particolarmente esposti alle pratiche di abuso di posizione dominante che possono essere perpetrate dalle piattaforme che decidano di accumulare un grande quantitativo di dati personali. Analogamente al caso *Bundeskartellamt* contro Facebook, nei casi in cui sia presente un evidente squilibrio di potere tra titolare del trattamento e interessato, risulta complesso poter riconoscere la presenza di un consenso al trattamento liberamente prestato. Ciò rientra perfettamente nel progetto del capitalismo della sorveglianza di raccogliere dati personali per la creazione di contenuti pubblicitari personalizzati, finalizzati a manipolare gli utenti e a potenzialmente condizionare la didattica. Il riconoscimento da parte dei tribunali e delle autorità amministrative competenti del valore di mercato dei dati personali e della possibilità di contrastare le condotte sopra descritte non solo tramite il GDPR, ma anche grazie alla normativa antitrust, fornisce un ulteriore strumento che, attraverso l’attività di erosione dei monopoli e oligopoli creati, tutela l’utente-studente sia come interessato al trattamento, sia come consumatore.

4.5 Il Digital Markets Act

Il *Digital Markets Act* (DMA) è un Regolamento europeo entrato in vigore il 1° Novembre 2022 e applicabile dal 2 maggio del 2023, dopo un *iter* legislativo sorprendentemente breve di soli tre anni.

A lungo si era ritenuto che le disposizioni generali in materia di concorrenza presenti agli articoli 101 e 102 del TFUE fossero idonee a disciplinare il mercato

⁷⁶¹ Autorità Garante della Concorrenza e del Mercato, avviata istruttoria nei confronti di Apple per presunto abuso di posizione dominante nel mercato delle app, consultabile al link: <https://www.agcm.it/dotcmsdoc/allegati-news/A561%20avvio.pdf>.

⁷⁶² G. Malgieri, A. Davola, «Data Powerful, questioning the concept of power in digital markets», p. 14, richiamando H. Richter, «The Property Paradigm in Private Law», in M. Bakhoum et al., *Personal Data in Competition, Consumer Protection and Intellectual Property Law: Towards a Holistic Approach?*, Heidelberg, Springer Berlin, 2018.

digitale⁷⁶³, finché nel 2019 il Report Crémer⁷⁶⁴ ha posto le basi per un florido dibattito⁷⁶⁵ sull' idoneità o meno delle norme in materia di concorrenza a risolvere i nuovi problemi dei mercati digitali.

La proposta del testo del DMA da parte della Commissione è arrivata il 15 dicembre 2020, il testo è stato poi affidato alla Commissione per il mercato interno e la protezione dei consumatori del Parlamento europeo. Il Parlamento in seduta plenaria ha approvato il testo proposto dalla Commissione parlamentare a dicembre del 2021. Sono successivamente iniziate le negoziazioni con la Commissione e il Consiglio, e il testo definitivo è stato approvato da Parlamento e Consiglio il 18 luglio del 2022.

L'articolo 1 del DMA sancisce la finalità del Regolamento, ovvero *«contribuire al corretto funzionamento del mercato interno stabilendo norme armonizzate volte a garantire, per tutte le imprese, che i mercati nel settore digitale nei quali sono presenti gatekeeper siano equi e contendibili in tutta l'Unione, a vantaggio degli utenti commerciali e degli utenti finali»*.

4.5.1 L'ambito di applicazione e alcune criticità

Per comprendere l'ambito di applicazione del nuovo Regolamento è necessario indagare i due concetti posti alla base, ovvero «servizi di piattaforma di base» e «gatekeeper» (in italiano «controllori dell'accesso»). Recita infatti, l'articolo 1, paragrafo 2:

«il presente regolamento si applica ai servizi di piattaforma di base forniti o offerti dai gatekeeper a utenti commerciali stabiliti nell'Unione o a utenti finali stabiliti o situati nell'Unione, a prescindere dal luogo di stabilimento o di residenza dei gatekeeper e dalla normativa altrimenti applicabile alla fornitura del servizio».

Per comprendere il significato del concetto di servizio di piattaforma di base, particolarmente utile sarà la lettura del Considerando numero 2:

«I servizi di piattaforma di base presentano una serie di caratteristiche che possono essere sfruttate dalle imprese che li forniscono. Un esempio di tali caratteristiche dei servizi di piattaforma di base sono le economie di scala estreme, derivanti spesso da costi marginali pari pressoché a zero per l'aggiunta di utenti commerciali o utenti finali. Tra le altre caratteristiche dei servizi di piattaforma di base figurano effetti di rete molto forti, una capacità di connettere molti utenti commerciali con molti utenti finali grazie alla multilateralità di tali servizi, un grado significativo di dipendenza sia degli utenti commerciali sia degli utenti finali, effetti di lock-in, l'indisponibilità per gli utenti finali del multihoming per uno stesso scopo, l'integrazione verticale

⁷⁶³ M. Vestager, «Fair Markets in a Digital World», discorso presso l'Autorità Garante per la Concorrenza e dei Consumatori danese, Copenaghen, 9 marzo 2018.

⁷⁶⁴ J. Cremer et al., «Competition policy for the Digital Era, 2019», consultabile al link: [/https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf](https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf).

⁷⁶⁵ Si v., ad esempio, Commissione europea, «Inception Impact Assessment: New Competition Tool», 2 giugno 2020, al link: https://competition-policy.ec.europa.eu/public-consultations/2020-new-comp-tool_en; si v. inoltre L. Khan, «Amazon's Antitrust Paradox».

e vantaggi basati sui dati. Tutte le caratteristiche sopraelencate, in combinazione con le pratiche sleali delle imprese che forniscono i servizi di piattaforma di base, possono compromettere considerevolmente la contendibilità dei servizi di piattaforma di base, nonché avere un impatto sull'equità del rapporto commerciale tra le imprese che forniscono tali servizi e i relativi utenti commerciali e finali. Nella pratica ciò determina riduzioni rapide e, potenzialmente, di ampia portata in termini di scelta per gli utenti commerciali e gli utenti finali e può pertanto conferire al fornitore di tali servizi la posizione cosiddetta di gatekeeper (controllore dell'accesso). Allo stesso tempo è opportuno riconoscere che i servizi che agiscono a fini non commerciali, come i progetti di collaborazione, non dovrebbero essere considerati servizi di piattaforma di base ai fini del presente regolamento».

L'articolo 2, numero 2, fornisce poi un elenco chiuso di quelli che sono considerati servizi di piattaforma di base ai fini del regolamento, ovvero:

«a)servizi di intermediazione online; b)motori di ricerca online; c)servizi di social network online; d)servizi di piattaforma per la condivisione di video; e)servizi di comunicazione interpersonale indipendenti dal numero; f)sistemi operativi; g)browser web; h)assistenti virtuali; i)servizi di cloud computing; j)servizi pubblicitari online, compresi reti pubblicitarie, scambi di inserzioni pubblicitarie e qualsiasi altro servizio di intermediazione pubblicitaria, erogati da un'impresa che fornisce uno dei servizi di piattaforma di base elencati alle lettere da a) a i)».⁷⁶⁶

Affinché sia possibile applicare le previsioni del DMA, è necessario che i servizi di piattaforma di base siano forniti da un'impresa gatekeeper, ovvero che, ai sensi dell'articolo 3, paragrafo 1: a) ha un impatto significativo sul mercato interno; b) fornisce un servizio di piattaforma di base che costituisce un punto di accesso (gateway) importante affinché gli utenti commerciali raggiungano gli utenti finali; e c) detiene una posizione consolidata e duratura, nell'ambito delle proprie attività, o è prevedibile che acquisisca siffatta posizione nel prossimo futuro. Tali condizioni si presumono rispettate quando:

«a)in relazione al paragrafo 1, lettera a), se raggiunge un fatturato annuo nell'Unione pari o superiore a 7,5 miliardi di EUR in ciascuno degli ultimi tre esercizi finanziari, o se la sua capitalizzazione di mercato media o il suo valore equo di mercato equivalente era quanto meno pari a 75 miliardi di EUR nell'ultimo esercizio finanziario, e se essa fornisce lo stesso servizio di piattaforma di base in almeno tre Stati membri; b)in relazione al paragrafo 1, lettera b), se fornisce un servizio di piattaforma di base che, nell'ultimo esercizio finanziario, annovera almeno 45 milioni di utenti finali attivi su base mensile, stabiliti o situati nell'Unione, e almeno 10 000 utenti commerciali attivi su base annua stabiliti nell'Unione, identificati e calcolati conformemente alla metodologia e agli indicatori di cui all'allegato; c)in relazione al paragrafo 1, lettera c), se le soglie di cui alla lettera b) del

⁷⁶⁶ Per una definizione di ognuno di questi servizi di piattaforma di base, si v. articolo 2, numero 3 del DMA.

presente paragrafo sono state raggiunte in ciascuno degli ultimi tre esercizi finanziari».

A mente dell'articolo 3, paragrafo 3, l'impresa che raggiunga le tre soglie di cui al paragrafo 2, deve effettuare una notifica alla Commissione, tuttavia, può dimostrare che eccezionalmente non soddisfa i requisiti di cui al primo paragrafo, pur soddisfacendo quelli del secondo paragrafo (articolo 3, paragrafo 5)

Invece, se un'impresa soddisfa i requisiti qualitativi ma non quelli quantitativi, il Regolamento riconosce il potere alla Commissione di determinare la necessità di un'indagine di mercato volta a individuare tale impresa come potenziale gatekeeper.⁷⁶⁷

In ogni caso, la qualifica di gatekeeper è sottoposta a un esame periodico a mente dell'articolo 4.

È stato notato che le definizioni si prestano a un ragionamento di tipo circolare: le imprese gatekeeper forniscono necessariamente un servizio di piattaforma di base e sembra che un servizio di piattaforma ottenga lo status di servizio di tale tipo quando viene fornito da un'impresa gatekeeper.⁷⁶⁸

I criteri qualitativi e quantitativi descritti dall'articolo 3 possono essere ricondotti alla teoria tradizionale che vede le piattaforme digitali come operatori intermediari dei mercati bilaterali.⁷⁶⁹ Nei mercati bilaterali, il valore economico aumenta all'aumentare del numero delle connessioni e scelte disponibili e, maggiore è l'effetto di rete, maggiore è la capacità dell'intermediario (quindi della piattaforma) di sfruttare la posizione di potere praticando prezzi asimmetrici.⁷⁷⁰ Tuttavia, si è recentemente diffusa l'idea per cui, accanto agli elementi che avvicinano le piattaforme alla figura degli intermediari nei mercati bilaterali, ulteriori elementi peculiari possano diversamente qualificare tali piattaforme.⁷⁷¹

Secondo Davola e Malgieri, inoltre, i criteri quantitativi utilizzati per indicare le imprese dotate di poteri di gatekeeping altro non sarebbero che i criteri tradizionalmente utilizzati per individuare il potere di mercato ai sensi dell'articolo 102 del TFUE. Tale approccio, secondo i due autori, faticherebbe a comprendere effettivamente la natura della disparità di «potere dei dati» nell'economia digitale, non riuscendo a individuare gli strumenti di correzione appropriati. Contro questo approccio tradizionale, gli autori propongono un'alternativa: la definizione del gatekeeping power dovrebbe insistere invece sul potere di alcune piattaforme di influenzare «l'architettura della scelta», ovvero di captare il consenso degli utenti in forza della presenza

⁷⁶⁷ Articolo 3, paragrafo 8.

⁷⁶⁸ N.M. Belloso, N. Petit, «The Eu Digital Markets Act, a Competition Hand in a Regulatory Glove», *European Law Review* (Forthcoming), April 5, 2023, p. 6.
SSRN: <https://ssrn.com/abstract=4411743>.

⁷⁶⁹ Per la spiegazione di tale concetto si v. paragrafo 1.3.3 del presente lavoro; per un approfondimento, si v. J. Rochet, J. Tirole, «Platform Competition in Two-Sided Markets», *Journal of the European Economic Association* 1, no. 4, 1 June 2003, pp. 990–1029. <https://doi.org/10.1162/154247603322493212>.

⁷⁷⁰ S. Wismer, C. Bongard, A. Rasek, «Multi-Sided Market Economics in Competition Law Enforcement», *Journal of European Competition Law & Practice* 8, no. 4, 1 April 2017, pp. 257-262. <https://doi.org/10.1093/jeclap/lpw082>.

⁷⁷¹ Ex multis, si v. G. Luchetta, «Is the Google Platform a Two-Sided Market?», *Journal of Competition Law & Economics* 10, no. 1, 1 March 2014, pp. 185–207. <https://doi.org/10.1093/joclec/nht026>.

dell'effetto rete e dello stato di lock-in di questi ultimi. Per fare ciò, l'analisi sul concetto di potere nell'ambiente digitale dovrebbe includere un approccio giuridico, socio-economico, psicologico e comportamentale.⁷⁷²

In generale, la stretta corrispondenza tra l'ambito di applicazione del DMA e i giganti tecnologici dell'universo GAFAM desta l'impressione che il legislatore europeo sia partito dalle peculiari caratteristiche delle piattaforme GAFAM per individuare il criterio di gatekeeping.⁷⁷³ Secondo alcuni, la normativa potrebbe essere diversamente articolata, così da riguardare un numero più ampio di aziende: occorre infatti tenere a mente che esistono altri *player* che, nonostante non ricoprano ancora una posizione dominante nei mercati di riferimento, potrebbero rapidamente veder crescere il proprio potere di mercato grazie all'effetto rete.⁷⁷⁴

4.5.2 Gli obblighi delle piattaforme con gatekeeping power

Similmente a una legge in materia di concorrenza, il DMA impone degli obblighi di carattere proibitivo alle piattaforme con gatekeeping power, ma si discosta dall'approccio tradizionale in materia di normativa antitrust nella parte in cui impone anche obblighi di carattere prescrittivo, agendo dunque *ex ante*.⁷⁷⁵

Gli articoli rilevanti per conoscere gli obblighi delle piattaforme gatekeeper sono enunciati dagli articoli 5, 6 e 7 del DMA. Si noti una prima peculiarità: gli obblighi di cui all'articolo 6 potranno essere «*oggetto di ulteriori specifiche a norma dell'articolo 8*». A parte questa distinzione generale, il testo del DMA non opera nessuna ulteriore distinzione tra i numerosi obblighi imposti.

Belloso e Petit hanno proposto una classificazione degli obblighi del DMA a seconda che questi rispondano all'interesse di controllare l'esclusione delle imprese concorrenti tramite la restrizione della concorrenza, l'abuso di posizione dominante o garantire la trasparenza delle operazioni dei gatekeeper.⁷⁷⁶

Gli obblighi finalizzati a controllare eventuali pratiche di esclusione delle imprese concorrenti sono i più numerosi. Le ipotesi di concorrenza⁷⁷⁷ previste dal DMA sono la concorrenza tra piattaforme, all'interno delle piattaforme e, secondo gli autori prima citati, al di fuori della piattaforme.⁷⁷⁸ Un'attenzione alla concorrenza tra piattaforme e all'interno della piattaforma è argomentata a partire dal Considerando numero 32: «*gli*

⁷⁷² Si v. A. Davola, G. Malgieri, «Data, Power and Competition Law: The (Im)Possible Mission of the DMA?», *Research in Law and Economics*, June 9, 2022.

<https://ssrn.com/abstract=4242574>.

⁷⁷³ N.M. Belloso, N. Petit, «The Eu Digital Markets Act, a Competition Hand in a Regulatory Glove», *European Law Review* (Forthcoming), April 5, 2023, p. 12.

<https://ssrn.com/abstract=4411743>.

⁷⁷⁴ P.G. Picht, H. Richter, «EU Digital Regulation 2022: Data Desiderata», *GRUR International*, Volume 71, Issue 5, May 2022, pp. 395–402, p. 400-401.

<https://doi.org/10.1093/grurint/ikac021>.

⁷⁷⁵ *Ibidem*, p. 12.

⁷⁷⁶ *Ibidem*, p. 14.

⁷⁷⁷ Per un approfondimento sui diversi modelli di concorrenza, si v., *Joined Cases 56 and 58-64, Établissements Consten S.à.R.L. and Grundig-Verkaufs-GmbH v Commission of the European Economic Community* [1966] ECR I-299, par.342.

⁷⁷⁸ N.M. Belloso, N. Petit, «The Eu Digital Markets Act, a Competition Hand in a Regulatory Glove», p. 14.

obblighi dovrebbero inoltre riguardare le situazioni in cui la posizione del gatekeeper potrebbe essere consolidata in misura tale che la concorrenza tra piattaforme non risulti efficace a breve termine, indicando la necessità di creare o incrementare la concorrenza all'interno delle piattaforme».

Più nello specifico, la concorrenza tra piattaforme si verifica tra una piattaforma gatekeeper e altre piattaforme per la fornitura di servizi di piattaforma di base agli utenti commerciali e finali. La concorrenza all'interno della piattaforma avviene invece tra gli utenti commerciali di servizi di piattaforma di base che sono impegnati nella stessa linea di commercio con gli utenti finali. La concorrenza al di fuori delle piattaforme, invece, si sviluppa tra le piattaforme gatekeeper e le terze parti per le vendite al di fuori di un servizio di piattaforma di base.⁷⁷⁹

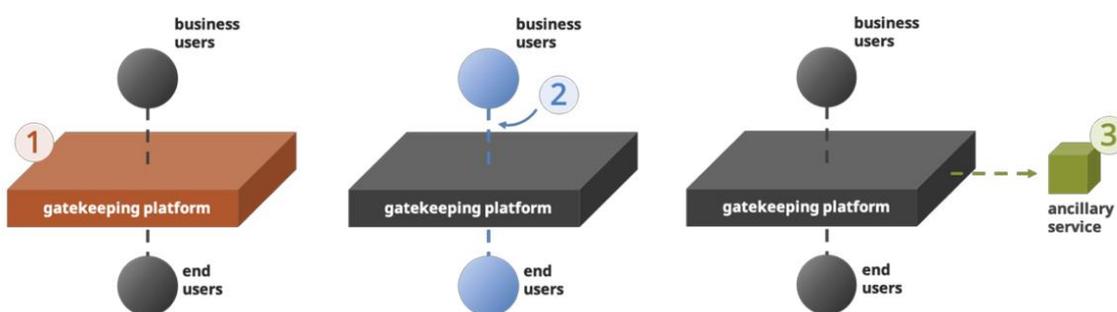


Figura 10: Rappresentazione grafica dei tre tipi di concorrenza descritti dal DMA.
 FONTE: N.M. Belloso, N. Petit, «The Eu Digital Markets Act, a Competition Hand in a Regulatory Glove», *European Law Review (Forthcoming)*, 5 aprile 2023, p. 16
<https://ssrn.com/abstract=4411743>

Secondo l'analisi degli autori prima citati, uno degli obblighi previsti per evitare pratiche finalizzate a escludere la concorrenza tra piattaforme è, a titolo esemplificativo, quello previsto dall'articolo 6 paragrafo 4 prevede che il gatekeeper:

«consente, anche a livello tecnico, l'installazione e l'uso effettivo di applicazioni software o di negozi di applicazioni software di terzi che utilizzano il suo sistema operativo o che sono interoperabili con esso e consente l'accesso a tali applicazioni software o negozi di applicazioni software con mezzi diversi dai pertinenti servizi di piattaforma di base di tale gatekeeper. Il gatekeeper, se del caso, non impedisce che le applicazioni software scaricate o i negozi di applicazioni software di terzi chiedano agli utenti finali di decidere se desiderano impostare come predefiniti tale applicazione software scaricata o tale negozio di applicazioni software. Il gatekeeper consente, a livello tecnico, agli utenti finali che decidono di impostare come predefiniti tale applicazione software scaricata o tale negozio di applicazioni software di effettuare facilmente tale modifica».

⁷⁷⁹ Ibidem, p. 14-15.

In generale, tale articolo mette al centro il concetto di interoperabilità, al fine di ridurre le barriere all'ingresso per nuove imprese concorrenti.⁷⁸⁰

Ancora, l'articolo 6, paragrafo 9, per cui:

«il gatekeeper fornisce, su richiesta e a titolo gratuito, agli utenti finali e a terzi autorizzati da un utente finale l'effettiva portabilità dei dati forniti dall'utente finale o generati mediante l'attività dell'utente finale nel contesto dell'utilizzo del pertinente servizio di piattaforma di base, anche fornendo a titolo gratuito strumenti per agevolare l'effettivo esercizio di tale portabilità dei dati, nonché fornendo un accesso continuo e in tempo reale a tali dati».

Per quanto riguarda invece gli obblighi finalizzati a evitare condotte che escludano la concorrenza all'interno della piattaforma, essi riguardano principalmente le imprese che operano sia da intermediari tra imprese e utenti finali, sia che competono con gli utenti commerciali.⁷⁸¹ Per evitare che tali piattaforme con poteri di gatekeeping utilizzino questa posizione privilegiata nei confronti degli utenti commerciali, il DMA prevede, *ex multis*, l'obbligo di cui all'articolo 6, paragrafo 5 e 7, in particolare:

«5. Il gatekeeper non garantisce un trattamento più favorevole, in termini di posizionamento e relativi indicizzazione e crawling, ai servizi e prodotti offerti dal gatekeeper stesso rispetto a servizi o prodotti analoghi di terzi. Il gatekeeper applica condizioni trasparenti, eque e non discriminatorie a tale posizionamento; (...)

7. Il gatekeeper consente, a titolo gratuito, ai fornitori di servizi e ai fornitori di hardware l'effettiva interoperabilità, nonché l'accesso ai fini dell'interoperabilità, con le stesse componenti hardware e software che sono disponibili per i servizi o l'hardware forniti dal gatekeeper e alle quali si accede o che sono controllate tramite il sistema operativo o l'assistente virtuale elencati nella decisione di designazione a norma dell'articolo 3, paragrafo 9. Inoltre, il gatekeeper consente, a titolo gratuito, agli utenti commerciali e ai fornitori alternativi di servizi forniti contestualmente o in ausilio ai servizi di piattaforma di base, l'effettiva interoperabilità, nonché l'accesso ai fini dell'interoperabilità, con lo stesso sistema operativo e le stesse componenti hardware o software che sono disponibili per il gatekeeper, o da esso utilizzati, al momento della fornitura di tali servizi, a prescindere dal fatto che tali componenti siano parte del sistema operativo».⁷⁸²

Infine, il DMA evita che una piattaforma con gatekeeping power escluda la concorrenza al di fuori delle piattaforme grazie, ad esempio, all'articolo 5 paragrafo 2, per cui il gatekeeper:

«a) non tratta, ai fini della fornitura di servizi pubblicitari online, i dati personali degli utenti finali che utilizzano servizi di terzi che si avvalgono di servizi di piattaforma di base del gatekeeper; b) non combina dati personali

⁷⁸⁰ Ibidem, p. 16-17.

⁷⁸¹ Un esempio è Amazon: esso è sia intermediario tra imprese e utenti, sia compete con gli utenti commerciali.

⁷⁸² N.M. Belloso, N. Petit, «The Eu Digital Markets Act, a Competition Hand in a Regulatory Glove», p. 18.

provenienti dal pertinente servizio di piattaforma di base con dati personali provenienti da altri servizi di piattaforma di base o da eventuali ulteriori servizi forniti dal gatekeeper o con dati personali provenienti da servizi di terzi⁷⁸³; c) non utilizza in modo incrociato dati personali provenienti dal pertinente servizio di piattaforma di base in altri servizi forniti separatamente dal gatekeeper, compresi altri servizi di piattaforma di base, e viceversa; e d) non fa accedere con registrazione gli utenti finali ad altri servizi del gatekeeper al fine di combinare dati personali, a meno che sia stata presentata all'utente finale la scelta specifica e quest'ultimo abbia dato il proprio consenso ai sensi dell'articolo 4, punto 11), e dell'articolo 7 del regolamento (UE) 2016/679. Se l'utente finale ha negato o revocato il consenso prestato ai fini del primo comma, il gatekeeper non ripete la sua richiesta di consenso per la stessa finalità più di una volta nell'arco di un anno. Il presente paragrafo lascia impregiudicata la possibilità per il gatekeeper di avvalersi dell'articolo 6, paragrafo 1, lettere c), d) ed e), del regolamento (UE) 2016/679, se del caso».⁷⁸⁴

Per quanto riguarda le misure finalizzate a ostacolare l'abuso di posizione dominante, molti degli obblighi previsti sono finalizzati a evitare uno sfruttamento degli utenti da parte delle piattaforme gatekeeper, in un'ottica più regolamentare che propria di una legge sulla concorrenza.⁷⁸⁵ Un esempio si legge all'articolo 5, paragrafo 2:

«Il gatekeeper non utilizza, in concorrenza con gli utenti commerciali, dati non accessibili al pubblico generati o forniti da tali utenti commerciali nel quadro del loro utilizzo dei pertinenti servizi di piattaforma di base o dei servizi forniti contestualmente o in ausilio ai pertinenti servizi di piattaforma di base, compresi i dati generati o forniti dai clienti di tali utenti commerciali».

L'ultima finalità degli obblighi previsti dal DMA è quella di garantire la trasparenza, il cui collegamento con la concorrenza è sancito da Considerando 72:

«garantire un livello adeguato di trasparenza delle pratiche di profilazione di cui si avvalgono i gatekeeper, compresa, a titolo esemplificativo, la profilazione ai sensi dell'articolo 4, punto 4), del regolamento (UE) 2016/679, agevola la contendibilità dei servizi di piattaforma di base. La trasparenza esercita una pressione esterna sui gatekeeper affinché non rendano la profilazione approfondita dei consumatori una norma del settore, dato che i potenziali concorrenti o le start-up non possono accedere ai dati in una misura e con un'accuratezza analoghe, né su una scala paragonabile. Una maggiore trasparenza dovrebbe consentire alle altre imprese che forniscono servizi di piattaforma di base di differenziarsi meglio attraverso l'uso di maggiori garanzie della privacy».

Risponde a tale esigenza, a titolo esemplificativo, l'articolo 14, che obbliga le piattaforme gatekeeper a informare la Commissione di qualsiasi progetto di concentrazione

⁷⁸³ Tale pratica, come visto, era stata già sanzionata dalla Commissione, si v. paragrafo 4.4.1 del presente lavoro.

⁷⁸⁴ N.M. Belloso, N. Petit, «The Eu Digital Markets Act, a Competition Hand in a Regulatory Glove», p. 19.

⁷⁸⁵ Ibidem.

«qualora le entità partecipanti alla concentrazione o l'oggetto della concentrazione forniscano servizi di piattaforma di base o qualsiasi altro servizio nel settore digitale o consentano la raccolta di dati, a prescindere dal fatto che sia notificabile alla Commissione a norma di tale regolamento o a un'autorità nazionale della concorrenza competente ai sensi delle norme nazionali sulle concentrazioni»,

oppure l'articolo 15, che prevede che il gatekeeper presenti *«alla Commissione entro sei mesi dalla sua designazione a norma dell'articolo 3 una descrizione sottoposta a audit indipendente delle tecniche di profilazione dei consumatori applicate dal gatekeeper ai suoi servizi di piattaforma di base»*, così da mettere a disposizione del pubblico una panoramica di tale descrizione, pur potendo tener conto delle esigenze legate al rispetto dei segreti aziendali.⁷⁸⁶

4.6 Altri interventi normativi dell'Unione europea nell'ambito della strategia europea dei dati: cenni

Il Digital Markets Act si colloca all'interno di un più ampio quadro di interventi dell'Unione europea finalizzati a rispondere alle trasformazioni dell'economia e della società dovute all'innovazione nell'ambito delle tecnologie digitali. Il 19 febbraio 2020, la Commissione europea ha infatti presentato la Comunicazione dell'adozione di una *«strategia europea dei dati»*.⁷⁸⁷ Questa strategia *«mira a far acquisire all'UE una posizione di leadership nella società basata sui dati. La creazione di un mercato unico consentirà ai dati di circolare liberamente all'interno dell'UE e in tutti i settori a vantaggio delle imprese, dei ricercatori e delle pubbliche amministrazioni»*.⁷⁸⁸ Tale obiettivo viene perseguito senza dimenticare che la protezione dei dati, soprattutto quelli personali, rappresenta un diritto fondamentale del cittadino, infatti

«in una società in cui è in costante aumento la quantità di dati generati dai singoli cittadini, la metodologia di raccolta e utilizzo di tali dati deve porre al primo posto gli interessi delle persone, conformemente ai valori, ai diritti fondamentali e alle norme europee.(...) L'Europa digitale dovrebbe riflettere le migliori qualità europee ed essere aperta, equa, diversificata, democratica e sicura».⁷⁸⁹

La strategia contribuisce a realizzare la visione di un autentico mercato unico dei dati, al fine di affrontare i problemi individuati mediante misure strategiche basate su quattro pilastri: (i) un quadro di governance intersettoriale per l'accesso ai dati e il loro utilizzo; (ii) investimenti nei dati e rafforzamento delle infrastrutture e delle capacità

⁷⁸⁶ Ibidem, p.20-21.

⁷⁸⁷ Commissione europea, comunicazione al Parlamento europeo, al Consiglio, al Comitato Economico e Sociale europeo e al Comitato delle regioni, «Una strategia europea dei dati», 19 febbraio 2020, consultabile al link:

<https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A52020DC0066>.

⁷⁸⁸ Sito web di riferimento, consultabile al link: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_it.

⁷⁸⁹ Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato Economico e Sociale europeo e al Comitato delle regioni, «Una strategia europea dei dati», 19 febbraio 2020, p.1.

europee per l'hosting, l'elaborazione e l'utilizzo dei dati, l'interoperabilità; (iii) fornire strumenti alle persone, investire nelle competenze e nelle piccole e medie imprese; (iv) spazi comuni europei di dati in settori strategici e ambiti di interesse pubblico.⁷⁹⁰ L'Unione europea si pone l'obiettivo di diventare «*un modello di riferimento per una società che, grazie ai dati, dispone di strumenti per adottare decisioni migliori, a livello sia di imprese sia di settore pubblico*».⁷⁹¹

La Commissione, riconoscendo che un ridotto numero di imprese tecnologiche, le cosiddette *Big Tech*, detiene attualmente una buona parte dei dati a livello mondiale, e il rischio che ciò riduca gli incentivi per le aziende basate sui dati che oggi devono emergere, crescere e innovare nell'UE, descrive la sua visione come la necessità di perseguire l'obiettivo di:

*«creare uno spazio unico europeo di dati – un autentico mercato unico di dati, aperto ai dati provenienti da tutto il mondo – nel quale sia i dati personali sia quelli non personali, compresi i dati commerciali sensibili, siano sicuri e le imprese abbiano facilmente accesso a una quantità pressoché infinita di dati industriali di elevata qualità, che stimolino la crescita e creino valore, riducendo nel contempo al minimo la nostra impronta di carbonio e ambientale. Dovrebbe trattarsi di uno spazio nel quale il diritto dell'UE possa essere applicato con efficacia e nel quale tutti i prodotti e i servizi basati sui dati siano conformi alle pertinenti normative del mercato unico dell'UE.»*⁷⁹²

La bussola dell'azione della Commissione è rappresentata dall'obiettivo della tutela della concorrenza e dall'*acquis* della libera circolazione, che rimangono al centro di una serie di norme che declinano la strategia europea dei dati con riferimento a specifici settori: il Digital Markets Act, come visto, si occupa delle piattaforme e della concorrenza, il Digital Services Act attenziona il fenomeno delle reti e dei servizi, il Digital Governance Act auspica la condivisione dei dati personali e non personali fra settore pubblico e privato e il Data Act, come una sorta di *summa*, si occupa dell'accessibilità al valore rappresentato dai dati.⁷⁹³

4.6.1 Il Digital Services Act

Con il Regolamento UE numero 2065 del 2022, l'Unione europea si dota di un ulteriore insieme di norme volte a disciplinare i servizi digitali, che, assieme al DMA, ha l'obiettivo di: «*(i) creare uno spazio digitale più sicuro in cui siano tutelati i diritti fondamentali di tutti gli utenti dei servizi digitali; (ii) creare condizioni di parità per*

⁷⁹⁰ Ibidem, p. 13 e ss.

⁷⁹¹ Ibidem, p. 1.

⁷⁹² Ibidem, p. 5.

⁷⁹³ G. Cerrina Feroni, «Luci e ombre della Data Strategy europea», Autorità Garante per la protezione dei dati personali per Agenda Digitale, 13 maggio 2022, p. 2, consultabile al link: <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9769786> oppure a: <https://www.agendadigitale.eu/cultura-digitale/cerrina-feroni-garante-privacy-luci-e-ombre-della-data-strategy-europea/>.

*promuovere l'innovazione, la crescita e la competitività, sia nel mercato unico europeo che a livello globale».*⁷⁹⁴

Il Digital Services Act (DSA) è stato pubblicato nella Gazzetta ufficiale il 25 ottobre 2022, è entrato in vigore il 16 novembre del 2022 e sarà applicabile in tutta l'UE dal 17 febbraio 2024 (articolo 93 DSA).

L'ambito di applicazione del nuovo Regolamento è descritto dall'articolo 2, paragrafo 1: *«il presente regolamento si applica ai servizi intermediari offerti a destinatari il cui luogo di stabilimento si trova nell'Unione o che sono ubicati nell'Unione, indipendentemente dal luogo di stabilimento dei prestatori di tali servizi intermediari».* La definizione di servizio intermedio viene invece fornita dall'articolo 3 lettera g), rubricato appunto «definizioni». Per servizio intermedio si intende uno dei seguenti servizi della società dell'informazione⁷⁹⁵: (i) semplice trasporto o *«mere conduit»*; (ii) memorizzazione temporanea (*«caching»*); (iii) memorizzazione di informazione (*«hosting»*).

Entro il 17 febbraio 2023, le piattaforme online e i motori di ricerca hanno dovuto pubblicare il numero di loro utenti attivi. Se questi superano i 45 milioni di utenti, tali piattaforme o motori di ricerca sono designate dalla Commissione come piattaforma online o motore di ricerca di dimensioni molto grandi (*Very Large Online Platforms, VLOPs e Very Large Online Search Engines, VLOSE*). Il DSA adotta dunque una struttura a più livelli, prevedendo obblighi maggiori per i servizi intermediari con un ruolo più importante.⁷⁹⁶ Dalla designazione, le piattaforme e i motori di ricerca hanno quattro mesi per conformarsi agli obblighi del DSA.

Tra gli elementi di novità particolarmente lodevoli,⁷⁹⁷ vi è un importante passo in avanti in materia di trasparenza. In particolare, l'articolo 14 è dedicato ai termini e alle condizioni, che, redatti in un linguaggio *«chiaro, semplice, comprensibile, facilmente fruibile e privo di ambiguità»* e resi disponibili al pubblico in un formato facilmente accessibile e leggibile meccanicamente, devono includere *«informazioni sulle restrizioni che impongono in relazione all'uso dei loro servizi per quanto riguarda le informazioni fornite dai destinatari del servizio»*, includendo anche *«le politiche, le procedure, le misure e gli strumenti utilizzati ai fini della moderazione dei contenuti, compresi il processo decisionale algoritmico e la verifica umana, nonché le regole procedurali del loro sistema interno di gestione dei reclami»*.

⁷⁹⁴ «Il pacchetto della legge sui servizi digitali», sito web della Commissione europea, disponibile al link: <https://digital-strategy.ec.europa.eu/it/policies/digital-services-act-package>.

⁷⁹⁵ La definizione di servizio della società dell'informazione accolta è quella prevista dall'articolo 1, paragrafo 1, lett. b) della direttiva (UE) 2015/1535: *«qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi»*.
[/https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32015L1535](https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32015L1535).

⁷⁹⁶ A. Strowel, L. Somaini, «Towards a Robust Framework for Algorithmic Transparency to Tackle the Dissemination of Illegal and Harmful Content on Online Platforms», CRIDES Working Paper, 2021.
https://cdn.uclouvain.be/groups/cms-editors-crides/droit-intellectuel/CRIDES_WP_2_2021_Alain%20Strowel%20and%20Laura%20Somaini.pdf.

⁷⁹⁷ G. Scorza, «Digital Services Act: Le luci e le poche ma gravi ombre delle nuove regole UE», Autorità Garante per la protezione dei dati personali per Agenda Digitale, 28 aprile 2022, p. 1 e ss, consultabile al link:
<https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9765212>.

Particolari obblighi di trasparenza sono previsti anche in materia di pubblicità, potenzialmente idonei a rappresentare un primo passo in avanti rispetto alla ricerca di una soluzione per le criticità descritte nel primo capitolo: l'utente quale consumatore è posto nelle condizioni di meglio orientare le sue scelte d'acquisto grazie alla possibilità di conoscere le logiche sottostanti alle inserzioni pubblicitarie e ai contenuti proposti. Ai sensi dell'articolo 26, infatti, i fornitori di piattaforme online devono provvedere affinché i destinatari del servizio possano identificare «*in modo chiaro, conciso, inequivocabile e in tempo reale*»: i) che l'informazione costituisce una pubblicità; ii) la persona fisica o giuridica per conto della quale viene presentata la pubblicità; iii) la persona fisica o giuridica che paga per la pubblicità, se diversa da quella per conto della quale la pubblicità è presentata; iv) informazioni rilevanti relative ai parametri utilizzati per determinare il destinatario al quale viene presentata la pubblicità.

Anche le criticità legate alla possibilità che le logiche del capitalismo della sorveglianza creino una «bolla» in cui vengono mostrati all'utente informazioni e contenuti accuratamente scelti grazie a sofisticati meccanismi di profilazione,⁷⁹⁸ trovano una potenziale soluzione nel DSA, in particolare all'articolo 27, rubricato «*trasparenza dei sistemi di raccomandazione*», che postula l'obbligo in capo alle piattaforme online di specificare «*in un linguaggio chiaro e intellegibile, i principali parametri utilizzati nei loro sistemi di raccomandazione, nonché qualunque opzione a disposizione dei destinatari del servizio che consente loro di modificare o influenzare tali parametri principali*».

Questi obblighi di trasparenza potrebbero provarsi particolarmente utili nel correggere il funzionamento delle piattaforme in modo da limitare la diffusione di disinformazione.⁷⁹⁹ Il DSA, infatti, contiene diversi riferimenti alla necessità di contrastare la disinformazione. Al Considerando numero 2, essa è considerata un «*rischio per la società*», mentre al Considerando numero 9 viene enunciato l'obiettivo

⁷⁹⁸ Preoccupazioni simili sono condivise anche dal DSA al Considerando 70: «*Un elemento essenziale dell'attività di una piattaforma online consiste nel modo in cui le informazioni sono messe in ordine di priorità e presentate nella sua interfaccia online per facilitare e ottimizzare l'accesso alle stesse da parte dei destinatari del servizio. Ciò avviene, ad esempio, suggerendo, classificando e mettendo in ordine di priorità le informazioni in base ad algoritmi, distinguendole attraverso testo o altre rappresentazioni visive oppure selezionando in altro modo le informazioni fornite dai destinatari. Tali sistemi di raccomandazione possono avere un impatto significativo sulla capacità dei destinatari di recuperare e interagire con le informazioni online, anche per facilitare la ricerca di informazioni pertinenti per i destinatari del servizio e contribuire a migliorare l'esperienza dell'utente. Essi svolgono inoltre un ruolo importante nell'amplificazione di determinati messaggi, nella diffusione virale delle informazioni e nella sollecitazione del comportamento online. Di conseguenza, le piattaforme online dovrebbero provvedere in modo coerente affinché i destinatari del loro servizio siano adeguatamente informati del modo in cui i sistemi di raccomandazione incidono sulle modalità di visualizzazione delle informazioni e possono influenzare il modo in cui le informazioni sono presentate loro. Esse dovrebbero indicare chiaramente i parametri di tali sistemi di raccomandazione in modo facilmente comprensibile per far sì che i destinatari del servizio comprendano la modalità con cui le informazioni loro presentate vengono messe in ordine di priorità. Tali parametri dovrebbero includere almeno i criteri più importanti per determinare le informazioni suggerite al destinatario del servizio e i motivi della rispettiva importanza, anche nel caso in cui le informazioni siano classificate in ordine di priorità sulla base della profilazione e del suo comportamento online.*».

⁷⁹⁹ A. Strowel, J. De Meyere, «The Digital Services Act: transparency as an efficient tool to curb the spread of disinformation on online platforms?», JIPITEC 66 para 1, 14, 2023, pp. 66-87, p.7. <https://www.jipitec.eu/issues/jipitec-14-1-2023/5708>.

di «*garantire un ambiente online sicuro, prevedibile e affidabile, in cui i diritti fondamentali sanciti dalla Carta siano efficacemente tutelati e l'innovazione sia agevolata, contrastando la diffusione di contenuti illegali online e i rischi per la società che la diffusione della disinformazione o di altri contenuti può generare*». Particolarmente significativo è anche il Considerando 84, in cui è chiesto ai VLOPs di

«concentrarsi anche sulle informazioni che non sono illegali ma contribuiscono ai rischi sistemici individuati nel presente regolamento. Tali fornitori dovrebbero pertanto prestare particolare attenzione al modo in cui i loro servizi sono utilizzati per diffondere o amplificare contenuti fuorvianti o ingannevoli, compresa la disinformazione».

Tale Considerando, infatti, affianca all'obbligo di contrastare senza ritardo i contenuti illegali quando vi sia stata una richiesta dalle autorità giudiziarie o amministrative competenti ai sensi dell'articolo 9 un'attenzione anche alla dimensione della mera disinformazione.

Il raggiungimento di tale obiettivo gioverebbe anche il mondo dell'istruzione: gli studenti avrebbero accesso a informazioni certamente più attendibili, che possono garantire loro lo sviluppo di un pensiero critico autonomo e non influenzato da pratiche poco trasparenti.

Degna di nota è inoltre l'attenzione data ai minori,⁸⁰⁰ protagonisti delle criticità legate alle attività didattiche svolte grazie all'ausilio delle grandi piattaforme. Nei confronti di questi ultimi è vietata la pubblicità mirata basata sul trattamento dei dati personali, recita infatti l'articolo 28, paragrafo 2:

«i fornitori di piattaforme online non presentano sulla loro interfaccia pubblicità basata sulla profilazione come definita all'articolo 4, punto 4), del regolamento (UE) 2016/679 che usa i dati personali del destinatario del servizio se sono consapevoli, con ragionevole certezza, che il destinatario del servizio è minore».

Questo è un passo in avanti da non sottovalutare: l'utilizzo di una piattaforma per finalità didattiche da parte di un istituto scolastico può, «*con ragionevole certezza*», rendere edotti i fornitori di piattaforme online del trattamento di dati personali di minori, vietando dunque la profilazione ai fini di pubblicità personalizzata. Dunque, anche se tale previsione non è pensata per il mondo della didattica, la spiccata attenzione nei confronti dei minori può comunque rappresentare un importante punto di riferimento per la tutela dell'autodeterminazione dei minori durante il progressivo spostamento verso un'«istruzione delle piattaforme».

Prima dell'approvazione del testo definitivo, la League of European Research Universities (LERU) aveva sollevato importanti perplessità relative al rischio che il DSA includesse, nel suo ambito di applicazione, anche le Università, gli archivi e le altre istituzioni accademiche,⁸⁰¹ imponendo dunque nuovi obblighi. Il richiamo alla direttiva

⁸⁰⁰G. Scorza, «Digital Services Act: Le luci e le poche ma gravi ombre delle nuove regole UE», p. 2.

⁸⁰¹ Si v. League of European Research Universities, «LERU says NO to the Digital Services Act», 5 aprile 2022, consultabile al link: <https://www.leru.org/news/leru-says-no-to-the-digital-services-act>.

UE 1535 del 2015, che definisce i servizi della società dell'informazione come servizi dietro retribuzione, sembrerebbe escludere la realtà universitaria dall'ambito di applicazione del DSA.⁸⁰² I dubbi tuttavia permangono, dal momento che le realtà sopra menzionate possono comunque svolgere un'attività di tipo economico. In questo caso, la Commissione europea chiarisce che la valutazione andrà fatta caso per caso, con esiti potenzialmente differenti tra gli Stati membri.⁸⁰³ La Commissione riconosce il processo di transizione che sta riguardando il mondo universitario e accademico che, come precedentemente descritto, sta andando da un'economia basata sulla fornitura dei contenuti verso una orientata all'analisi dei dati, pertanto non esclude l'applicazione futura del DSA anche al mondo universitario. Sono particolarmente significative le parole utilizzate dalla Commissione:

*«Through the seamless provision of these services, companies with clients in higher education can invisibly and strategically influence, and perhaps exert control over, key university decisions – ranging from student assessments to research integrity to financial planning. Data about students, faculties, research outputs, institutional productivity and more have a potential for enormous competitive value. Data analytics is a potential multibillion dollar market (perhaps multi-trillion, when the value of intellectual property is factored in), but data capture and use by companies could significantly reduce institutions' and scholars' rights to their data and related intellectual property. A set of companies is moving aggressively to capitalise on this and thus many data from the universities and academia in general could soon be provided as an economic activity through public-private partnerships or by intermediaries. Hence, much data generated by universities and academia could – at least in the future – be encompassed by the proposed DSA should the data be available or used as input for intermediate services as defined in the DSA».*⁸⁰⁴

4.6.2 Il Data Governance Act e la proposta del Data Act

I due Regolamenti rappresentano un tentativo di dettare le prime regole in materia di monetizzazione dei dati.⁸⁰⁵

⁸⁰²Commissione europea, Study on the Digital Services Act and the Digital Markets Act and their possible impact on research, 2022, p. 13: «When universities, repositories and other academic institutions based on legal requirements are creating, collecting and storing data in databases or on platforms for sharing or re-using data, they should not generally be considered providing economic or commercial services» Si v. il link:

<https://op.europa.eu/en/publication-detail/-/publication/49677a41-1144-11ed-8fa0-01aa75ed71a1/language-en/format-PDF/source-262356279>.

⁸⁰³ Ibidem, p. 9: «It should be clear that the pDSA can apply to data-driven university or repository services that provide an economic activity of hosting services for research results. Determining if such a service is a public service or constitutes an economic activity requires case-by-case analysis». Si v. anche p. 19: «The outcome of such analyses can differ from Member State to Member State, from university to university, from repository to repository and from service to service».

⁸⁰⁴ Ibidem, p. 10.

⁸⁰⁵ G. Scorza, «Digital Services Act: Le luci e le poche ma gravi ombre delle nuove regole UE», p. 5.

Il Data Governance Act (DGA) è entrato in vigore il 23 giugno 2020 e sarà applicabile a decorrere dal 24 settembre 2023.⁸⁰⁶

Il DGA è uno strumento intersettoriale, che persegue l'obiettivo di rendere disponibili più dati, tanto personali quanto non personali, regolando il riutilizzo di dati pubblici e protetti, aumentando la condivisione di dati attraverso la regolamentazione di nuovi intermediari e incoraggiando la condivisione dei dati a scopi altruistici.⁸⁰⁷ Un ruolo centrale è dunque ricoperto dal concetto di «altruismo dei dati», a cui è dedicato il capo IV del Regolamento, ovvero

*«la condivisione volontaria di dati sulla base del consenso accordato dagli interessati al trattamento dei dati personali che li riguardano, o sulle autorizzazioni di altri titolari dei dati volte a consentire l'uso dei loro dati non personali, senza la richiesta o la ricezione di un compenso che vada oltre la compensazione dei costi sostenuti per mettere a disposizione i propri dati, per obiettivi di interesse generale, stabiliti nel diritto nazionale, ove applicabile, quali l'assistenza sanitaria, la lotta ai cambiamenti climatici, il miglioramento della mobilità, l'agevolazione dell'elaborazione, della produzione e della divulgazione di statistiche ufficiali, il miglioramento della fornitura dei servizi pubblici, l'elaborazione delle politiche pubbliche o la ricerca scientifica nell'interesse generale».*⁸⁰⁸

Ai sensi dell'articolo 3, il riutilizzo di determinate categorie di dati detenuti da enti pubblici protetti da riservatezza commerciale, riservatezza statistica, proprietà intellettuale o protezione dei dati personali non rientranti nella direttiva UE 2019/2024, non riguarda i dati detenuti da enti culturali e di istruzione. Pertanto, i dati delle istituzioni universitarie e scolastiche prodotti durante la didattica a distanza sembrano non rientrare tra quelli riutilizzabili ai sensi del presente Regolamento.

Il DGA, all'articolo 2, numero 11, introduce anche il concetto di «servizio di intermediazione dei dati», ovvero

«un servizio che mira a instaurare, attraverso strumenti tecnici, giuridici o di altro tipo, rapporti commerciali ai fini della condivisione dei dati tra un numero indeterminato di interessati e di titolari dei dati, da un lato, e gli utenti dei dati, dall'altro, anche al fine dell'esercizio dei diritti degli interessati in relazione ai dati personali».

Tali intermediari di dati potrebbero ricoprire un ruolo importante nella ricerca di soluzioni per i gravi fallimenti di mercato nell'economia dei dati, perché possono mettere in contatto i titolari dei dati e gli utenti, così da implementare una migliore accessibilità ai dati e ridurre le asimmetrie informative.⁸⁰⁹ Gli intermediari potrebbero dunque contribuire alla creazione di un più efficiente controllo dei dati, consentendo e

⁸⁰⁶ Si v. articolo 38 del DGA.

⁸⁰⁷ Commissione europea, «Illustrata la legge sulla governance dei dati», consultabile, al link: <https://digital-strategy.ec.europa.eu/it/policies/data-governance-act-explained>.

⁸⁰⁸ Articolo 2, numero 16) del DGA.

⁸⁰⁹ H. Richter, «Looking at the Data Governance Act and Beyond: How to Better Integrate Data Intermediaries in the Market Order for Data Sharing», GRUR International, Volume 72, Issue 5, May 2023, pp. 458–470, p. 462.

<https://doi-org.ezp.biblio.unitn.it/10.1093/grurint/ikad014>.

promuovendo la condivisione, ma al contempo impedendola quando necessario per garantire la conformità alla legge, compreso il GDPR.⁸¹⁰

Ai sensi dell'articolo 12, il fornitore di servizi di intermediazioni non può utilizzare i dati per i quali fornisce tali servizi per scopi diversi dalla messa a disposizione di tali dati agli utenti dei dati. Rimane tuttavia poco chiaro se le *Big Tech* possano o meno operare come servizi di intermediazione dei dati, e, in caso di risposta positiva, quali siano le misure idonee a garantire che non vi sia un utilizzo dei dati diverso dalla mera messa a disposizione.⁸¹¹

La proposta del Regolamento Data Act è invece arrivata a febbraio del 2022 e il 14 marzo del 2023 il Parlamento ha approvato la proposta di Regolamento, sono dunque in corso i negoziati con il Consiglio. Tale proposta riconosce il valore di risorsa fondamentale per la crescita economica dell'Unione dei dati anche non strettamente personali, mirando a potenziare, oltre ai diritti del consumatore e dell'interessato, anche quelli delle aziende medie e piccole, che spesso non sono in grado di negoziare accordi equilibrati di condivisione dei dati con soggetti più forti.⁸¹²

Gli obiettivi specifici della proposta sono: (i) facilitare l'accesso ai dati e il relativo utilizzo da parte dei consumatori e delle imprese, preservando nel contempo gli incentivi a investire in modalità di generazione del valore grazie ai dati; (ii) prevedere che enti pubblici e istituzioni, agenzie o organismi dell'Unione possano utilizzare i dati detenuti dalle imprese in determinate situazioni in cui vi sia una necessità eccezionale di dati; (iii) facilitare il passaggio tra diversi servizi cloud ed edge; (iv) adottare garanzie contro il trasferimento illecito di dati senza notifica da parte dei fornitori di servizi cloud; (v) prevedere l'elaborazione di norme di interoperabilità per il riutilizzo dei dati tra i vari settori, nel tentativo di eliminare gli ostacoli alla condivisione dei dati tra spazi comuni europei di dati specifici per settore, coerentemente con le prescrizioni di interoperabilità settoriali, e tra altri dati che non rientrano nell'ambito di uno spazio comune europeo dei dati specifico.⁸¹³

L'articolo 1 della proposta del Regolamento 1«*include nel suo ambito di applicazione i fabbricanti di prodotti e i fornitori di servizi correlati immessi sul mercato dell'Unione e agli utenti di tali prodotti o servizi*». Più nello specifico, sono inclusi «*i prodotti fisici che ottengono, generano o raccolgono, mediante i loro componenti, dati relativi alle loro prestazioni, al loro uso o al loro ambiente e che sono in grado di comunicare tali dati tramite un servizio di comunicazione elettronica accessibile al pubblico (spesso denominato "internet delle cose")*», ovvero «*veicoli, apparecchiature domestiche e beni di consumo, dispositivi medici e sanitari o macchine agricole e industriali*». ⁸¹⁴ Invece, rimangono *expressis verbis* esclusi «*determinati prodotti progettati principalmente per visualizzare o riprodurre contenuti o per registrare e trasmettere contenuti, anche per l'uso da parte di un servizio online*» quali, ad esempio, «*personal computer, server, tablet e smartphone, telecamere, webcam, sistemi di*

⁸¹⁰ Ibidem, p.465.

⁸¹¹ J.Ruohonen, S. Mickelsson, «Reflections on the Data Governance Act», DISO 2, 10,2023, p.7. <https://doi-org.ezp.biblio.unitn.it/10.1007/s44206-023-00041-7>.

⁸¹² G. Scorza, «Digital Services Act: Le luci e le poche ma gravi ombre delle nuove regole UE», p. 6.

⁸¹³ Relazione alla proposta di Regolamento del Parlamento europeo del Consiglio, si v. il link: <https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52022PC0068>.

⁸¹⁴ Si v. Considerando 14.

registrazione sonora e scanner di testo», dal momento che essi «richiedono un contributo umano per produrre varie forme di contenuto, quali documenti di testo, file audio, file video, giochi, mappe digitali». ⁸¹⁵ Tale esclusione è parsa ad alcuni incongruente, dal momento che gli odierni smartphone e tablet, controllando gli oggetti dell'IoT, si prestano a diventare un oggetto dell'universo dell'IoT stesso. ⁸¹⁶

Vista l'attuale formulazione della proposta di Data Act, le piattaforme utilizzate per fini di didattica a distanza restano escluse dall'ambito di applicazione.

Un elemento di particolare novità è rappresentato dall'articolo 5 della proposta, che obbliga il titolare dei dati a mettere a disposizione di terzi, senza indebito ritardo e con la stessa qualità di cui dispone il titolare dei dati e, ove applicabile, in modo continuo e in tempo reale, i dati generati dall'uso di un prodotto o di un servizio correlato quando pervenga una richiesta di un utente. Tale norma seguirebbe un approccio finalizzato a modellare il mercato, creando nuovi diritti paralleli e ridefinendo l'infrastruttura legale sulla quale si sviluppano i mercati. ⁸¹⁷

Il diritto all'articolo 5 si differenzia dall'articolo 20 del GDPR che prevede il diritto alla portabilità dei dati, non solo poiché la messa a disposizione deve avvenire in modo continuo e in tempo reale, ma anche perché, ai sensi del Considerando 31:

«Esso conferisce agli utenti il diritto di accedere a tutti i dati generati dall'uso di un prodotto o di un servizio correlato, e di metterli a disposizione di terzi, indipendentemente dalla loro natura di dati personali, dalla distinzione tra dati forniti attivamente o osservati passivamente e dalla base giuridica del trattamento. A differenza degli obblighi tecnici di cui all'articolo 20 del regolamento (UE) 2016/679, il presente regolamento impone e garantisce la fattibilità tecnica dell'accesso di terzi a tutti i tipi di dati che rientrano nel suo ambito di applicazione, siano essi personali o non personali».

Se è vero che anche l'articolo 6, paragrafo 9 del DMA riconosce

«agli utenti finali e a terzi autorizzati da un utente finale l'effettiva portabilità dei dati forniti dall'utente finale o generati mediante l'attività dell'utente finale nel contesto dell'utilizzo del pertinente servizio di piattaforma di base, anche fornendo a titolo gratuito strumenti per agevolare l'effettivo esercizio di tale portabilità dei dati, nonché fornendo un accesso continuo e in tempo reale a tali dati».

questo, come visto, si applica solo alle piattaforme con gatekeeping power ai sensi dell'articolo 3 dello stesso Regolamento, mentre il Data Act insiste sul diritto alla portabilità dei dati a prescindere dal potere di mercato del titolare dei dati; allo stesso tempo, tuttavia, l'ambito di applicazione della proposta del DA è ristretta ai soli dati

⁸¹⁵ Si v. Considerando 15.

⁸¹⁶ C. Gallese, «A first commentary to the proposal for a new Regulation on fair access and use of Data (Data Act)», *MediaLaws*, 3/2022, pp. 237-270, p. 245.

⁸¹⁷ H. Schweitzer, A. Metzger, «Data Access under the Draft Data Act, Competition Law and the DMA: Opening the Data Treasures for Competition and Innovation?», *GRUR International*, Volume 72, Issue 4, April 2023, pp. 337-356, p. 338.
<https://doi-org.ezp.biblio.unitn.it/10.1093/grurint/ikad012>.

generati dall'uso prodotti, mentre il DMA si applica ai dati generati dall'uso dei servizi di piattaforma di base dei gatekeeper.⁸¹⁸

Questo diritto mira dunque a evitare una situazione di lock-in, permettendo l'uso dei dati per le micro, piccole e medie imprese, garantendo una distribuzione più equa nell'economia dei dati,⁸¹⁹ soprattutto perché ai sensi dell'articolo 5, paragrafo 2, le imprese che forniscono servizi di piattaforma di base designate come *gatekeeper* ai sensi dell'articolo 3 del DMA non possono essere nominate come terzo destinatario della messa a disposizione dei dati.

4.6.3 Considerazioni di sintesi sulla strategia europea dei dati e le criticità legate alla didattica a distanza

Le norme della strategia europea in materia di dati non sono state ideate per le criticità legate all'affidamento delle attività didattiche ai capitalisti della sorveglianza, tuttavia, ponendosi l'obiettivo di dotare l'UE di una posizione di leadership nella società basata sui dati, al fine di erodere il primato delle *Big Tech* nel mercato dei dati, generano una serie di benefici per gli studenti e per tutte le parti coinvolte nel fenomeno dell'«istruzione delle piattaforme».

Il Digital Markets Act, *in primis*, con la sua attenzione alla dimensione della concorrenza tra piattaforme, insiste sull'interoperabilità, sul diritto alla portabilità dei dati e sulla necessità di abbattere le barriere all'entrata, per favorire l'ingresso di nuove imprese concorrenti. Una puntuale applicazione di tali disposizioni può permettere dunque l'ingresso di nuovi *player* che, auspicabilmente, offrano come alternativa piattaforme non proprietarie e open source per lo svolgimento delle attività didattiche da remoto.

Inoltre, perseguendo l'obiettivo di rafforzare la trasparenza circa le pratiche di profilazione di cui si avvalgono i *gatekeeper*, il DMA, quando obbliga questi ultimi a mettere a disposizione del pubblico una panoramica sulla descrizione delle tecniche di profilazione, dota in generale tutti gli utenti di maggiori possibilità di conoscere pienamente i termini dell'uso dei dati personali raccolti. Nel mondo della didattica, ciò significa poter scegliere con maggiore cautela e consapevolezza le piattaforme da utilizzare per lo svolgimento delle attività scolastiche e accademiche, optando per quelle che meno rispondono alle logiche di estrazione e accumulazione dei dati del capitalismo della sorveglianza.

Anche il Digital Services Act, insistendo sulla trasparenza in materia di pubblicità e sistemi di raccomandazione, tutela l'utente e – di riflesso – gli studenti.

La possibilità di conoscere il modo con cui gli algoritmi determinano il destinatario di una pubblicità o la condivisione prioritaria di un contenuto in luogo di altri è infatti strumentale per un pieno diritto di autodeterminazione dell'individuo e, ancor di più, dello studente. Lo studente è ulteriormente tutelato grazie all'attenzione alla disinformazione e, quando minore, grazie al divieto di pubblicità basata su profilazione.

⁸¹⁸ Ibidem, p. 344.

⁸¹⁹ Ibidem, p. 345.

Il DSA rappresenta dunque uno strumento critico per aumentare la responsabilità delle piattaforme online.⁸²⁰

Un importante ruolo nell'implementazione del principio di trasparenza spetta al recentemente fondato Centro europeo per la trasparenza algoritmica (ECAT),⁸²¹ che, con competenza scientifica e tecnica, intende lavorare a fianco della Commissione europea per vigilare sul rispetto degli obblighi previsti dal DSA, collaborando con esperti del settore, il mondo accademico e le organizzazioni della società civile, al fine di migliorare la comprensione circa il funzionamento degli algoritmi.⁸²²

L'approccio al principio di trasparenza potrebbe però spingersi ancora oltre: il legislatore potrebbe imporre un principio generale di trasparenza e un correlato diritto alla trasparenza per gli utenti delle piattaforme, così da far ricoprire alla trasparenza il ruolo di norma e non più di eccezione, al pari di quanto avviene nell'ambito delle pubbliche amministrazioni.⁸²³

Il Data Governance Act e la proposta del Data Act, invece, non rappresentano una soluzione alle criticità legate al capitalismo della sorveglianza nell'ambito della didattica a distanza. Come visto, il concetto di altruismo di dati previsto dal Data Governance Act non include i dati detenuti da enti culturali e di istruzione, pertanto si perde l'occasione di condividere i dati generati durante le attività didattiche svolte online per finalità di ricerca scientifica, così da poter implementare una migliore offerta di servizi pubblici – anche digitali – nell'ambito del settore dell'istruzione.

La proposta di Data Act, invece, applicandosi ai soli prodotti e servizi correlati, rappresenta un'occasione mancata soprattutto con riferimento al diritto di condividere i dati con terzi di cui all'articolo 5. Laddove il Data Act si applicasse anche alle piattaforme, gli utenti e gli studenti godrebbero di un importante strumento in grado di ridurre la loro condizione di lock-in nei confronti delle piattaforme delle Big Tech, permettendo l'ingresso di piccole e medie imprese europee all'interno del mercato dei servizi digitali per la didattica.

Il quadro legislativo descritto è certamente un primo approccio preliminare per gestire il potere delle piattaforme online nel mondo dell'istruzione, ma al momento manca una cornice legislativa unica che regoli le criticità specifiche legate allo svolgimento delle attività didattiche tramite il supporto delle piattaforme proprietarie.⁸²⁴

⁸²⁰ E. Celeste, G. De Gregorio, «Towards a Right to Digital Education? Constitutional Challenges of Edtech», p. 249.

⁸²¹ Commissione europea, «Sneak Peek: How the Commission Will Enforce the DSA & DMA», 5 luglio 20220, consultabile al link:

https://ec.europa.eu/commission/presscorner/detail/en/statement_22_4327.

⁸²² «Centro europeo per la trasparenza algoritmica», sito web consultabile al link: https://algorithmic-transparency.ec.europa.eu/index_en?etrans=it.

⁸²³ A. Strowel, J. De Meyere, «The Digital Services Act: transparency as an efficient tool to curb the spread of disinformation on online platforms?», p.81.

⁸²⁴ E. Celeste, G. De Gregorio, «Towards a Right to Digital Education? Constitutional Challenges of Edtech», p. 248-249.

CONCLUSIONI

«Education is the most powerful weapon which you can use to change the world».

Nelson Mandela

A parere di chi scrive, l'istruzione deve essere considerata un settore strategico sia del Paese sia dell'Unione europea. È necessario che le criticità legate alla scelta dello Stato di lasciare a oligopoli privati (per giunta, esteri) le infrastrutture necessarie per lo svolgimento delle attività didattiche vengano poste al centro del dibattito politico in materia di istruzione.

Pur potendosi oggi affermare il superamento dell'emergenza pandemica, le tecnologie care alla didattica a distanza si prestano infatti a restare un utile strumento di sussidio alle esigenze logistiche del mondo tanto scolastico quanto accademico, con il rischio di una progressiva crescita del fenomeno dell'«istruzione delle piattaforme».

Nella presente tesi si sono illustrate diverse strategie finalizzate a contenere i rischi legati all'incursione delle logiche del capitalismo della sorveglianza all'interno del mondo dell'istruzione.

In primis, coerentemente da quanto auspicato da Karen Maex, vi è la possibilità di sviluppare un'infrastruttura propria del mondo accademico e scolastico, che possa quindi contrastare la situazione di *lock-in* nei confronti delle grandi piattaforme proprietarie. In questa cornice si colloca la piattaforma *open source* del Consortium GARR, che ha conosciuto e conosce una scarsa diffusione nel mondo accademico e universitario, nonostante fosse già esistente e funzionante durante il periodo pandemico di svolgimento delle attività didattiche a distanza.

Un tentativo analogo è stato compiuto anche nel mondo della scuola con il disegno di legge, mai approvato, per la creazione di una piattaforma digitale unica per tutti i servizi e le funzionalità utili per le scuole, compresa la didattica a distanza.

La scelta di appaltare a imprese statunitensi oligopolistiche le infrastrutture per lo svolgimento delle attività didattiche, come visto, solleva peculiari criticità con riferimento anche alla sovranità digitale dell'Unione europea, intesa quale potere degli Stati membri dell'Unione di determinare autonomamente l'utilizzo e il funzionamento dei sistemi digitali, di mantenere il controllo sui dati prodotti e garantire l'accesso agli stessi. Tanto la Francia quanto il progetto Gaia-X dimostrano che è possibile implementare un'infrastruttura digitale indipendente dalle logiche del capitalismo della sorveglianza, che garantisca il controllo sui dati e un trattamento dei dati personali conforme al GDPR.

Accanto a questi interventi strutturali vi è poi il quadro normativo esistente a livello europeo. *In primis*, il GDPR, che garantisce un alto livello di protezione dei dati personali e un ampio catalogo di diritti per l'interessato ma che soprattutto limita i poteri di sorveglianza e monitoraggio, tanto delle *Big Tech* quanto dei servizi di *intelligence* stranieri, nel momento in cui sottopone a condizioni stringenti la possibilità di effettuare trasferimenti transfrontalieri di dati verso Paesi terzi. Il GDPR e il rispetto delle prescrizioni in esso contenute dovrebbero rappresentare una bussola che orienta

la scelta delle istituzioni scolastiche di utilizzare, ai fini dello svolgimento delle attività didattiche, piattaforme proprietarie.

Al GDPR si aggiunge il recentemente approvato Digital Markets Act, che tenta un approccio congiunto tra antitrust e tutela dei dati personali, riconoscendo l'idoneità di questi ultimi a rappresentare un importante *market asset* idoneo ad accrescere il potere di mercato delle imprese operanti nei mercati digitali. Anche se il DMA non è stato pensato per il mondo della didattica, una puntuale applicazione delle sue disposizioni potrebbe permettere l'ingresso all'interno del mercato dei servizi digitali per la didattica di nuovi *player*, che, auspicabilmente, offrano piattaforme non proprietarie e open source per lo svolgimento delle attività didattiche.

Più in generale, la scelta dei tribunali e delle autorità amministrative indipendenti di applicare congiuntamente la normativa a tutela dei dati personali e la disciplina antitrust può rappresentare un importante passo in avanti nella lotta all'erosione dei monopoli e oligopoli dell'universo GAFAM. Tali norme, tutelando l'utente-studente tanto quanto soggetto interessato al trattamento quanto consumatore, riescono a ridurre la condizione di vulnerabilità in cui si trovano i soggetti coinvolti dalla didattica, cagionata dallo squilibrio di potere tra questi ultimi e le piattaforme digitali e dalle pratiche di abuso di posizione dominante.

Come osservato, il legislatore europeo, con la «strategia europea dei dati» intende arricchire il quadro normativo europeo con dispositivi normativi che permettano all'Unione europea di affermarsi quale leader di una società europea basata sui dati, in cui i dati, conformemente al GDPR, alla normativa europea e ai diritti fondamentali, circolano liberamente, stimolando la crescita e producendo valore. Tra le nuove norme (DSA, DGA e proposta del Data Act), anche se non ideato specificamente per il mondo della didattica, merita sicuramente una particolare attenzione il Regolamento DSA per la sua attenzione al principio di trasparenza in materia di pubblicità e sistemi di raccomandazione di contenuti, che risulta strumentale ad un pieno diritto di autodeterminazione dell'utente e dunque anche dello studente, e per il divieto di profilazione per fini di pubblicità personalizzata quando il trattamento riguardi un minore.

Tutto ciò, però, non basta: a parere di chi scrive, spetta al legislatore europeo farsi carico del compito di garantire che il ruolo strategico dell'istruzione non venga esautorato dalle logiche di accumulazione dei dati delle grandi piattaforme.

In questa sede si condivide dunque il pensiero di Karen Maex e Matthias Bakker: il mondo delle Università sembra sfuggire dagli atti normativi della strategia europea dei dati. Sarebbe invece maggiormente auspicabile l'emanazione di un «*Digital University Act*», che fornisca un controllo pubblico sui dati dell'Università, così da riconoscerne il ruolo di infrastruttura decisiva per la società.⁸²⁵ Maex⁸²⁶ si auspica che con l'implementazione di una normativa europea che abbia al centro l'Università possa realizzarsi un mondo accademico in cui gli strumenti digitali di apprendimento e di ricerca siano sotto il controllo pubblico e su pubbliche infrastrutture. Anche laddove

⁸²⁵ K. Maex, M. Bakker, «The university in the age of platforms and algorithms», p. 45.

⁸²⁶ Si v. anche K. Maex, «Protect independent and public knowledge», discorso tenuto l'8 gennaio 2021 per il 389° *dies natalis* dell'Università di Amsterdam, consultabile al link: <https://www.eua.eu/downloads/content/speech-karen-maex---dies-2021.pdf>.

fossero necessarie parziali collaborazioni con piattaforme private, alle Università andrebbe comunque lasciato il potere di influenzare le scelte di sviluppo e controllare la raccolta e l'elaborazione dei dati degli utenti.⁸²⁷

Anche la League of European Research Universities (LERU) ritiene che il legislatore, nell'implementare nuove strategie in materia di dati personali, debba prestare particolare attenzione al rispetto dei diritti fondamentali alla libertà di ricerca e insegnamento e all'istruzione. Le Università, dal canto loro, dovrebbero condurre un'analisi strutturale dei rischi per evitare dipendenze indesiderate dai fornitori digitali nei processi di ricerca e istruzione, cercando modalità per evitare situazioni di *lock-in* verso piattaforme informatiche specifiche.⁸²⁸

Se le autorevoli argomentazioni appena riportate hanno a mente soprattutto il mondo dell'istruzione superiore, si ritiene in questa sede che tali considerazioni possano riguardare anche il mondo della scuola, e, dunque, dell'istruzione in generale: *«l'insegnamento, almeno se è inteso come paideia e non come addestramento, ha bisogno della pubblicità in senso strutturale, vale a dire in quanto partecipe di una comunità politica che si riconosca come democratica in un senso non solo propagandistico»*.⁸²⁹

⁸²⁷ M.C. Pievatolo, «I custodi del sapere», bollettino telematico di filosofia politica, 3 giugno 2021, p.4, consultabile al link: <https://zenodo.org/record/4897854>.

⁸²⁸ League of European Research Universities «LERU Data Statement», dicembre 2021, p. 2-3, consultabile al link:

<https://www.leru.org/publications/is-university-autonomy-threatened-by-eu-data-policy-and-law>.

⁸²⁹ M.C. Pievatolo, «Sulle spalle dei mercanti? Teledidattica e civiltà tecnologica», p. 20.

BIBLIOGRAFIA

Abba B., Sulaiman M., Mustapha N., Perumal T., «HMM-Based Decision Model for Smart Home Environment», *International Journal of Smart Home*, gennaio 2014.
https://www.researchgate.net/publication/284351676_HMM-

Acquisti A., Taylor C., Wagman L., «The Economics of Privacy», *Journal of Economic Literature*, 54(2),2016, pp. 442-492.

Alpa P.G., «L'identità digitale e la tutela della persona. Spunti di riflessione», *Contratto e impresa*, 3/2017, pp. 723-727.

Angiolini C., Ducato R., Giannopoulou A., Schneider G., «Remote Teaching During the Emergency and Beyond: Four Open Privacy and Data Protection Issues of 'Platformised' Education», *Opinio Juris in Comparatione*, vol. 1,2020, November 13, 2020, pp. 45-72.
<https://ssrn.com/abstract=3779238>.

Aspesi C., Brand A., «In Pursuit of Open Science, Open Access Is Not Enough», *Science* 368, fasc. 6491, 8 maggio 2020, pp. 574-577.
<https://doi.org/10.1126/science.aba3763>.

Aspesi C., Starr Allen N., Crow R., Daugherty S., Joseph H., McArthur J.T.W., Shockey N., «SPARC Landscape Analysis: The Changing Academic Publishing Industry – Implications for Academic Institutions», Preprint, LIS Scholarship Archive, 3 aprile 2019.
<https://doi.org/10.31229/osf.io/58yhb>.

Aspesi C., Starr Allen N., Crow R., Daugherty S., Joseph H., McArthur J.T.W., Shockey N., «SPARC Roadmap for Action: Academic Community Control of Data Infrastructure», Preprint, LIS Scholarship Archive, 19 novembre 2019.
<https://doi.org/10.31229/osf.io/a7nk8>.

Aspesi C., Starr Allen N., Crow R., Daugherty S., Joseph H., McArthur J.T.W., Shockey N., «2020 Update: SPARC Landscape Analysis & Roadmap for Action», Preprint, LIS Scholarship Archive, 22 giugno 2020.
<https://doi.org/10.31229/osf.io/2pwft>.

Aspesi C., Starr Allen N., Crow R., Daugherty S., Joseph H., McArthur J.T.W., Shockey N., «2020 Update: SPARC Landscape Analysis & Roadmap for Action», Preprint. LIS Scholarship Archive, 22 settembre 2021.

Astone A., «Capitalism of Digital Surveillance and Digital Disintermediation in the Era of the Pandemic», *European Journal of Privacy Law & Technologies*, fasc. 2, 2020, pp. 163-171.

<https://universitypress.unisob.na.it/ojs/index.php/ejplt/article/view/1215>.

Atlas S., «ChatGPT for Higher Education and Professional Development: A Guide to Conversational AI», 2023.

https://digitalcommons.uri.edu/cba_facpubs/548.

Autolitano S., Pawlowska A., «Europe's Quest for Digital Sovereignty: GAIA-X as a Case Study», *IAI Papers*, n. 21, 2021.

<https://www.iai.it/en/pubblicazioni/europes-quest-digital-sovereignty-gaia-x-case-study>.

Barrett L., «Rejecting Test Surveillance in Higher Education», July 29, 2021, 1 *Mich. St. L. Rev.* forthcoming 2023. <https://ssrn.com/abstract=3871423>.

Bassoli E., «La Ciber-Etica: luci e ombre della predittività algoritmizzata», in *Liber Amicorum* per Pasquale Costanzo, 2020.

http://www.giurcost.org/LIBERAMICORUM/bassoli_scrittiCostanzo.pdf.

Belloso N.M., Petit N., «The Eu Digital Markets Act, a Competition Hand in a Regulatory Glove», *European Law Review* (Forthcoming), April 5, 2023.

<https://ssrn.com/abstract=4411743>.

Bianca M., «La filter bubble e il problema dell'identità digitale», *MediaLaws. Riv. dir. media*, 2, 2019, pp. 39-53.

Bincoletto G., «La privacy by design: un'analisi comparata nell'era digitale», Ariccia, Aracne editrice, 2019.

Bincoletto G., «Italy - E-Proctoring During Students' Exams: Emergency Remote Teaching at Stake», *European Data Protection Law Review* 7, fasc. 4, 2021, pp. 586-591.

<https://doi.org/10.21552/edpl/2021/4/15>.

Boehme-Neßler V., «Privacy: A Matter of Democracy. Why Democracy Needs Privacy

and Data Protection», *International Data Privacy Law* 6, fasc. 3, agosto 2016, pp. 222-229.

<https://doi.org/10.1093/idpl/ipw007>.

Borgman C. L., «Open Data, Grey Data, and Stewardship: Universities at the Privacy Frontier», 2018, pp. 365-412.

<https://doi.org/10.15779/Z38B56D489>.

Brembs B., Förstner K., Goedicke M., Konrad U., Wannemacher K., Kett, J., «Plan I - Towards a Sustainable Research Information Infrastructure», 21 gennaio 2021.

<https://zenodo.org/record/4454640>.

Calisai F., «I diritti dell'interessato», in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, Torino, Giappichelli, 2019, pp.327-351.

Caso R., «The Darkest Hour: Private Information Control and the End of Democratic Science», *Trento Law and Technology Research Group Research Papers*, nr. 35, 2018.

<https://ssrn.com/abstract=3189519>.

Caso R., «La società della mercificazione e della sorveglianza: dalla persona ai dati» (versione 1.0), Zenodo, 2021.

<https://doi.org/10.5281/ZENODO.4603174>.

Caso R., «La valutazione autoritaria e la privatizzazione della conoscenza contro la scienza aperta», Zenodo, 2022.

<https://doi.org/10.5281/zenodo.7396228>.

Caso R., Pievatolo M.C., «A Liberal Infrastructure in a Neoliberal World: The Italian Case of GARR», *Journal of Intellectual Property, Information Technology and Electronic Commerce*, 2023.

<https://zenodo.org/record/7561821#.Y8655BPMK3I>.

Cavanillas J.M., Curry E., Wahlster W., a c. di. «New Horizons for a Data-Driven Economy» Cham: Springer International Publishing, 2016.

<https://doi.org/10.1007/978-3-319-21569-3>.

Celeste E., De Gregorio G., «Towards a Right to Digital Education? Constitutional Challenges of Edtech», *JIPITEC* 234, 14, para 1, 2023, pp. 234-250.

<https://www.jipitec.eu/issues/jipitec-14-2-2023/5735>.

Chugh R., Ruhi U., «Social Media for Tertiary Education» in A. Tatnall (ed), Encyclopedia of Education and Information Technologies, Springer International Publishing, 2019.
https://doi.org/10.1007/978-3-319-60013-0_202-1.

Cockburn I.M., Henderson, R., Stern S., «The impact of artificial intelligence on innovation», National Bureau of Economic Research, 2018.

Constantiou I., D. Kallinikos, J., «New Games, New Rules: Big Data and the Changing Context of Strategy», Journal of Information Technology 30, fasc. 1, marzo 2015, pp. 44-57.
<https://doi.org/10.1057/jit.2014.17>.

Conyon M. J., «Big Technology and Data Privacy», Cambridge Journal of Economics 46, fasc. 6, 31 dicembre 2022, pp. 1369-1385.
<https://doi.org/10.1093/cje/beac052>.

Cremer J. et al., «Competition policy for the Digital Era», 2019,
[/https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf](https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf)

Cuéllar M.F., Huq, A., «Economies of Surveillance», Harvard Law Review 133, no. 4, 2020, pp. 1280-1336.

D'Ippolito G., «Commercializzazione dei dati personali: il dato personale tra approccio morale e negoziale», Il diritto dell'informazione e dell'informatica, n.3, 2020, pp. 634-674.

D'Souza K.A., Siegfeldt D.V., «A Conceptual Framework for Detecting Cheating in Online and Take-Home Exams», Decision Sciences Journal of Innovative Education 370, 2017.

Daskin A.J., Wu, L. «Observation on the Multiple Dimension of Market Power», American Bar Association 6, 2005, pp. 54-58.

Davola A., Malgieri G., «Data, Power and Competition Law: The (Im)Possible Mission of the DMA?», Research in Law and Economics, Forthcoming, 2023.
<https://ssrn.com/abstract=4242574>

De Franceschi A. «Il “pagamento” mediante dati personali», in V. Cuffaro, V. D'Orazio, V. Ricciuto (a cura di), I dati personali nel diritto europeo, Torino, Giappichelli, 2019.

Draper N., Turow J. «Audience Constructions, Reputations and Emerging Media Technologies: New Issues of Legal and Social Policy» in R. Brownsword, E. Scotford, K. Yeung (eds), *The Oxford Handbook of Law, Regulation and Technology*, Oxford University Press 2017, pp. 1143–67.

Drechsler L., Elbi A., Kindt E., Kun E., Meszaros, J., Vranckaert K., «Third Time Is the Charm? The Draft Data Privacy Framework for International Personal Data Transfers From the European Union to the United States», *CiTiP Working Paper*, giugno 2023.
<http://dx.doi.org/10.2139/ssrn.4477120>.

Ducato R., Priora G., Angiolini C., Giannopoulou A., Jutte B., La Diega G., Pascault L., Schneider G., «Didattica di emergenza o Emergency Remote Teaching: un'analisi empirica in tema di privacy e diritto d'autore dei termini e condizioni dei servizi online più diffusi», *Law and Media working paper series*, no.2/2020.

Fiebig T. et al, «Heads in the Clouds: Measuring the Implications of Universities Migrating to Public Clouds», 2021.
<https://arxiv.org/abs/2104.09462>.

Fiormonte D., Sordini P., «Geopolitica della conoscenza digitale. Dal web aperto all'impero di GAFAM», *DigitCult. Scientific Journal on Digital Cultures*, 17 giugno 2019, pp. 21-36.
<https://doi.org/10.4399/97888255263183>.

Florio M., «La privatizzazione della conoscenza», Bari, Editori Laterza, 2021.

Franch C., «Il capitalismo dei monopoli intellettuali e l'editoria della sorveglianza. Un'analisi delle politiche europee sull'open science e sulla regolazione dei dati», *Zenodo*, 2023.
<https://doi.org/10.5281/zenodo.7770242>.

Furman J., «Unlocking Digital Competition, Report of the Digital Competition Expert Panel», UK Government, 2019.
[/https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf).

Gallese C., «A first commentary to the proposal for a new Regulation on fair access and use of Data (Data Act)», *MediaLaws*, 3/2022, pp. 237-270.

Giacalone M., «Verso Schrems III? Analisi del nuovo EU-US Data Privacy Framework», European papers, quaderni europei, 14 giugno 2023, consultabile al link: <https://www.europeanpapers.eu/en/europeanforum/verso-schrems-iii-analisi-nuovo-eu-us-data-privacy-framework>.

Giannopoulou A., Ducato R., Angiolini C., Schneider G., «From data subjects to data suspects: challenging e-proctoring systems as a university practice», JIPITEC 278, 14, para 1, 2023, pp. 278-306.
<https://www.jipitec.eu/issues/jipitec-14-2-2023/5737>.

Giovanella F., «Copyright and Information Privacy. Conflicting Rights in Balance», Cheltenham, Edward Elgar, 2017.

Gourlay L., «Surveillance and Datafication in Higher Education: Documentation of the Human», Postdigit Sci Educ, 2022.
<https://doi.org/10.1007/s42438-022-00352-x>.

Guarda P., Bincoletto G., «Diritto comparato della privacy e della protezione dei dati personali», Zenodo, 2023.
<https://doi.org/10.5281/zenodo.7805085>.

Harari Y.N., «Homo deus. Breve storia del futuro», Firenze-Milano, Giunti- Bompiani, 2017.

Hucap J., «Data protection and Antitrust: new types of abuse cases? An economist view in light of the German Facebook Decision», CPI Antitrust Chronicle, 2019.

Jackwerth K., «Great expectations: the Facebook case and subsequent legislative approaches to regulate large online platforms and digital markets», JIPITEC, 13,2022, pp. 200-223.
<https://www.jipitec.eu/issues/jipitec-13-3-2022/5556>.

Kaminski M., «The developing law of AI Regulation: A Turn to Risk Regulation», The LawFare Institute, 2023.
<https://www.lawfaremedia.org/article/the-developing-law-of-ai-regulation-a-turn-to-risk-regulation>.

Kaplan J., «Artificial Intelligence. What everyone needs to know», New York, Oxford University Press USA, 2016.

Kerber W., Zolna K., «The German Facebook Case: The Law and Economics of the Relationship between Competition and Data Protection Law», *European Journal of Law and Economics*, November 14, 2021.

<http://dx.doi.org/10.2139/ssrn.3719098>.

Khan L., «Amazon's Antitrust Paradox», *Yale Law Journal*, Vol. 126, 31, 2017, pp. 710-805.

<https://ssrn.com/abstract=2911742>.

Khan L., «The End of Antitrust History Revisited», *133 Harvard Law Review*, 2020, pp.1655-1682.

<https://ssrn.com/abstract=3552132>.

Krafft P. M., Young M., Katell M., Huang K., Bugingo G., «Defining AI in Policy versus Practice in Proceedings of the 2020 AAAI/ACM Conference on AI, Ethics, and Society», New York, NY, USA, 2020, pp. 72-78.

Kramer B., Bosman J., «101 Innovations in Scholarly Communication - the Changing Research Workflow», 1805291 Bytes. figshare, 2015.

<https://doi.org/10.6084/M9.FIGSHARE.1286826>.

Krukta D.G., Smits R.M., Willhelm T.A., «Don't be evil: should we use Google in schools?», *TechTrends*. 65(4), 2021, pp. 421-431.

doi:10.1007/s11528-021-00599-4.

La Bella A., «Sfide, opportunità e minacce dell'economia data driven», in A. Morace Pinelli (a cura di), *La circolazione dei dati: persona, contratto e mercato*, Pisa, Pacini Giuridica, 2023.

Landes W.M., Posner, R.A., «Market Power in Antitrust Cases», *Harvard Law Review* 937, 1981, pp. 493-554.

Lessig L., «Code and other Laws of Cyberspace», New York, Basic Books, 1999.

Li T.C., «Privacy in Pandemic: Law, Technology, and Public Health in the COVID-19 Crisis», *52 Loyola University of Chicago Law Journal*, 2021, pp. 767-865.

Ligorio M.B., Cacciamani S., Cesareni D., «Didattica blended. Teorie, metodi ed esperienze», Milano, Mondadori Education, 2022.

Luchetta G., «Is the Google Platform a Two-Sided Market», *Journal of Competition Law & Economics* 10, no. 1,1 March 2014, pp. 185-207.
<https://doi.org/10.1093/joclec/nht026>; -and-network-effects.

Maex K., «Protect independent and public knowledge», discorso tenuto l'8 gennaio 2021 per il 389° *dies natalis* dell'Università di Amsterdam.
<https://www.eua.eu/downloads/content/speech-karen-maex---dies-2021.pdf>.

Maex K., Bakker M., « The university in the age of platforms and algorithms» in A. M. Cauce, Y. Flückiger, B. van der Zwaan (Eds) *Universities as fifth Power? Opportunities, Risks and Strategies*, Geneva, The Glion Colloquium, Volume Nr. 13, 2022.
<https://glion.org/universities-as-fifth-poweropportunities-risks-and-strategies/>

Malgieri G., Custers B., «Pricing Privacy: The Right to Know the Value of Your Personal Data», *Computer Law & Security Review*», 2018.
<https://ssrn.com/abstract=3047257>.

Malgieri G., Davola A., «Data Powerful, questioning the concept of power in digital markets», 2022.
<http://dx.doi.org/10.2139/ssrn.4027370>

Mati R., «Personal Data and Consumer Protection: What do they have in common?», in M. Bakhom et al., *Personal Data in Competition, Consumer Protection and Intellectual Property Law: Towards a Holistic Approach?*, Heidelberg, Springer Berlin, 2018.

McCarthy J., Minsky M. L., Rochester N., Shannon C. E., «A proposal for the Dartmouth Summer Research Project on Artificial Intelligence», 1955.

Monella P., «Istruzione e GAFAM: dalla coscienza alla responsabilità», *Umanistica Digitale* No. 11, 25 gennaio 2022, pp. 27-45.
<https://doi.org/10.6092/ISSN.2532-8816/13685>.

Mortier R., «Explainer: The Internet of Things», *The Conversation*, 2 August 2013.

Noto La Diega G., «Internet of Things and the Law: Legal Strategies for Consumer-Centric Smart Technologies», *Routledge Research in the Law of Emerging Technologies*, London, Routledge, 2022.

O'Brien P., Young S.W.H., Arlitsch K., Benedict K., «Protecting Privacy on the Web: A Study of HTTPS and Google Analytics Implementation in Academic Library Websites»,

Online Information Review 42, fasc. 6, 13 settembre 2018, pp.734-751.
<https://doi.org/10.1108/OIR-02-2018-0056>.

Ohlhausen M.K, Okuliar A.P., «Competition, Consumer Protection and the right (approach) to privacy», *Antitrust Law Journal*, 2015.
<https://ssrn.com/abstract=2561563>.

Ostrom E., «Governing the Commons: The Evolution of Institutions for Collective Action», Cambridge University Press 1990.

Pagano U., «The Crisis of Intellectual Monopoly Capitalism», *Cambridge Journal of Economics* 38, fasc. 6, 1 novembre 2014, pp. 1409-1429.
<https://doi.org/10.1093/cje/beu025>.

Pagnanelli V., «Conservazione dei dati e sovranità digitale. Una rilettura della (big) data governance pubblica alla luce delle nuove sfide globali», *Rivista italiana di informatica e diritto* 3, fasc. 1, 3 luglio 2021, pp. 11–26.
<https://doi.org/10.32091/RIID0022>.

Pascuzzi G., «Il problem solving nelle professioni legali», Bologna, il Mulino, 2017.

Pascuzzi G., «Il diritto dell'era digitale», Bologna, il Mulino, 2020.

Pasquale F., Caderblom, M., «The New Antitrust: Realizing the Promise of Methodological Pluralism», 2022.

Picht P.G., Richter H. «EU Digital Regulation 2022: Data Desiderata», *GRUR International*, Volume 71, Issue 5, May 2022, pp. 395-402.
<https://doi.org/10.1093/grurint/ikac021>.

Pievatolo M.C., «I custodi del sapere», *bollettino telematico di filosofia politica*, 3 giugno 2021.
<https://zenodo.org/record/4897854>.

Pievatolo M.C., «Sulle spalle dei mercanti? Teledidattica e civiltà tecnologica», *bollettino tematico di filosofia politica*, 10 aprile 2022.
<https://doi.org/10.5281/ZENODO.6461431>.

Piromalli L., «L'università digitale», Roma, Carocci editore, 2023.

Polanyi K., «La grande trasformazione. Le origini economiche e politiche della nostra epoca», Torino, Einaudi, 1974.

Pooley J., «Surveillance Publishing», *The Journal of Electronic Publishing* 25, fasc. 1,26 aprile 2022, pp. 39-49.

<https://doi.org/10.3998/jep.1874>.

Posner R.A., «The Chicago School of Antitrust Analysis», 127, *U. PA. Law. Review*, 1979, pp. 925-948.

Quarta A., Smorto G., «Diritto privato dei mercati digitali», Milano, Mondadori - Le Monnier Università, 2020.

Reidenberg J.R., «Lex Informatica: The formulation of Information Policy Rules through Technology», 76 *Tex. L. Rev.*, 1997-1998, pp. 553-593.

Resta G., Zencovich Z., «Volontà e consenso nella fruizione dei servizi di Rete», in *Riv. trim. dir. e proc. civ.*, 2018, 2, pp. 411-440.

Riccio G.M., Scorza G., Bellisario E., «GDPR e normativa privacy, commentario», Milano, Wolters Kluwer, 2018.

Richter H., «The Property Paradigm in Private Law», in M. Bakhoun et al., *Personal Data in Competition, Consumer Protection and Intellectual Property Law: Towards a Holistic Approach?*, Heidelberg, Springer Berling, 2018.

Richter H. «Looking at the Data Governance Act and Beyond: How to Better Integrate Data Intermediaries in the Market Order for Data Sharing», *GRUR International*, Volume 72, Issue 5, May 2023, pp. 458-470.

<https://doi-org.ezp.biblio.unitn.it/10.1093/grurint/ikad014>.

Rikap C., Lundvall B., «The Digital Innovation Race, conceptualizing the emerging New World Order», London, Palgrave Macmillan, 2021.

<https://doi.org/10.1007/978-3-030-89443-6>.

Rochet J., Tirole J., «Platform Competition in Two-Sided Markets», *Journal of the European Economic Association* 1, no. 4, 1 June 2003, pp. 990-1029.

<https://doi.org/10.1162/154247603322493212>.

Rodotà S., «Tecnologie e diritti» Bologna, Il mulino, 1995.

Rodotà S., «Riservatezza», Enciclopedia Treccani, VI appendice, 2000, consultabile al link: https://www.treccani.it/enciclopedia/riservatezza_%28Enciclopedia-Italiana%29/.

Rodotà S., Discorso conclusivo della 26esima Conferenza internazionale sulla protezione dei dati, settembre 2004, consultabile al link: <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1049293>.

Roosendaal A., «Facebook Tracks and Traces Everyone: Like This!», SSRN Electronic Journal, 2010.
<https://doi.org/10.2139/ssrn.1717563>.

Ruohonen J., Mickelsson S. «Reflections on the Data Governance Act», DISO 2, 10, 2023.
<https://doi-org.ezp.biblio.unitn.it/10.1007/s44206-023-00041-7>.

Santaniello M., «Sovranità digitale e diritti fondamentali: un modello europeo di Internet governance», Rivista italiana di informatica e diritto. 4, 1, mar. 2022, pp. 47-51.
<https://doi.org/10.32091/RIID0058>.

Scassa, T., «The Surveillant University: Remote Proctoring, AI, and Human Rights», 8 The Canadian Journal of Comparative and Contemporary Law, 2022, pp. 271-312.

Schulz T., «Schrems v. Data Protection Commissioner (C.J.E.U.)». International Legal Materials, 56(2), 2017, pp. 245-272.
doi:10.1017/ilm.2017.8.

Schweitzer H., Metzger A. «Data Access under the Draft Data Act, Competition Law and the DMA: Opening the Data Treasures for Cowmpetition and Innovation?», GRUR International, Volume 72, Issue 4, April 2023, pp. 337–356.
<https://doi-org.ezp.biblio.unitn.it/10.1093/grurint/ikad012>.

Siems R., «When your journal reads you – user tracking on science publisher platforms», Elephant in the Lab, 2021.
<https://doi.org/10.5281/zenodo.4683778>.

Sloan A., «Schrems II: Commission 0», 41, Business Law Review, Issue 6, 2019, pp. 257-259.
<https://kluwerlawonline-com.ezp.biblio.unitn.it/JournalArticle/Business+Law+Review/41.6/BULA2020127>

Snowden E., «Errore di Sistema», Milano, Longanesi, 2019.

Solove D., Schwartz P.M., «Information Privacy Law», New York, Wolters Kluwer Law & Business, 2021.

Soro A., «Liberi e connessi», Torino, codice edizioni, 2016.

Speziale I., «L'ingresso dei dati nella prospettiva causale dello scambio: i modelli contrattuali di circolazione», Contratto e impresa, febbraio 2021, pp. 602-629.

Spulber D.F., «The economics of markets and platforms», Journal of Economics & Management Strategy, vol. 28, no. 1, 2019, pp. 159-72.

Star S.L., «The Ethnography of Infrastructure», American Behavioral Scientist 43, 3, 1999, pp. 377-391.

<https://purl.archive.org/purl/mcpievatolocit/star>.

Stazi A., Corrado F., «Datificazione dei rapporti socio-economici e questioni giuridiche: profili evolutivi in prospettiva comparatistica», Il diritto dell'informazione e dell'informatica, 2/2019, pp. 443-487.

Strowel A., Somaini L., «Towards a Robust Framework for Algorithmic Transparency to Tackle the Dissemination of Illegal and Harmful Content on Online Platforms», CRIDES Working Paper, 2021.

https://cdn.uclouvain.be/groups/cms-editors-crides/droit-intellectuel/CRIDES_WP_2_2021_Alain%20Strowel%20and%20Laura%20Somaini.pdf>.

Strowel A., De Meyere J. «The Digital Services Act: transparency as an efficient tool to curb the spread of disinformation on online platforms?», JIPITEC 66, 14, para 1, 2023, pp. 66-83.

<https://www.jipitec.eu/issues/jipitec-14-1-2023/5708>.

Swauger S., «Software That Monitors Students during Tests Perpetuates Inequality and Violates Their Privacy». MIT Technology Review, 2020, consultabile al link:

<https://www.technologyreview.com/2020/08/07/1006132/software-algorithms-proctoring-online-tests-ai-ethics/>.

Tafari D., «Sistemi fuori controllo o prodotti fuorilegge? La cosiddetta “intelligenza artificiale” e il risveglio del diritto», bollettino telematico di filosofia politica, maggio 2023.

<https://doi.org/10.5281/zenodo.7953605>.

Tardieu H., «Role of Gaia-X in the European Data Space Ecosystem», in: Otto, B., ten Hompel, M., Wrobel, S. (eds) *Designing Data Spaces*, Springer, Cham. 2022.
https://doi.org/10.1007/978-3-030-93975-5_4.

Thaler R.H., Sustein C.R., «Nudge: Improving Decision About Health, Wealth and Happiness», Penugin, New York 2009.

Titone A., «EU-US. Data Privacy Framewor: è (finalmente) realtà!», *Medialaws*, 2023, consultabile al link:
<https://www.medialaws.eu/eu-u-s-data-privacy-framework-e-finalmente-realta/>

Tlili A., Shehata B., Adarkwah M.A. et al. «What if the devil is my guardian angel: ChatGPT as a case study of using chatbots in education», *Smart Learn. Environ.* 10, 15, 2023.
<https://doi-org.ezp.biblio.unitn.it/10.1186/s40561-023-00237-x>.

Van der Hof S., Lievens E., «The importance of privacy by design and data protection impact assessment in strengthening protection of children’s personal data under the GDPR», *Communications Law*, Vol. 23, No.1, 2018.
<https://ssrn.com/abstract=3107660>.

Varian, H. R., «Beyond Big Data». *Business Economics* 49, fasc. 1, gennaio 2014, pp.27-31.
<https://doi.org/10.1057/be.2014.1>.

Vestager M. «Fair Markets in a Digital World», discorso presso l’Autorità Garante per la Concorrenza e dei Consumatori danese, Copenaghen, 9 marzo 2018.

Warren S.D., Brandeis L.D. «The Right to Privacy», 4 *Harv. L. Rev.*, 1890, pp.193-220.

Wismer S., Bongard C., Rasek A, «Multi-Sided Market Economics in Competition Law Enforcement», *Journal of European Competition Law & Practice* 8, no. 4,1 April 2017, pp. 257-262.
<https://doi.org/10.1093/jeclap/lpw082>.

Witt A. C., «Excessive Data Collection as a Form of Anticompetitive Conduct – The German Facebook Case», 66(2), *Jean Monnet Working Paper* 1/20, *Antitrust Bulletin*, 2021, pp. 276–307.

<http://dx.doi.org/10.2139/ssrn.3671445>.

Wong J., Racine L., Henderson T., Ball K., «Online Learning as Commons: supporting student's data protection preferences through a collaborative digital environment», JIPITEC, 14, para 1, 2023, pp. 251-277.

<https://www.jipitec.eu/issues/jipitec-14-2-2023/5736>.

Wu T., «La maledizione dei giganti: un manifesto per la concorrenza e la democrazia», Bologna, Il Mulino, 2020.

Wu T., «The Curse of Bigness: New Deal Supplement», 2020.

<http://dx.doi.org/10.2139/ssrn.3646258>.

Yeung K., «Five Fears about Mass Predictive Personalization in an Age of Surveillance Capitalism», International Data Privacy Law 8, fasc. 3, 1 agosto 2018, pp. 258-269.

<https://doi.org/10.1093/idpl/ipy020>.

Zehner F., Hahnel C., «Artificial intelligence on the advance to enhance educational assessment: Scientific clickbait or genuine gamechanger?», Journal of Computer Assisted Learning, volume 39, Issue 3, 2023, pp. 695-702.

<https://doi-org.ezp.biblio.unitn.it/10.1111/jcal.12810>.

Zhou J., Ke, P., Qiu, X. et al. «ChatGPT: potential, prospects, and limitations. Front Inform Technol Electron Eng», 2023.

<https://doi-org.ezp.biblio.unitn.it/10.1631/FITEE.2300089>.

Zuboff S. «Big Other: Surveillance Capitalism and the Prospects of an Information Civilization», Journal of Information Technology 30, fasc. 1, marzo 2015, pp. 75-89.

<https://doi.org/10.1057/jit.2015.5>.

Zuboff S. «Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri», Roma, Luiss University Press, 2019.

INDICE DELLE DECISIONI

Giurisprudenza della Corte di Giustizia dell'Unione europea

Corte di Giustizia dell'Unione europea, Sentenza della Corte, 24 ottobre 1995, Causa C-101/01, consultabile al

link:<https://curia.europa.eu/juris/document/document.jsf?docid=48382&doclang=IT>.

Corte di Giustizia dell'Unione europea, sentenza della Corte (Grande Sezione), 13 maggio 2014, Google Spain SL e Google Inc. Contro Agencia Española de Protección de Datos (AEPD) e Mario Costeja González, Causa C-131/12. Consultabile al link:
<https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A62012CJ0131>.

Corte di Giustizia dell'Unione europea, Sentenza della Corte (Grande Sezione), 6 ottobre 2015, Maximilian Schrems contro Data Protection Commissioner, Causa C-362/14, consultabile al link:
<https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:62014CJ0362>.

Corte di Giustizia, Sentenza della Corte (Seconda Sezione), 29 luglio 2019, Fashion ID GmbH & Co. KG contro Verbraucherzentrale NEW eV, Causa C-40/17, consultabile al link:
<https://curia.europa.eu/juris/document/document.jsf;jsessionid=031958705DEB419CB2DC5D5FE6A4AC69?text=&docid=216555&pageIndex=0&doclang=IT&mode=lst&dir=&occ=first&part=1&cid=286775>.

Corte di Giustizia dell'Unione europea, Sentenza della Corte (Grande Sezione), 16 luglio 2020, Data Protection Commissioner contro Facebook Ireland Limited e Maximilian Schrems, Causa C-311/18, consultabile al link:
<https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A62018CJ0311>.

Corte di Giustizia dell'Unione europea, Sentenza della Corte (Grande Sezione), 4 luglio 2023, Meta Platforms, già Facebook Inc., Meta Platforms Ireland Ltd, già Facebook Ireland Ltd, Facebook Deutschland GmbH contro Bundeskartellamt, Causa 252/21, consultabile al link:
<https://curia.europa.eu/juris/document/document.jsf;jsessionid=D79FF609E07A861EB91C4BE8B5B19882?text=&docid=275125&pageIndex=0&doclang=IT&mode=req&dir=&occ=first&part=1&cid=154729>.

Giurisprudenza della Corte europea dei diritti dell'uomo

Corte europea dei diritti dell'uomo, Kjeldsen, Busk Madsen and Pedersen v. Denmark, 7.12.1976, consultabile al link:
[https://hudoc.echr.coe.int/fre#{%22itemid%22:\[%22001-57509%22\]}](https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-57509%22]}).

Corte europea dei diritti dell'uomo, Catan and Others v. the Republic of Moldova and Russia [GC], 19.10.2012, consultabile al link:
[https://hudoc.echr.coe.int/fre#{%22itemid%22:\[%22002-7212%22\]}](https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22002-7212%22]}).

Giurisprudenza italiana

Corte di Cassazione, n. 4487 del 1956.

Corte di Cassazione, n. 990 del 1963.

Corte di Cassazione, n.2129 del 1975.

Corte di Cassazione, n.978 del 1996.

TAR Lazio, sez. I, 10 gennaio 2020 n. 261.

Consiglio di Stato, sezione VI, 29 marzo 2021, n. 2631, consultabile al link:

https://www.giustizia-amministrativa.it/portale/pages/istituzionale/visualizza/?nodeRef=&schema=cds&nrg=202001825&nomeFile=202102631_11.html&subDir=Provvedimenti.

TAR Lazio, sezione I, 18 novembre 2022, n. 15326 consultabile al link:

https://www.giustizia-amministrativa.it/portale/pages/istituzionale/visualizza?nodeRef=&schema=tar_rm&nrg=202113870&nomeFile=202215326_01.html&subDir=Provvedimenti.

TAR Lazio, sezione I, 18 novembre 2022, n. 15317, consultabile al link:

https://www.giustizia-amministrativa.it/portale/pages/istituzionale/visualizza?nodeRef=&schema=tar_rm&nrg=202113949&nomeFile=202215317_01.html&subDir=Provvedimenti.

Giurisprudenza statunitense

Corte Suprema degli Stati Uniti, Griswold v. Connecticut, 1965, consultabile al link:

<https://constitutioncenter.org/the-constitution/supreme-court-case-library/griswold-v-connecticut>.

Corte Suprema degli Stati Uniti, Roe v. Wade, 1975, consultabile al link:

<https://constitutioncenter.org/the-constitution/supreme-court-case-library/roe-v-wade>.

Corte Suprema degli Stati Uniti, Whalen v. Roe, 1977, consultabile al link:

<https://supreme.justia.com/cases/federal/us/429/589/>.

Altre pronunce

Bundeskartellamt, 6th Decision division, decisione n. B6-22/16, 6 Febbraio 2019, versione in lingua inglese consultabile al link:

http://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Entscheidungen/Missbrauchsaufsicht/2019/B6-22-16.pdf%3F__blob%3DpublicationFile%26v%3D5.

CNPD, Deliberação/2021/622, consultabile al link:

<https://www.cnpd.pt/comunicacao-publica/noticias/aplicacoes-respondus-violam-rgpd/>.

Data Protection Commission irlandese, Decision of the Data Protection Commission made pursuant to Section 111 of the Data Protection Act, 2018 and Articles 60 and 65 of the General Data Protection Regulation, 12 maggio 2023. Consultabile al link:

https://edpb.europa.eu/system/files/2023-05/final_for_issue_ov_transfers_decision_12-05-23.pdf.

Gerechtshof Amsterdam - 200.280.852/01, consultabile in lingua inglese al link:

https://gdprhub.eu/index.php?title=Gerechtshof_Amsterdam_-_200.280.852/01.

Rechtbank Amsterdam, 11 giugno 2020, C/13/684665 / KG ZA 20-481, consultabile al link:

<https://uitspraken.rechtspraak.nl/#!/details?id=ECLI:NL:RBAMS:2020:2917>.

ALTRI DOCUMENTI, PARERI, COMUNICAZIONI

Autorità Garante della Concorrenza e del Mercato, provvedimento n. 27432 del 29 novembre 2018, consultabile al link:

www.agcm.it/dotcmsdoc/allegati-news/PS11112_scorr_sanz.pdf.

Autorità Garante della Concorrenza e del Mercato, provvedimento n. 29888 del 9 novembre 2021, consultabile al link:

https://www.agcm.it/dotcmsdoc/allegati-news/PS11150%20prov%20chiusura_estratto.pdf.

Autorità Garante della Concorrenza e del Mercato, provvedimento n. 29890 del 16 novembre 2021, consultabile al link:

https://www.agcm.it/dotcmsdoc/allegati-news/PS11147%20chiusura_estratto.pdf.

Autorità Garante della Concorrenza e del Mercato, avviata istruttoria nei confronti di Apple per presunto abuso di posizione dominante nel mercato delle app, 2 maggio 2023, consultabile al link:

<https://www.agcm.it/dotcmsdoc/allegati-news/A561%20avvio.pdf>.

Autorità Garante per la protezione dei dati personali, didattica a distanza, prime indicazioni, provvedimento del 26 marzo 2020, consultabile al link:

<https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9300784>.

Autorità Garante per la protezione dei dati personali, ordinanza ingiunzione nei confronti di Università Commerciale 'Luigi Bocconi' di Milano - 16 settembre 2021 [doc. web. n. 9703988], pubblicata in Registro dei provvedimenti n. 317 del 16 settembre 2021, consultabile al link:

<https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9703988>.

Autorità Garante per la protezione dei dati personali, La scuola a prova di privacy. Vademecum ed. 2023, 15 maggio 2023, consultabile al link:

<https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9886884>.

Commissione europea, Decisione 2000/520/CE, a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio sull'adeguatezza della protezione offerta dai principi di approdo sicuro, 26 luglio 2000, consultabile al link:

<https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32000D0520>.

Commissione europea, caso COMP/M.4731 - Google/DoubleClick, 11 marzo 2008. La sintesi è liberamente consultabile al link:

[https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52008XC0722\(03\)](https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52008XC0722(03)).

Commissione europea, Decisione 2010/87, relativa alle clausole contrattuali tipo per il trasferimento di dati personali e incaricati al trattamento stabiliti in paesi terzi a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio, 5 febbraio 2010.

Commissione europea, caso COMP/M.7217 – Facebook/Whatsapp, 3 ottobre 2012, consultabile al link:

[/https://ec.europa.eu/competition/mergers/cases/decisions/m7217_20141003_20310_3962132_EN.pdf](https://ec.europa.eu/competition/mergers/cases/decisions/m7217_20141003_20310_3962132_EN.pdf).

Commissione europea, Comunicazione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni Verso una florida economia basata sui dati, 2 luglio 2014, consultabile al link:

<https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:52014DC0442>.

Commissione europea, Decisione di esecuzione (UE) 2016/1250, a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio, sull'adeguatezza della protezione offerta dal regime dello scudo UE-USA per la privacy, 12 luglio 2016, consultabile al link:

<https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32016D1250>.

Commissione europea, Regulation (EC) NO 138/2004 merger procedure, case M.8124 - Microsoft/LinkedIn, 6 dicembre 2016, consultabile al link:

https://ec.europa.eu/competition/mergers/cases/decisions/m8124_1349_5.pdf.

Commissione europea, imposing fines under Article 14(1) of Council Regulation (EC) No. 139/2004 for the supply by an undertaking of incorrect or misleading information, (Case No.M.8228 – Facebook/WhatsApp), decisione 17 maggio 2017, consultabile al link:

https://ec.europa.eu/competition/mergers/cases/decisions/m8228_493_3.pdf.

Commissione europea, Comunicazione al Parlamento europeo, al Consiglio, al Comitato Economico e Sociale europeo e al Comitato delle regioni, «Una strategia europea dei dati», 19 febbraio 2020, consultabile al link:

<https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A52020DC0066>.

Commissione europea, Inception Impact Assessment: New Competition Tool, 2 giugno 2020, consultabile al link:

https://competition-policy.ec.europa.eu/public-consultations/2020-new-comp-tool_en.

Commissione europea, piano d'azione per l'istruzione digitale 2021-2027, 30 settembre 2020, consultabile al link:

<https://education.ec.europa.eu/it/focus-topics/digital-education/action-plan>.

Commissione europea, uno spazio europeo per l'istruzione entro il 2025, 30 settembre 2020, consultabile al link:

<https://education.ec.europa.eu/it/about-eea/the-eea-explained>.

Commissione europea, Decisione di esecuzione (UE) 2021/914, relativa alle clausole contrattuali tipo per il trasferimento dei dati personali verso paesi terzi a norma del

regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, 4 giugno 2016, consultabile al link:

<https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32016D0679>.

Commissione europea, Directorate general for Education, Youth and Sports, Ethical guidelines on the use of artificial intelligence (AI) and data in teaching and learning for educators, Publications Office of the European Union, 25 ottobre 2022, consultabile al link:

<https://data.europa.eu/doi/10.2766/153756>.

Commissione europea, Study on the Digital Services Act and the Digital Markets Act and their possible impact on research, 2022, consultabile al link:

<https://op.europa.eu/en/publication-detail/-/publication/49677a41-1144-11ed-8fa0-01aa75ed71a1/language-en/format-PDF/source-262356279>.

Commissione europea, Bozza di decisione di adeguatezza pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under EU-US Data Privacy Framework, 2022, consultabile al link:

[/https://commission.europa.eu/system/files/2022-12/Draft%20adequacy%20decision%20on%20EU-US%20Data%20Privacy%20Framework_0.pdf](https://commission.europa.eu/system/files/2022-12/Draft%20adequacy%20decision%20on%20EU-US%20Data%20Privacy%20Framework_0.pdf).

Commissione europea, implementing decision of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the UE-UE Data Privacy Framework, 10 luglio 2023, consultabile al link:

https://commission.europa.eu/system/files/2023-07/Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework_en.pdf.

Consiglio d'Europa, Consultative committee of the convention for the protection of individuals with regard to automatic processing of personal data, Convention 108, Children's Data Protection in Education Systems: Challenges and Possible Remedies, 15 novembre 2019, consultabile al link:

<chrome-extension://efaidnbnmnibpcjpcglclefindmkaj/https://rm.coe.int/t-pd-2019-06final-eng-report-children/1680a01b47>.

Consiglio d'Europa, Children's data protection in an education setting, guidelines, dicembre 2020, consultabili al link:

<https://rm.coe.int/prems-001721-gbr-2051-convention-108-txt-a5-web-web-9-1680a9c562>.

Consiglio Europeo, Programma di Stoccolma, un'Europa aperta e sicura al servizio e a tutela dei cittadini, 2010/C115/01, 4 maggio 2010, consultabile al link:

<https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX%3A52010XG0504%2801%29>.

EPIC, In re Online Test Proctoring Companies, 2020, consultabile al link:

[https://epic.org/documents/in-re-online-test-proctoring-companies/#:~:text=On%20December%209%2C%202020%2C%20EPIC,Act%20\(DCCPPA\)%20and%20the%20Federal](https://epic.org/documents/in-re-online-test-proctoring-companies/#:~:text=On%20December%209%2C%202020%2C%20EPIC,Act%20(DCCPPA)%20and%20the%20Federal).

European Data Protection Board, Linee guida 2/2018 sulle deroghe di cui all'articolo 49 del regolamento 2016/679, 25 maggio 2018. Consultabili al link:

https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_it.pdf.

European Data Protection Board, Linee guida 1/2018 relative alla certificazione e all'identificazione di criteri di certificazione in conformità degli articoli 42 e 43 del regolamento (UE) 2016/679, versione 3.0, 4 giugno 2019, consultabile al link:

https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_it.pdf.

European Data Protection Board, Linee guida 1/2019 sui codici di condotta e sugli organismi di monitoraggio a norma del GDPR, versione 2.0, 4 giugno 2019, consultabili al link:

https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201901_v2.0_codesofconduct_it.pdf.

European Data Protection Board, Initial Legal Assessment of the Impact of the US Cloud Act on the EU Legal Framework for the Protection of Personal Data and the Negotiations of an EU-US Agreement on Close Border Access to Electronic Evidence, luglio 2019, consultabile al link:

https://edpb.europa.eu/sites/default/files/files/file2/edpb_edps_joint_response_us_cloudact_annex.pdf.

European Data Protection Board, Raccomandazioni 1/2020 relative alle misure che integrano gli strumenti di trasferimento al fine di garantire il rispetto del livello di protezione dei dati personali dell'UE, 10 novembre 2020, consultabili al link:

https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_it.pdf.

European Data Protection Board, Linee guida 2/2020 sull'articolo 46, paragrafo 2, lettera a), e paragrafo 3, lettera b), del Regolamento 2016/679 per i trasferimenti di dati personali tra autorità ed organismi pubblici del SEE e di paesi non appartenenti al SEE, versione 2.0, 15 dicembre 2020, consultabili al link:

[/https://edpb.europa.eu/system/files/2021-05/edpb_guidelines_202002_art46guidelines_internationaltransferspublicbodies_v2_it.pdf](https://edpb.europa.eu/system/files/2021-05/edpb_guidelines_202002_art46guidelines_internationaltransferspublicbodies_v2_it.pdf).

European Data Protection Board, Linee guida 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR, versione 2.0, 7 luglio 2021, consultabili al link:

https://edpb.europa.eu/system/files/2022-02/eppb_guidelines_202007_controllerprocessor_final_it.pdf

European Data Protection Board, Linee guida 7/2022 sulla certificazione come strumento per i trasferimenti, versione 2.0, 14 febbraio 2023, consultabili al link:

https://edpb.europa.eu/system/files/2023-05/edpb_guidelines_07-2022_on_certification_as_a_tool_for_transfers_v2_it_0.pdf.

European Data Protection Board, Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-UE Data Privacy Framework, 28 febbraio 2023, consultabili al link:

https://edpb.europa.eu/system/files/2023-02/edpb_opinion52023_eu-us_dpf_en.pdf.

European Data Protection Board, Binding decision 1/2023 on the dispute submitted by the Irish SA on data transfers by Meta Platforms Limited for its Facebook Services, 13 aprile 2023, consultabile al link:

https://edpb.europa.eu/our-work-tools/consistency-findings/binding-decisions_it

European Data Protection Supervisor, «Privacy e competitività nell'era dei Big Data», 26 marzo 2014, consultabile al link: https://edps.europa.eu/press-publications/press-news/press-releases/2014/privacy-and-competitiveness-age-big-data_en?etrans=it.

Gruppo di Lavoro ex articolo 29, Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools), 11 febbraio 2009, consultabile al link:

<https://ec.europa.eu/justice/article-29/documentation/opinion>.

Gruppo di Lavoro ex articolo 29, Parere 6/2014 sul concetto di interesse legittimo del responsabile del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE, adottato il 9 aprile 2014, consultabile al link:

https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_it.pdf.

Gruppo di lavoro ex articolo 29, Parere 8/2014 sui recenti sviluppi dell'internet degli oggetti, 16 settembre 2014, consultabile al link:

https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_it.pdf.

Gruppo di Lavoro ex articolo 29, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, 4 aprile 2018, consultabile al link:

<https://ec.europa.eu/newsroom/article29/items/611236>.

Parlamento europeo, Draft motion for a resolution to wind up the debate on the statement by the Commission, pursuant to rule 132(2) of the Rules of Procedure on the adequacy of the protection afforded by the EU-US Data Privacy Framework, 2023/2501(RSP), 14 febbraio 2023, consultabile al link:

https://www.europarl.europa.eu/doceo/document/LIBE-RD-740749_EN.pdf.

Parlamento europeo, Note tematiche sull'Unione europea, politica della concorrenza, aprile 2023, consultabile al link:

<https://www.europarl.europa.eu/factsheets/it/sheet/82/politica-della-concorrenza>.

Parlamento europeo, Risoluzione dell'11 maggio 2023 sull'adeguatezza della protezione offerta dal UE-U.S. Data Privacy Framework, 11 maggio 2023, consultabile al link:

https://www.europarl.europa.eu/doceo/document/TA-9-2023-0204_IT.html.

OECD, Data Driven Innovation, big data for growth and well-being, OECD Publishing, Paris, 2015, consultabile al link:

<https://www.oecd.org/sti/data-driven-innovation-9789264229358-en.htm>.

OECD, The State of Higher Education: One Year into the COVID-19 Pandemic, Organisation for Economic Co-operation and Development, 2021, consultabile al link:

<https://www.oecd-ilibrary.org/>.

Presidente degli Stati Uniti d’America, Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities, 7 ottobre 2022, consultabile al link: <https://www.whitehouse.gov/briefing-room/presidential-actions/2022/10/07/executive-order-on-enhancing-safeguards-for-united-states-signals-intelligence-activities/>.

Protocollo d’intesa tra Ministero dell’Istruzione, Apple Distribution International Limited e Osservatorio Permanente Giovani – Editori, 4 gennaio 2021, consultabile al link: <https://www.miur.gov.it/-/protocollo-di-intesa-tra-ministero-istruzione-apple-distribution-international-limited-e-osservatorio-permanente-giovani-editori>

Public Interest Advocacy Center Submission to the Governor Consultation on a Digital Economy Strategy for Canada, 2010, consultabile al link: <https://www.piac.ca/research-reports/piac-submission-to-the-government-consultation-on-a-digital-economy-strategy-for-canada/>.

UNESCO and McKinsey & Company, Covid-10 Response – Remote Learning Strategy, 2020.

ARTICOLI DI GIORNALE E COMUNICATI

Autorità Garante della Concorrenza e del Mercato, «Sanzioni per 20 milioni a Google e Apple per uso dei dati degli utenti a fini commerciali», 26 novembre 2021, consultabile al link: <https://www.agcm.it/media/comunicati-stampa/2021/11/PS11147-PS11150>

Autorità Garante per la protezione dei dati personali, «Intelligenza artificiale, il Garante blocca Chat GPT. Raccolta illecita di dati personali, assenza di sistemi per la verifica dell’età dei minori», 30 marzo 2023, consultabile al link: <https://www.gpdp.it/home/docweb/-/docweb-display/docweb/9870847>.

Basile M., «New York, avvocato presenta una causa usando ChatGpt. Ed è un disastro», la Repubblica, 23 maggio 2023, consultabile al link: https://www.repubblica.it/esteri/2023/05/29/news/chatgpt_avvocato_intelligenza_artificiale_avianca-402397182/#:~:text=Le%20scuse%20di%20Schwartz&text=Schwartz%20non%20era%20un%20avvocato,la%20prima%20volta%20il%20ChatGpt.

Cadwalladr C., Graham-Harrison E., «Revealed: 50 Million Facebook Profiles Harvested

for Cambridge Analytica in Major Data Breach», The Guardian, sez. News, 17 marzo 2018, consultabile al link:

<https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>.

CNIL, «La CNIL chiede cambiamenti nell'uso degli strumenti di collaborazione statunitensi per l'istruzione superiore e la ricerca», consultabile al link:

<https://www.cnil.fr/fr/la-cnil-appelle-evolutions-dans-utilisation-outils-collaboratifs-etatsuniens-enseignement-superieur-recherche>.

Commissione europea, «Illustrata la legge sulla governance dei dati», 30 agosto 2020, consultabile al link:

<https://digital-strategy.ec.europa.eu/it/policies/data-governance-act-explained>.

Commissione europea, «Sneak Peek: How the Commission Will Enforce the DSA & DMA», 5 luglio 2022, consultabile al link:

https://ec.europa.eu/commission/presscorner/detail/en/statement_22_4327.

Commissione europea, «Speech by Executive Vice-President Margrethe Vestager on a New Digital Education Action Plan 2021-2027 and a New European Research Area», 30 September 2020, consultabile al link:

<https://ec.europa.eu/commission/presscorner/detail/en/>.

Confessore N., «Cambridge Analytica and Facebook: The Scandal and the Fallout So Far», The New York Times, 4 aprile 2018, consultabile al link:

<https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html>.

Dastin J., «Amazon Scraps Secret AI Recruiting Tool That Showed Bias against Women», Reuters, 10 ottobre 2018, consultabile al link:

<https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G>.

Economist, «The world's most valuable resource is no longer oil, but data», maggio 2017, consultabile al link:

<https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>.

EDPB, «EDPB resolves dispute on transfers by Meta and creates task force on Chat GPT», 13 aprile 2023, consultabile al link:
https://edpb.europa.eu/news/news/2023/edpb-resolves-dispute-transfers-meta-and-creates-task-force-chat-gpt_en.

Elsen-Rooney M., «NYC education department blocks ChatGPT on school devices, network», Chalkbeat New York, 4 gennaio 2023, consultabile al link:
<https://ny.chalkbeat.org/2023/1/3/23537987/nyc-schools-ban-chatgpt-writing-artificial-intelligence>.

Fontana A., «Gaia-X, 2023 anno della crescita: opportunità per aziende e fornitori Ict», Il Sole 24 ORE, 31 gennaio 2023, consultabile al link:
<https://amp24-ilsole24ore.com.cdn.ampproject.org/c/s/amp24.ilsole24ore.com/pagina/AEC90TeC>.

MIUR, Ministero dell'istruzione e del merito, «Coronavirus, emanata la nota con le indicazioni operative per la didattica a distanza», 17 marzo 2020, consultabile al link:
<https://www.miur.gov.it/web/guest/-/coronavirus-emanata-la-nota-con-le-indicazioni-operative-per-la-didattica-a-distanza>.

MIUR, Ministero dell'istruzione e del merito, «Scuola, Ministero al lavoro su piattaforma digitale unica Azzolina: "Acceleriamo innovazione, costruiamo la scuola del futuro"», 11 dicembre 2020, consultabile al link:
<https://www.miur.gov.it/web/guest/-/scuola-ministero-al-lavoro-su-piattaforma-digitale-unica-azzolina-acceleriamo-innovazione-costruiamo-la-scuola-del-futuro->.

Office of the Privacy Commissioner of Canada, «Office of the Privacy Commissioner of Canada launches investigation into CHATGPT», 4 aprile 2023, consultabile al link:
https://www.priv.gc.ca/en/opc-news/news-and-announcements/2023/an_230404/.

POLIFLASH MAGAZINE - Il Politecnico digitale, «Al via con successo la didattica online», 13 marzo 2020, consultabile al link:
https://poliflash.polito.it/in_ateneo/il_politecnico_digitale_al_via_con_successo_la_didattica_online.

Repubblica, «Maxi-multa Ue a Facebook per aver collegato gli account di Whatsapp: 110 milioni», 18 maggio 2017, consultabile al link:
https://www.repubblica.it/economia/finanza/2017/05/18/news/maxi-multa_ue_a_facebook_per_aver_collegato_gli_account_di_whatsapp-165722348/.

Rolland S., «Fin de la récréation : Microsoft et Google exclus de l'école par l'Éducation nationale», La Tribune, 24 novembre 2022, consultabile al link:
<https://www.latribune.fr/technos-medias/internet/fin-de-la-recreation-microsoft-et-google-exclus-de-l-ecole-par-l-education-nationale-942051.html>.

Scialpi G., «Didattica a distanza, Ministero lavora ad una piattaforma unica. Abbia anche impronta pedagogica», Orizzonte Scuola Notizie, 28 giugno 2020, consultabile al link:
<https://www.orizzontescuola.it/didattica-a-distanza-ministero-lavora-ad-una-piattaforma-unica-abbia-anche-impronta-pedagogica/>.

Zoja S., «La scuola italiana al mercato dei dati. Così il controllo sulla didattica rafforza lo strapotere delle multinazionali», Altreconomia, marzo 2022.

BLOG

Arcidiacono G., «Gaia-X: lo standard europeo per il cloud e i suoi progetti principali», Agenda Digitale, 27 aprile 2022,
<https://www.agendadigitale.eu/infrastrutture/gaia-x-lo-standard-europeo-per-il-cloud-e-i-suoi-progetti-principali/>.

Ars Technica, «Even When Told Not to, Windows 10 Just Can't Stop Talking to Microsoft», 13 agosto 2015,
<https://arstechnica.com/information-technology/2015/08/even-when-told-not-to-windows-10-just-cant-stop-talking-to-microsoft/>.

Barchiesi A. et al., «Fare cloud senza rinunciare al controllo di dati e risorse: la ricetta GARR», Agenda Digitale, 13 gennaio 2022,
<https://www.agendadigitale.eu/infrastrutture/fare-cloud-senza-rinunciare-al-controllo-di-dati-e-risorse-la-ricetta-garr/>.

Binario Etico, «UNIRE, la Rete di interconnessione unica nazionale dell'istruzione», 24 marzo 2021.
https://binarioetico.it/digital_transformation/2021/03/24/unire/.

Caso R., «Università delle piattaforme: la DAD, il business dei dati personali e la fine dell'autonomia», Agenda Digitale, 12 agosto 2021,
<https://www.agendadigitale.eu/sicurezza/privacy/universita-delle-piattaforme-la-dad-il-business-dei-dati-personali-e-la-fine-dellautonomia/>.

Castigli M., «ChatGPT: cos'è, come si usa e cosa può fare», Agenda Digitale, 19 aprile 2023, <https://www.agendadigitale.eu/cultura-digitale/introduzione-a-chatgpt-cose-come-si-usa-e-cosa-puo-fare/>.

Cerrina Feroni G., «Luci e ombre della Data Strategy europea», Autorità Garante per la protezione dei dati personali per Agenda Digitale, 13 maggio 2022, consultabile al link: <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9769786> oppure a <https://www.agendadigitale.eu/cultura-digitale/cerrina-feroni-garante-privacy-luci-e-ombre-della-data-strategy-europea/>.

Garofalo L., «Cloud sovrano in Francia, il governo voltafaccia ai Gafam», Key4biz (blog), 15 settembre 2022, <https://www.key4biz.it/cloud-sovrano-in-francia-il-governo-voltafaccia-ai-gafam-e-sostiene-lecosistema-nazionale-e-litalia/415944/>.

Giannopoulou A., Ducato R., Schneider G., Angiolini C., «Critical Notes on 'Platformised' Education: Untangling Privacy and Data Protection in Postpandemic Universities», European Law Blog, 8 marzo 2021, <https://europeanlawblog.eu/2021/03/08/critical-notes-on-platformised-education-untangling-privacy-and-data-protection-in-postpandemic-universities/>.

Hanson C., «User Tracking on Academic Publisher Platforms», Prepared for the Coalition for Networked Information Spring 2019 Member Meeting, St. Louis, Missouri, April 8-9, 2019. <https://www.codyh.com/writing/tracking.html>.

Harvard Kennedy School, Belfer Center for science and international affair, «Tech Spotlight Casebook, spring 2021», 2021 <https://hks-spotlight.netlify.app/assets/tech-spotlight-casebook-2021>.

Hodges C. et al., «The difference between Emergency Remote Teaching and Online Learning», 27 marzo 2020, Educause, <https://er.educause.edu/articles/2020/3/the-difference-between-emergency-remote-teaching-and-online-learning>.

LERU, «LERU Data Statement», dicembre 2021, <https://www.leru.org/publications/is-university-autonomy-threatened-by-eu-data-policy-and-law>.

LERU, «LERU says NO to the Digital Services Act», 5 aprile 2022, <https://www.leru.org/news/leru-says-no-to-the-digital-services-act>.

Noyb, «La telecamera nel soggiorno: la privacy nei sistemi di videoconferenza», 2 aprile 2020,
<https://noyb.eu/it/trasmissione-interrotta>.

Noyb, «Opening Pandora Box, how companies addressed our questions about their international data transfers after the CJEU's ruling in C-311/18- Schrems II» 25 settembre 2020,
https://noyb.eu/sites/default/files/2021-10/Replies_from_controllers_on_EU-US_transfers.pdf.

Noyb, «Il nuovo quadro transatlantico sulla privacy dei dati è in gran parte una copia del "Privacy Shield". Noyb impugnerà la decisione», 10 luglio 2023,
<https://noyb.eu/it/european-commission-gives-eu-us-data-transfers-third-round-cjeu>.

Pagano U., «Il capitalismo dei monopoli intellettuali», Menabò di Etica ed Economia (blog), 14 dicembre 2021,
<https://archivio.eticaeconomia.it/il-capitalismo-dei-monopoli-intellettuali/>.

Pinto V. «Didattica blended: una tappa verso l'università delle piattaforme?», Roars, 24 giugno 2020,
<https://www.roars.it/didattica-blended-una-tappa-verso-luniversita-delle-piattaforme/>.

Privacy Network, «Il mercato dei dati»,
<https://privacy-network.it/mercato-dei-dati/>.

Salucci G., «Il flusso della pubblicazione nella editoria accademica», Academic Publishing Services, 23 marzo 2019,
<https://www.academic-publishing-services.it/flusso-della-pubblicazione-nella-editoria-accademica/>.

Salvadori G., «Smart Home: significato, mercato, applicazioni della casa intelligente», 4 febbraio 2021,
https://blog.osservatori.net/it_it/smart-home-italia-significato.

Scorza G., «Digital Services Act: Le luci e le poche ma gravi ombre delle nuove regole UE», Autorità Garante per la protezione dei dati personali per Agenda Digitale, 28 aprile 2022, consultabile al link:
<https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9765212>.

Scorza G., «Executive order di Biden, ecco i punti critici, quelli positivi e quelli da chiarire», Autorità Garante per la protezione dei dati personali per Agenda Digitale, 10 ottobre 2022, consultabile al link:

<https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9813161>.

Watters A., «Education technology and the age of surveillance capitalism», Hack Education, 28 Agosto 2019,

<http://hackededucation.com/2019/08/28/surveillance-ed-tech>.

Williamson B., «Datificazione e governo algoritmico dell'Università durante e dopo il Covid 19», Roars, 3 luglio 2020,

<https://www.roars.it/datificazione-e-governo-algoritmico-delluniversita-durante-e-dopo-il-covid-19/>.

SITOGRAFIA

«About Gaia-X - Gaia-X: A Federated Secure Data Infrastructure», <https://gaia-x.eu/what-is-gaia-x/about-gaia-x/>.

«About Us», EPIC - Electronic Privacy Information Center, <https://epic.org/about/>.

«Anvur», <https://www.anvur.it/>.

«Centro europeo per la trasparenza algoritmica»

https://algorithmic-transparency.ec.europa.eu/index_en?etrans=it.

«Consortium GARR», <https://www.garr.it/it/chi-siamo>.

«Cos'è Gaia-X, Gaia-X Hub Italia», <https://www.gaiax-italia.eu/cosa-facciamo>.

«Discord Privacy Policy», <https://discord.com/privacy#control>.

«Enciclopedia Treccani», liberamente accessibile al link:

<https://www.treccani.it/enciclopedia/>.

«Gaia-X»,

<https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html>.

«GAIA-X: Driver of Digital Innovation in Europe»,
https://www.data-infrastructure.eu/GAIA/Redaktion/EN/Publications/gaia-x-driver-of-digital-innovation-in-europe.pdf?__blob=publicationFile&v=8.

«Gaia-X: The European project kicks off the next phase»,
https://www.data-infrastructure.eu/GAIA/Redaktion/EN/Publications/gaia-x-the-european-project-kicks-of-the-next-phase.pdf?__blob=publicationFile&v=7.

«Google, norme sulla privacy»,
<https://policies.google.com/privacy?hl=it#europeanrequirements>.

«Honorlock», <https://honorlock.com/>.

«Il pacchetto della legge sui servizi digitali», sito web della Commissione europea,
<https://digital-strategy.ec.europa.eu/it/policies/digital-services-act-package>.

«Impact Factor (IF)».
<http://biblioteche.unipv.it/home/risorse/indicatori-bibliometrici/impact-factor-if>.

«Indicatori Bibliometrici».
<http://biblioteche.unipv.it/home/risorse/indicatori-bibliometrici>.

«Informativa sulla privacy di Google Cloud»,
<https://cloud.google.com/terms/cloud-privacy-notice?hl=it>.

«Informativa sulla privacy di Google Workspace for Education»,
https://workspace.google.com/terms/education_privacy.html#privacy-police-revamp-your-info.

«IoRestoACasa», <https://iorestoacasa.work/>.

«Jitsi Privacy Supplement», <https://jitsi.org/meet-jit-si-privacy/>.

«Meta, informativa sulla privacy», <https://www.facebook.com/privacy/policy/>.

«Microsoft, riepilogo sul Regolamento generale sulla protezione dei dati»,
<https://learn.microsoft.com/it-it/compliance/regulatory/gdpr?view=o365-worldwide#gdpr-faqs>.

«MoodleCloud Privacy notice», <https://moodle.com/privacy-notice/>.

«Panoramica delle nozioni di base sulla privacy per le app Youtube»,
<https://support.google.com/youtube/answer/10364219?hl=it#zippy=>.

«Piano d'azione per l'istruzione digitale – azione 6»,
<https://education.ec.europa.eu/it/focus-topics/digital-education/action-plan/action-6?>.

«Piano d'azione per l'istruzione digitale – azione 8»,
<https://education.ec.europa.eu/it/focus-topics/digital-education/action-plan/action-8?>.

«Privacy and Microsoft Teams»,
<https://learn.microsoft.com/en-us/microsoftteams/teams-privacy>.

«Proctorio», <https://proctorio.com/>
<https://proctorio.com/products/online-proctoring>.

«Respondus», <https://web.respondus.com/he/lockdownbrowser/>.
<https://web.respondus.com/he/monitor/>.

«Skype Legal», <https://www.skype.com/en/legal/>.

«Strategia europea in materia di dati», https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_it.

«Zoom, data subject access rights request form»,
<https://zoom-privacy.my.onetrust.com/webform/65962359-ef0d-4399-9db4-572d06de08aa/f277f9f7-bfee-4233-815e-80e290139bc2>.

«Zoom, informativa sulla privacy»,
<https://explore.zoom.us/it/privacy/>.

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/2/>

Freely downloadable papers already published:

STUDENT PAPER N. 89

Il «danno da movida» tra tutela inibitoria e risarcimento del danno

ANNALIA MAISTRELLI. Il «danno da movida» tra tutela inibitoria e risarcimento del danno. Trento Law and Technology Research Group, Student Paper Series; 89. Trento: Università degli Studi di Trento.

STUDENT PAPER N. 88

Disvelamento dei fatti e responsabilità civile. La funzione sociale del giornalismo d'inchiesta e del whistleblowing

ALBERTO SCANDOLA. Disvelamento dei fatti e responsabilità civile. La funzione sociale del giornalismo d'inchiesta e del whistleblowing. Trento Law and Technology Research Group, Student Paper Series; 88. Trento: Università degli Studi di Trento.

STUDENT PAPER N. 87

Responsabilità e accountability in materia di protezione dei dati personali: il contesto dell'Internet of Things

ANDREA BLATTI. Responsabilità e accountability in materia di protezione dei dati personali: il contesto dell'Internet of Things. Trento Law and Technology Research Group, Student Paper Series; 87. Trento: Università degli Studi di Trento.

STUDENT PAPER N. 86

Il capitalismo dei monopoli intellettuali e l'editoria della sorveglianza. Un'analisi delle politiche europee sull'open science e sulla regolazione dei dati

CAMILLA FRANCH. Il capitalismo dei monopoli intellettuali e l'editoria della sorveglianza. Un'analisi delle politiche europee sull'open science e sulla regolazione dei dati. Trento Law and Technology Research Group, Student Paper Series; 86. Trento: Università degli Studi di Trento.

STUDENT PAPER N. 85

Transformative Agreements: i nuovi contratti tra editori scientifici e istituzioni accademiche per l'accesso alle risorse scientifiche digitali. Un'analisi critica

MIRIANA FIERRO. Transformative Agreements: i nuovi contratti tra editori scientifici e istituzioni accademiche per l'accesso alle risorse scientifiche digitali. Un'analisi critica. Trento Law and Technology Research Group, Student Paper Series; 85. Trento: Università degli Studi di Trento.

STUDENT PAPER N. 84

La blockchain, tra proprietà e proprietà intellettuale. Analisi comparata di tre applicazioni nel diritto civile

NICOLÒ CANAL. La blockchain, tra proprietà e proprietà intellettuale. Analisi comparata di tre applicazioni nel diritto civile. Trento Law and Technology Research Group, Student Paper Series; 84. Trento: Università degli Studi di Trento.

STUDENT PAPER N.83

La ricerca di un criterio di quantificazione tipologico per il danno da perdita di chance nella responsabilità medica: una missione impossibile?

VALERIA LUCCARINI. La ricerca di un criterio di quantificazione tipologico per il danno da perdita di chance nella responsabilità medica: una missione impossibile. Trento Law and Technology Research Group, Student Paper Series; 83. Trento: Università degli Studi di Trento.

STUDENT PAPER N.82

La responsabilità civile da deficit organizzativo del sistema sanitario e l'emergenza pandemica: una comparazione fra Germania e Italia

JESSICA RIVA. La responsabilità civile da deficit organizzativo del sistema sanitario e l'emergenza pandemica: una comparazione fra Germania e Italia. Trento Law and Technology Research Group, Student Paper Series; 82. Trento: Università degli Studi di Trento.

STUDENT PAPER N. 81

La vaccinazione infausta fra tutela indennitaria e risarcitoria: infausta fra tutela indennitaria e risarcitoria: la gestione del danno da vaccino dopo la pandemia

VERONICA MAYRHOFER. La vaccinazione infausta fra tutela indennitaria e risarcitoria: la gestione del danno da vaccino dopo la pandemia, Trento Law and Technology Research Group, Student Paper Series; 81. Trento: Università degli Studi di Trento.

STUDENT PAPER N. 80

La responsabilità civile per i veicoli a guida autonoma nell'ordinamento tedesco: spunti per il legislatore italiano

ELENA TOGNON, La responsabilità civile per i veicoli a guida autonoma nell'ordinamento tedesco: spunti per il legislatore italiano, Trento Law and Technology Research Group, Student Paper Series; 80. Trento: Università degli Studi di Trento.

STUDENT PAPER N. 79

La tutela delle indicazioni geografiche per i prodotti non comparabili: il ruolo dei gruppi di produttori nella valorizzazione del segno

MARTINA DURIGON, La tutela delle indicazioni geografiche per i prodotti non comparabili: il ruolo dei gruppi di produttori nella valorizzazione del segno, Trento Law and Technology Research Group, Student Paper Series; 79. Trento: Università degli Studi di Trento.

STUDENT PAPER N. 78

Il diritto alle prese con la vulnerabilità del turismo, fra guerra e persistente pandemia

FRANCESCA ROMANA BARBA; GIACOMO MARTINO BELLUZZO; SEBASTIANO BORILE; MATTEO BUDELLINI; CHIARA BUOSI; WIKTOR BURIGO; PAOLO CAPOTI; SERENA CARRUBBA; ALESSANDRA CASAGRANDE; FEDERICO DE VINCENZO; EMILIA FASCINELLI; CATERINA FAVA; ANTONIO FERRARO; CAROLINA FILICE; ALESSIA GIZZARELLI; ARIANNA LANEVE; MATTIA LEONE; MARTINA LUCE; MATTEO MAIOLI; 227 ALESSANDRO MARRAS; SARA MATTÈ; ILARIA MELCHIORETTO; ALESSIO MIRA; GIULIA MOCANU; DANIELA NESPOLO; ALESSANDRO OLIVA; ELENA PAGLIAI; ALESSANDRO PALLAORO; SILVIA PEDROTTI; GIACOMO PILI; ALFIO RACITI; FRANCESCA RIZZI, SARA ROSSO; SARA SCARAMUZZA; MARTINO SERAFINI; ELISA SERVIDIO; DENIS SOMMARIVA; CAROLA STEFENELLI; MARTINA TADDEI; JENNY TURRIN (2022), Trento Law and Technology Research Group, Student Paper Series; 78. Trento: Università degli Studi di Trento.

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, L'enforcement del diritto d'autore e la tutela dei dati personali: il nuovo art. 17 Dir. 2019/790, Trento Law and Technology Research Group, Student Paper Series; 77. Trento: Università degli Studi di Trento.

STUDENT PAPER N. 76

Il binomio «sport e salute» nella riforma del diritto dello sport: istituzioni, strutture,

professionalità e responsabilità

NICOLA INTRONA (2022), Il binomio «sport e salute» nella riforma del diritto dello sport: istituzioni, strutture, professionalità e responsabilità, 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), La libertà di panorama: profili critici e spunti comparatistici, Trento Law and Technology Research Group, Student Paper Series; 75. Trento: Università degli Studi di Trento.

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.

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.

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'ÉVA, MARTINA; DELMARCO, MARTINA; DELLA MURA, MARCO; DI MASCIÒ, 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 TRENCHI (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; BORTOLOTTI, FABIO; BRUZZO, PIERLUIGI; CALZOLARI, GIULIA; CAMPOS SANTOS, DIEGO; CARLINO, PIETRO; CAVALLERA, LORENZO; CEPAROTTI, 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, AYLÀ; 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 confronto, 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

MAGGILO 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 judgements 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 judgements 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 University, 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 Analysis 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 Analysis

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)

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).

