UNIVERSITY OF TRENTO
Faculty of Law

lawtech

Trento Law and Technology Research Group
Student Paper n. 87

RESPONSABILITÀ E ACCOUNTABILITY IN MATERIA DI PROTEZIONE DEI DATI PERSONALI: IL CONTESTO DELL'INTERNET OF THINGS

Andrea Blatti

About the author

Andrea Blatti (andreafrancescoblatti@gmail.com) graduated in Law at University of Trento under the supervision of Prof. Roberto Caso (March 2023).
The opinion stated in this paper and all possible errors are the Author's only.

KEY WORDS

Privacy – Protezione dei dati personali – Accountability – Internet of Things - Responsabilità

Sull'autore

Andrea Blatti (andreafrancescoblatti@gmail.com) ha conseguito la Laurea in Giurisprudenza presso l'Università di Trento con la supervisione del Prof. Roberto Caso (Marzo 2023).
Le opinioni e gli eventuali errori contenuti sono ascrivibili esclusivamente all'autore.

PAROLE CHIAVE

Privacy – Protezione dei dati personali – Accountability – Internet of Things - Responsabilità

RESPONSABILITÀ E ACCOUNTABILITY IN MATERIA DI PROTEZIONE DEI DATI PERSONALI: IL CONTESTO DELL'INTERNET OF THINGS

Abstract

This work aims to investigate the adequacy of accountability and civil liability systems in the context of the *Internet of Things*.

In order to carry out this examination, different approaches have been used: in particular, the benefits of historical, sociological and technical analysis have been relied upon, to be integrated with the study of norms, decisions and practices typical of the jurist.

The first chapter aims to provide the main coordinates for understanding the phenomenon of the *Internet of Things*: this required a historical and technical approach, albeit minimal. Today's state of the art is in fact the result of the development of fundamental technologies such as *cloud computing*, and the more modern *edge computing* and *fog computing*. These, in turn, required an introduction to how they work.

In the second chapter, the focus shifted to the relationship between law and technology, with a focus on digital technologies. The protection of personal data, that is the subject of this thesis can in fact be traced back to the vast field of studies known as Law&Tech, characterised by the influence that technology exerts on law.

In addition to this, the second chapter was dedicated to the framing of personal data, the object of the protection of the discipline under examination. The main reference was Article 4 of the GDPR and Opinion No. 4 of 2007 of the Article 29 Working Party. The latter, by issuing soft law acts (opinions and guidelines) plays a key role in the interpretation of data protection provisions. A great importance was attached to soft law in the course of the thesis: the acts of the European Data Protection Board, of the Italian Data Protection Authority, of the European Data Protection Supervisory, and the European agencies (such as Enisa) constitute first-rate references for the analysis of regulatory texts and for the evaluation of technological implementation practices.

The third chapter was devoted to the *accountability* principle. This has been considered by important commentators as the element on which the modernisation of the data protection discipline was based: it was in fact introduced by the GDPR, and in contrast to the former Directive 95/46/EC, it imports a series of obligations aimed to making the main figures accountable for processing: the controller and the processor.

This paradigm shift is analysed by retracing the main stages that led to today's accountability principle, with particular emphasis on the minimum security measures provided for in Article 33 of the former Italian privacy code.

The fourth chapter focuses instead on civil liability for unlawful processing of personal data. The reference provision is Article 82 of the GDPR, and starting from it, the active and passive subjective profiles, the objective profiles, the nature of the criterion of imputation of liability, and the relationship between the injured party and the damaging party were examined. The protracted study took into consideration the unresolved problems of Italian civil liability, especially as regards the criterion of imputation of liability and the relationship between the injured party and the damaged party.

This analysis was supplemented by a systematic reading of the Regulation, with the consequence of finding the minimum and maximum limits of civil liability in the compliance with the principle of accountability. In particular, the balance set by the GDPR between the circulation and protection of personal data, the principle of adequacy, and finally the limits of the state of the art and implementation costs were examined.

The results obtained in the third and fourth chapters on accountability and civil liability systems were then tested in the context of the *Internet of Things*. This necessitated an introduction on the circulation model of personal data, and the risks arising from it: in particular, algorithmic discrimination and influences on personal self-determination were examined.

Algorithms were taken into consideration, by virtue of their great inferential capacity, as tools for the extraction of new data, sometimes burdened by biases imprinted at the time of design, and at other times vitiated by biases that emerged later than the time of programming.

Respecting the principle of accountability in the *IoT*, so as not to be condemned for damages under Article 82 GDPR, is very complex. The technological phenomenon in question is very intricate, characterised by great opacity and chains of processing. The lack of transparency makes it complex to be accountable, while the concatenation of accountable treatments, in certain cases, can lead to the inconsistency of personal data protection.

Finally, some problematic liability profiles linked to the industrialisation of relations were compared to those arising from their digitalisation.

RESPONSABILITÀ E ACCOUNTABILITY IN MATERIA DI PROTEZIONE DEI DATI PERSONALI: IL CONTESTO DELL'INTERNET OF THINGS

Abstract

Il presente elaborato nasce dall'intento di indagare l'adeguatezza dei sistemi di responsabilizzazione e responsabilità civile nell'*Internet of Things*.

Per operare tale disamina si è proceduto mediante diversi approcci: in particolare, si è fatto affidamento sui benefici dell'analisi storica, sociologica e tecnica, da integrare allo studio delle norme, delle decisioni e delle prassi tipico del giurista.

Il primo capitolo si pone l'obiettivo di fornire le coordinate principali per la comprensione del fenomeno dell'*Internet of Things*: ciò ha richiesto un approccio, seppur minimo, di tipo storico e tecnico. L'odierno stato dell'arte si deve infatti allo sviluppo di tecnologie fondamentali quali il *cloud computing*, e le più moderne *edge computing* e *fog computing*. Queste, a loro volta, hanno richiesto un'introduzione relativa al loro funzionamento.

Nel secondo capitolo si è invece spostata l'attenzione sul rapporto tra diritto e tecnologia, con *focus* sulle tecnologie digitali. La protezione dei dati personali oggetto della tesi è infatti riconducibile al vasto ambito di studi conosciuto come Law&Tech, caratterizzato dall'influenza che la tecnologia esercita sul diritto.

Oltre a ciò, il secondo capitolo è stato dedicato all'inquadramento del dato personale, oggetto della tutela della disciplina in esame. Si è preso come riferimento principale l'articolo 4 del GDPR e il parere numero 4 del 2007 del Gruppo di lavoro *ex* articolo 29. Quest'ultimo, mediante l'emanazione di atti di *soft law* (pareri e linee guida) gioca un ruolo fondamentale per l'interpretazione delle disposizioni relative alla protezione dei dati personali. Proprio al *soft law* è stato attribuito grande importanza nel corso dell'intera trattazione: gli atti del Gruppo di lavoro, del Garante italiano, del Garante europeo e di agenzie europee (quali ad esempio l'Enisa) costituiscono riferimenti di prim'ordine dell'analisi dei testi normativi e per la valutazione delle prassi tecnologiche applicative.

Il terzo capitolo è stato dedicato al principio di *accountability*. Questo è stato considerato da importanti commentatori l'elemento su cui basare l'ammodernamento della disciplina della protezione dei dati personali: esso è infatti stato introdotto dal GDPR, e differentemente rispetto a quanto previsto dalla direttiva madre, importa una serie di obblighi volti a responsabilizzare le figure principali del trattamento: il titolare ed il responsabile del trattamento.

Tale mutamento di paradigma è stato analizzando ripercorrendo le principali tappe che hanno portato all'odierno principio di accountability, con particolare enfasi sulle misure minime di sicurezza previste dall'articolo 33 del vecchio codice privacy.

Il quarto capitolo è invece incentrato sulla responsabilità civile da illecito trattamento dei dati personali. La disposizione di riferimento è l'articolo 82 del GDPR, e partendo da essa sono stati esaminati i profili soggettivi attivi e passivi, i profili oggettivi, la natura del criterio di imputazione della responsabilità, e il rapporto intercorrente tra danneggiato e danneggiante. Lo studio protratto ha tenuto in considerazione i problemi irrisolti della responsabilità civile, soprattutto in merito al criterio di imputazione della responsabilità e al rapporto tra danneggiante e danneggiato.

Tale analisi è stata integrata mediante una lettura sistematica del Regolamento, con la conseguenza di rinvenire i limiti minimi e massimi della responsabilità civile nel rispetto del principio di *accountability*. In particolare, sono stati esaminati l'equilibrio fissato dal GDPR tra circolazione e protezione dei dati personali, il principio di adeguatezza, e infine i limiti dello stato dell'arte e dei costi di attuazione.

I risultati ottenuti nel terzo e nel quarto capitolo sui sistemi di responsabilizzazione e responsabilità civile sono poi stati testati nel contesto dell'*Internet of Things*. Ciò ha imposto un'introduzione sul modello di circolazione dei dati personali, e dei rischi che da questo derivano: in particolare sono state esaminate la discriminazione algoritmica e le influenze sull'autodeterminazione della persona.

Gli algoritmi sono stati presi in considerazione, in virtù della loro grande capacità inferenziale, come strumenti per l'estrazione di nuovi dati, talvolta gravati da *bias* impressi al momento della progettazione, e altre volte viziati da pregiudizi emersi in momenti successivi rispetto a quello della programmazione.

Il rispetto del principio di *accountability* nell'*IoT*, di modo da non essere condannati al risarcimento del danno previsto dall'articolo 82 GDPR, risulta assai complesso. Il fenomeno tecnologico in questione è assai intricato, caratterizzato da grande opacità e da catene di trattamenti. La mancanza di trasparenza rende complesso essere *accountable*, mentre la concatenazione di trattamenti *accountable*, in certi casi, può comportare l'inconsistenza della protezione dei dati personali.

Infine, sono stati paragonati alcuni profili problematici della responsabilità civile legati alla industrializzazione dei rapporti a quelli derivanti dalla digitalizzazione degli stessi.

Indice

RESPONSABILITÀ E ACCOUNTABILITY IN MATERIA DI PROTEZIONE DEI DATI PERSONALI: IL CONTESTO DELL'INTERNET OF THINGS

Introduzione

Il concetto di *Internet of Things* (*IoT*) si riferisce ad un fenomeno complesso, da intendersi come un insieme di oggetti intelligenti (*smart objects*), capaci di identificare o essere identificati in modo univoco, interconnessi tra loro attraverso internet (o senza Internet), capaci di percepire la realtà fisica in molteplici modi, sia mediante un *input* umano sia autonomamente.

La complessità dell'*IoT* in questione è ben rappresentata dall'etimologia del termine: dal latino *complexus*, "tessuto insieme". Ogni analisi sul tema, infatti, finisce per includere diverse discipline, ingegneristiche, sociologiche, sull'etica, e non ultime quelle giuridiche, dal diritto civile, al diritto costituzionale e penale. L'analisi del fenomeno verrà dunque protratta attraverso il metodo interdisciplinare, strumento fondativo e fondamentale del *Law & Technology*. L'elaborato che si presenta si propone di indagare l'impianto della responsabilità civile derivante da trattamento illecito di dati personali all'interno del contesto dell'*Internet of Things*, che richiederà un'analisi dell'elemento maggiormente caratterizzante la responsabilità: il principio di *accountability*.

Nel primo capitolo si introdurrà l'Internet delle cose. Dai primi *smart objects* riconducibili a tale fenomeno, alla loro evoluzione, sino ad arrivare agli elementi tecnologici maggiormente rilevanti oggigiorno: il *cloud computing*, il *fog computing*, l'*edge computing*, e gli algoritmi di *machine learning*, veri attori moderni (ma soprattutto futuri) dell'era digitale. Oltre ciò, verranno offerti i più diffusi esempi di ambienti interconnessi, dalla *smart home*, alle *smart cars*, sino ad arrivare ad applicazioni di dettaglio, quali *smartwatches* o sistemi di gestione del traffico.

Il secondo capitolo invece è dedicato innanzitutto al rapporto tra diritto e tecnologia. Nello specifico si esporrà l'esempio della protezione dei dati personali, disciplina che continua a modificarsi in forza dei mutamenti tecnologici. Il rapporto tra *Law* & *Technology* verrà descritto scomponendolo in quattro fasi: l'innovazione tecnologica; l'espandersi di interessi socialmente rilevanti; l'intervento della dottrina e della giurisprudenza; ed infine l'eventuale approdo legislativo. Nel proseguo del capitolo verranno forniti alcuni elementi fondamentali della disciplina della protezione dei dati personali: rilevanti ai fini dell'elaborato: le fonti, con particolare riguardo al Regolamento sulla protezione e circolazione dei dati personali (GDPR), il concetto di dato personale, la pseudonimizzazione e l'anonimizzazione.

Il terzo capitolo sarà dedicato invece al principio di *accountability*, considerato la chiave di volta per l'interpretazione delle norme del

Regolamento. Esso ha costituito il principio maggiormente innovatore rispetto alla normativa previgente, basata sulla Direttiva 95/46 CE. Il concetto sottostante tale principio è stato tradotto (forse poco opportunamente) dal testo italiano del Regolamento come "responsabilizzazione". Esso richiede da un lato che sia garantita la conformità al GDPR, dall'altro che tale conformità possa essere in ogni momento essere dimostrata.

Il quarto capitolo invece si concentrerà sull'articolo 82 GDPR, norma principe dell'impianto di responsabilità fissato dal GDPR. La disposizione in esame risulta tuttavia complessa, richiedendo all'interprete di analizzare ogni suo elemento per un'applicazione concreta. Dopo aver inizialmente chiarito chi siano i soggetti obbligati a rispondere ai sensi della citata norma, si procederà alla ricostruzione del criterio d'imputazione della responsabilità e alla delineazione del rapporto, contrattuale o extracontrattuale, che lega il titolare del trattamento e l'interessato. Si dedicherà un paragrafo specifico al criterio della responsabilità oggettiva per rischio d'impresa, dottrina di successo elaborata in Italia negli anni Sessanta. Si descriveranno i limiti normativi della responsabilità: lo stato dell'arte e i costi di attuazione. Infine, si evidenzierà lo stretto legame tra il principio di *accountability* e il sistema di responsabilità civile stabilito dal Regolamento.

Il quinto ed ultimo capitolo indagherà invece il rapporto tra il principio di *accountability* e l'Internet delle cose. Innanzitutto, si descriverà brevemente l'odierno modello di circolazione dei dati personali, prendendo come spunto la celeberrima dottrina del "capitalismo della sorveglianza". In un secondo momento verranno discussi alcuni dei rischi derivanti dal trattamento dei dati personali nei contesti di *Internet of Things*, in particolare il pericolo di discriminazione e di autodeterminazione, sia individuale che collettiva. Si farà dunque un breve riferimento alla dimensione collettiva della privacy. L'analisi del principio di *accountability* nell'*Internet of Things* seguirà l'indagine di alcune norme specifiche, di particolare difficoltà applicativa, quali quelle relative al principio di trasparenza o di *data protection by design*. L'ultimo paragrafo verterà infine su alcuni problemi rinvenibili nel rapporto tra *accountability*, responsabilità ed *Internet of Things*.

Capitolo 1 - L'*Internet of Things (IOT)*.

1.1 Le origini e lo sviluppo dell'*Internet of Things*

1.1.1 Le origini

Nel 1999, Kevin Ashton, assistente *brand manager* presso Procter & Gamble (in seguito P&G), si accorse che una determinata cromia di rossetto spariva ripetutamente dagli scaffali del suo negozio. Notò che anche negli altri negozi di P&G quella stessa tinta terminava prima delle altre. Indagando sulla catena di fornitura scoprì che in realtà il magazzino era sempre pienamente rifornito, e che l'errore era stato commesso da qualche addetto ai lavori. L'inventario era gestito tramite lettore di codice a barre da una persona, e come di sovente accade quando grandi quantità di dati sono gestite da un essere umano, quei dati (relativi alla presenza o mancanza dei rossetti) erano inesatti.

L'espressione *Internet of Things* (in seguito: *IoT*) nasce come titolo di una presentazione dello stesso Ashton per P&G. L'obiettivo era quello di migliorare la catena di fornitura dell'impresa, e il mezzo per conseguirlo era la tecnologia *radio frequency identification* (in seguito *RFID*), ossia

> «una tecnologia per la localizzazione di oggetti mediante segnali radio. Creata nel 1998 presso il MIT, si basa su etichette (tags) contenenti le informazioni relative all'oggetto su cui sono poste, che entro una certa distanza fisica possono essere lette da un apposito apparecchio capace di captare i segnali radio riflessi o emessi dal tag stesso»[1].

L'obiettivo della presentazione di Ashton era quello di convincere l'impresa a collegare tale tecnologia *RFID* alla rete Internet in modo da consentire ai chip di comunicare le informazioni relative alla presenza o assenza dei beni venduti da P&G. Ciò a cui Ashton mirava era l'abolizione dell'errore umano.

Nell'articolo "*That "Internet of things" thing"* del 2009, quindi 10 anni dopo la prima enunciazione dell'espressione, Ashton spiegava cosa intendesse nella sua prima presentazione. Scriveva che alla fine degli anni '90 i computer erano ancora essenzialmente dipendenti dall'essere umano.

[1] Enciclopedia Treccani, voce *RFID*, disponibile online al seguente link: https://www.treccani.it/enciclopedia/rfid/#:~:text=Sigla%20di%20radio%20frequency%20identification,di%20oggetti%20mediante%20segnali%20radio

Senza quest'ultimo, infatti, le macchine non potevano ottenere alcuna informazione in merito al mondo esterno: serviva un'azione umana, un *input*. Internet era ancora l'Internet delle persone. Proprio in questa azione umana necessaria egli vedeva il principale limite dei computer, e così scriveva che se fosse stato possibile avere computer capaci di conoscere tutto ciò che riguarda il mondo fisico, attraverso dati raccolti da essi stessi in modo autonomo, sarebbe stato possibile tracciare e contare tutto, riducendo così in grande misura perdite, sprechi e costi. Si sarebbe anche stati in grado di sapere quando manutenere gli oggetti e quando sostituirli. Per fare ciò sarebbe stato necessario implementare i computer in modo da dotarli di un'autonoma percezione della realtà in tutte le sue forme. Il tutto attraverso la tecnologia *RFID* e i sensori di modo che questi possano osservare, identificare e comprendere il mondo senza il necessario *input* umano[2].

Dalla presentazione del 1999 di Ashton il mondo prende coscienza delle potenzialità di un Internet delle cose: un Internet formato da oggetti intelligenti (o *smart objects*[3]) connessi tra loro, in grado di comunicare anche senza l'intervento umano. Sebbene questo venga considerato il momento in cui il mondo scopre l'*IoT*, vi sono degli esempi di oggetti intelligenti connessi tra loro risalenti a momenti precedenti la presentazione di Ashton del 1999.Nel 1990 John Romkey inventa quello che ad oggi viene ancora considerato il primo esempio di *smart object*: un tostapane in grado di attivarsi ed essere utilizzato attraverso la rete Internet[4]. Nel 1993 gli Stati Uniti permettono ai civili di utilizzare il segnale *Global Positioning System* (in seguito: *GPS*), prima destinato ad uso esclusivamente militare. Quando il ricevitore *GPS* (es. *smartphones*, navigatori satellitari o orologi) si attiva per rilevare la posizione, si collega al segmento spaziale (satelliti) e al segmento di controllo (basi di controllo terrestri), in modo da triangolare e comunicare la posizione dell'utente nella misura più precisa possibile. Un altro antenato degli odierni dispositivi *IoT* è lo strumento di sicurezza automobilistico OnStar, distribuito nel 1996 da General Motors, che rendeva molto più semplice ed immediato richiedere assistenza in situazioni di emergenza; anziché utilizzare il cellulare, infatti, bastava premere un bottone, contattando così un operatore in grado di localizzare il veicolo e quindi occuparsi da remoto della situazione di emergenza. Oltretutto, nell'eventualità di un incidente, il dispositivo era anche in grado di comunicare la posizione dell'abitacolo in maniera autonoma, senza che fosse necessaria un'azione umana. In caso di incidente o nel caso in cui il guidatore avesse premuto il pulsante di assistenza, il sistema OnStar avrebbe

[2] Ashton K., *That "Internet of things"* thing, Journal, 22 Giugno 2009, disponibile online al seguente link: https://www.rfidjournal.com/that-internet-of-things-thing

[3] Firouzi F., Chakrabarty K., Nassif S. (edito da), *Intelligent Internet of Things*, Springer, Cham, 2020, pag. 52.

[4] Bouhai N., Saleh I., *Internet of Things: Evolutions and Innovations*, John Wiley & Sons Inc., 29 Novembre 2017, pag. 22.

fatto partire una chiamata di emergenza ad una torre di telecomunicazione, comunicando anche la posizione. La torre avrebbe reindirizzato la chiamata al primo operatore disponibile, trasmettendo anche la posizione dell'abitacolo, di modo che si potesse avviare la procedura di soccorso.

Questi sono alcuni degli esempi di *smart objects* del ventesimo secolo[5]. In quel periodo questi oggetti venivano connessi reciprocamente al precipuo scopo di migliorare servizi di diagnostica ed assistenza. I dati raccolti venivano infatti trasferiti in *real time* dalla macchina a chi gestiva il servizio di manutenzione, e una volta effettuata questa, le informazioni raccolte venivano eliminate. Mancava ancora l'intuizione che avrebbe portato all'espansione dell'*IoT*: i dati raccolti per un determinato fine possono diventare enormemente preziosi se utilizzati per scopi ulteriori, o se uniti ad altri dati raccolti per altri fini.

1.1.2 Lo sviluppo

Allo sviluppo dell'*IoT* hanno contribuito fattori di diversa natura, che è opportuno cogliere per comprendere l'odierno stato dell'arte e anche le diverse previsioni prospettate in merito alla portata e alla diffusione futura di questi oggetti connessi. É da segnalare innanzitutto la consistente e continua diminuzione dei costi relativi ai componenti dei dispositivi, *in primis* i chip e i sensori[6] (che permettono appunto di captare informazioni dall'ambiente circostante), che ha reso possibile la progettazione e creazione di *smart objects* su larga scala, rivolti alla generalità del pubblico. A ciò si aggiunge la moderna possibilità di archiviare grandi quantità di dati infrastrutture digitali come il *cloud computing*[7] (cfr. 1.4.2) a costi accessibili alla maggior parte dei consociati e la diminuzione delle tariffe per la connettività ad Internet. L'espressione *Internet of Things* viene coniata in un momento, il 1999, in cui si era già capito che le potenzialità di questo modo di vedere Internet erano enormi, anche se non si era ancora compreso come sfruttarle appieno. Per descrivere quanto le prospettive fossero chiare già all'epoca è utile richiamare quanto nel 2005 affermava l'International Telecommunication Union (in seguito ITU), secondo cui la creazione dell'Internet delle cose avrebbe comportato la connessione di oggetti di uso comune a diversi tipi di reti, da quelle *peer-to-peer*, a quelle aziendali, ad Internet. Si era compreso il ruolo che avrebbe avuto nell'industria delle telecomunicazioni e che avrebbe portato alla nascita di nuovi modelli di

[5] Per altri esempi vedasi la *timeline* disponibile in:
http://IoToast.altervista.org/timeline/?doing_wp_cron=1653061814.7762238979339599609375

[6] Firouzi F., Chakrabarty K., Nassif S. (edito da), *Intelligent Internet of Things*, 2020, pag. 55.

[7] Definito come «paradigma che consente l'accesso in rete a un insieme scalabile ed elastico di risorse fisiche e virtuali con approvvigionamento self-service e amministrazione a richiesta», da Pascuzzi G., *Il diritto dell'era digitale*, Il Mulino, Bologna, 2020, pag. 265.

business[8]. In quegli anni mancavano però le tecnologie per rendere possibile quanto si intravedeva. Queste si sono però evolute in fretta per fronteggiare le sfide che stavano sorgendo.

Un fenomeno fondamentale che ha portato all'affermazione dell'*IoT* è quello dei *Big Data* (cfr. 1.4.1.), che il McKinsey Global Institute nel 2011 definiva «*datasets whose size is beyond the ability of typical database software tools to capture, store, manage, and analyze*»[9]. Tale definizione è particolarmente significativa in quanto restituisce il contesto tecnologico di quegli anni: le tecnologie relative alla raccolta dei dati erano superiori a quelle deputate all'immagazzinamento e all'elaborazione. In sostanza vi erano più dati di quanti se ne potessero effettivamente sfruttare. Storicamente, sfide come queste hanno portato ad una rapida evoluzione delle tecnologie: «è capitato, ad esempio, negli anni '80 del secolo scorso, quando per gestire i dati strutturati si è passati ai database relazionali»[10] . Con l'avvento dei *Big Data*, tuttavia, i database relazionali si sono rivelati infruttuosi in quanto non avevano le capacità computazionali per sorreggere il lavoro richiesto da questa nuova mole di dati (soprattutto quelli non strutturati[11]).

Tra le soluzioni trovate per far fronte alle sfide dei *Big Data*, molto importante risulta quella relativa al calcolo distribuito: «ovvero la possibilità di dividere un carico di lavoro tra più computer che operano in parallelo al fine di scambiarsi i risultati intermedi per giungere al prodotto finale»[12]. Difatti, risulta sconveniente progettare un'infrastruttura *IoT* basandola su un controllo centralizzato: la mole di informazioni raccolta metterebbe a dura prova le capacità di *storage* di simili sistemi e l'estensione delle capacità di immagazzinamento diverrebbe troppo onerosa. Da qui lo sviluppo di sistemi distribuiti, gestiti a livello fisico come *clusters* separati, ma con un solo file di sistema distribuito che permette la distribuzione dei dati eliminando il problema della scalabilità[13]. Dunque, il problema della

[8] ITU Internet Reports, *The Internet of things*, Novembre 2005, disponibile online al seguente link: https://www.itu.int/net/wsis/tunis/newsroom/stats/The-Internet-of-Things-2005.pdf

[9] McKinsey Global Institute, *Big Data*: *The next frontier for innovation, competition and productivity*, Maggio 2011, disponibile online al seguente link: https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/big%20data%20the%20next%20frontier%20for%20innovation/mgi_big_data_exec_summary.pdf

[10] Pascuzzi G., *Il diritto dell'era digitale*, 2020, pag. 267: il Database relazionale è un «database nel quale i dati sono utilizzati secondo un modello relazionale", che a sua volta è definito come un "modello di dati la cui struttura è basata su un set di relazioni». Ibidem, pag. 266.

[11] Ibidem, pag. 267, Per dati non strutturati si intende «dati caratterizzati dal non avere alcuna struttura che non sia quella di record o di file (esempio: testo libero)».

[12] Ibidem, pag. 268.

[13] Margioti F., *Internet of things (IoT): applicazioni e problematiche*, Settembre 2019, disponibile online al seguente link:
https://www.tuttoreti.it/index.php/articoli/windows/112-internet-of-things-IoT.html

scalabilità[14] è poi stato risolto con l'altra grande conquista nella sfida ai *Big Data*, ossia il c*loud computing*.

La mole di dati prodotta era in crescente aumento, e questo perché i dispositivi connessi erano sempre di più: per offrire un'idea basti pensare che tra il 2008 e il 2009, secondo Cisco[15], i dispositivi connessi ad Internet avevano superato il numero di persone nel mondo[16]; tra il 2013 ed il 2015 invece, secondo Bernard Marr[17], sono stati prodotti più dati che in tutta la storia dell'uomo fino a quel momento.

Come si vedrà nel paragrafo 1.4, la tecnologia ha fatto ulteriori balzi in avanti, si parla infatti oggi di *fog* ed *edge computing*. Per quanto concerne invece alcune previsioni per il prossimo futuro, secondo l'ultimo report annuale di Cisco[18] il numero di dispositivi connessi a reti mobili, entro il 2023, sarà superiore al triplo della popolazione globale; entro lo stesso anno oltre il 70% della popolazione mondiale sarà dotata di connessione mobile e circa 300 milioni di applicazioni verranno scaricate. L'*IoT* sembra dunque essere destinato ad espandersi, fino a diventare una parte fondamentale della quotidianità dell'uomo medio.

1.2 Definizioni.

1.2.1 Definizioni tecniche

Ogniqualvolta lo studioso tenta di illustrare *ex novo* una questione, uno dei primi punti da chiarire è l'inquadramento sintetico della stessa questione, ossia la sua definizione; tuttavia, alle volte ciò non risulta né agevole, né opportuno.

Dal punto di vista giuridico, per quanto concerne concetti come l'*Internet of Things*, la questione della definizione si manifesta in tutta la sua

[14] Il Cambridge Dictionary definisce la scalabilità come «*the ability of a business or system to grow larger*». Disponibile online al seguente link: https://dictionary.cambridge.org/it/dizionario/inglese/scalability

[15] Società specializzata nella fornitura di apparati di *networking* e molto presente nel processo di evoluzione dell'*IoT*.

[16] Evans D., Cisco, *The Internet of things How the Next Evolution of the Internet Is Changing Everything*, Aprile 2011, disponibile online al seguente link: https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

[17] Forbes, Marr B., *Big Data: 20 Mind-Boggling Facts Everyone Must Read*, Settembre 2015, disponibile online al seguente link:
https://www.forbes.com/sites/bernardmarr/2015/09/30/big-data-20-mind-boggling-facts-everyone-must-read/?sh=1f537a3217b1

[18] Cisco, *Annual Internet Report (2018–2023)*, disponibile online al seguente link: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.pdf

complessità. L'*IoT* rappresenta uno dei molteplici casi di incontro tra il mondo della tecnologia e quello del diritto, con quest'ultimo che, con molte difficoltà, tenta di imbrigliare il primo in atti aventi forza di legge, sentenze, ecc. (questo ambito di studio è conosciuto come "*Law and Technology*"). Sono molte le difficoltà che il diritto incontra nel fornire definizioni giuridiche relative ai fenomeni della tecnologia (o di altri settori estremamente tecnici), e questo costituisce la principale ragione per la quale non vi sono legislazioni che definiscono l'*Internet of Things*. Inquadrare un problema in poche o molte righe ed imprimere queste in un atto avente forza di legge non è però l'unico modo di approcciarsi giuridicamente a quel problema: si vedrà infatti come sia possibile affrontare un tema prescindendo dalla sua definizione. Gli operatori giuridici hanno da tempo familiarizzato con alcuni concetti per i quali risulta molto difficile offrire una definizione (si pensi alle nozioni di vita umana, di dignità, di genere, ecc.).

Se da un lato alle volte i legislatori non ritengono opportuno formulare le definizioni di questi concetti, dall'altro lato vi sono diverse altre scienze che soccorrono in aiuto dei giuristi. L'interdisciplinarità, intesa come metodo di studio dato dalla convergenza di diverse discipline che si integrano e interagiscono, è «motore di innovazione e progresso della conoscenza»[19] e costituisce oggi un fermo punto di partenza per la quasi totalità degli operatori del diritto. Per quanto concerne l'*IoT*, ad esempio, pur non essendoci una definizione legale, ve ne sono di altro genere: da quelle tecniche, fornite da organizzazioni internazionali competenti, ad altre più neutre.

Nel 2010, il Professor Rolf H. Weber definiva laconicamente l'*Internet of Things* come «*an emerging global Internet based information architecture facilitating the exchange of goods and services in global supply chain networks*»[20].

L'enciclopedia Treccani fornisce invece un'immagine (un po') più chiara, definendolo una «rete di oggetti dotati di tecnologie di identificazione, collegati fra di loro, in grado di comunicare sia reciprocamente sia verso punti nodali del sistema, ma soprattutto in grado di costituire un enorme network di cose dove ognuna di esse è rintracciabile per nome e in riferimento alla posizione»[21]. L' Institute of Electrical and Electronics Engineers (in seguito IEEE), un istituto internazionale formato da professionisti con l'obiettivo di promuovere l'ingegneria elettrica ed

[19] Caso R., *La società della mercificazione e della sorveglianza: dalla persona ai dati. Casi e problemi di diritto civile*, Ledizioni, Febbraio 2021, pag. 44.

[20] Rolf H. Weber, *Internet of things – New security and privacy challenges*, in "Computer Law & Security Review", volume 26, numero1, pag. 23, disponibile online al seguente link:

https://www.sciencedirect.com/science/article/pii/S0267364909001939?fr=RR-2&ref=pdf_download&rr=70ebfe5e5875f91f

[21] Enciclopedia Treccani, alla voce "Internet of things". Disponibile online al seguente link:

https://www.treccani.it/enciclopedia/internet-of-things_(Lessico-del-XXI-Secolo)

elettronica e le tecnologie dell'informazione tecnologica, invece, relativamente a contesti caratterizzati da un elevato numero di oggetti intelligenti interconnessi, afferma che

> «*Internet of Things envisions a self configuring, adaptive, complex network that interconnects 'things' to the Internet through the use of standard communication protocols. The interconnected things have physical or virtual representation in the digital world, sensing/actuation capability, a programmability feature and are uniquely identifiable. The representation contains information including the thing's identity, status, location or any other business, social or privately relevant information. The things offer services, with or without human intervention, through the exploitation of unique identification, data capture and communication, and actuation capability. The service is exploited through the use of intelligent interfaces and is made available anywhere, anytime, and for anything taking security into consideration*»[22].

Ancora, l'International Telecommunication Union (in seguito ITU), organizzazione internazionale delle Nazioni Unite che si occupa del settore dell'ICT (informazione, comunicazione e telecomunicazione), nel suo particolare organo permanente chiamato ITU-T, che si occupa di emettere raccomandazioni al fine di definire gli standard nelle telecomunicazioni e nell'uso delle onde radio, nel 2012 scriveva che l'*Internet of Things* è un'infrastruttura globale per la società dell'informazione, con implicazioni tecnologiche e sociali, che permette lo sviluppo di servizi avanzati attraverso l'interconnessione di oggetti fisici e virtuali, la raccolta, l'elaborazione e la comunicazione di dati e la capacità di identificazione [23]. La varietà di definizioni ad oggi offerte[24] rende evidente il perché non si abbiano legislazioni che provino a fissare con precisione il significato dell'espressione *Internet of Things*. Inoltre, nonostante già nel 1999 Ashton avesse coniato l'espressione, nel 2011 Cisco[25] osservava che esso «*did not yet exist in 2003*

[22] IEEE, *Towards a definition of the Internet of things (IoT)*, pag.74. Disponibile online al seguente link:
https://IoT.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf

[23] Raccomandazione ITU-T Y.2060, *Overview of the Internet of things*, Giugno 2012, pagina 1. Disponibile online al seguente link: https://www.itu.int/rec/T-REC-Y.2060-201206-I

[24] *Ex multis*, il Working Group RFID della European Technology Platform (ETP) nel 2008 scriveva «*The semantic origin of the expression is composed by two words and concepts: "Internet" and "Thing", where "Internet" can be defined as "The world-wide network of interconnected computer networks, based on a standard communication protocol, the Internet suite (TCP/IP)", while "Thing" is "an object not precisely identifiable" Therefore, semantically, "Internet of things" means "a world-wide network of interconnected objects uniquely addressable, based on standard communication protocols*», disponibile online al seguente link: https://docbox.etsi.org/erm/Open/CERP%2020080609-10/Internet-of-Things_in_2020_EC-EPoSS_Workshop_Report_2008_v1-1.pdf

[25] Cisco Systems Inc. è una multinazionale leader nel settore del *networking*.

because the number of connected things was relatively small given that ubiquitous devices such as smart-phones were just being introduced»[26]; come visto in precedenza nel paragrafo 1.1.1, infatti, la formazione dell'*IoT* odierno si deve allo sviluppo di alcuni fattori in momenti diversi, motivo per il quale non è ragionevole tentare di fornire un'unica definizione. Per ogni evoluzione tecnologica si aveva un nuovo e diverso tipo di *IoT*, e quindi una nuova definizione. Una delle principali difficoltà che si riscontra ogniqualvolta si tenti di definire tecnologie informatiche quali l'*IoT*, infatti, è la rapida evoluzione di queste[27].

Tutti questi repentini cambiamenti, tipici delle infrastrutture digitali, rendono poco prudente una definizione a livello legislativo, di per sé immobile.

1.2.2 Definizioni legali

Nel 1995 l'Unione europea (o Ue) adottava il primo atto vincolante avente portata generale in materia di protezione dei dati personali: la Direttiva 95/46/CE, la quale prevedeva all'articolo 29 l'istituzione di un gruppo di lavoro competente, tra le altre cose, a promuovere la coerente applicazione della suddetta direttiva all'interno dei paesi firmatari, il cosiddetto Gruppo di lavoro *ex* articolo 29 (o Gruppo di lavoro). Dall'entrata in vigore del Regolamento generale sulla protezione dei dati personali (in seguito GDPR) nel 2018, il Gruppo di lavoro non esiste più, ed al suo posto è stato istituito il Comitato europeo per la protezione dei dati personali (o il Comitato), il quale costituisce una continuazione del lavoro svolto dal gruppo di lavoro fondato sull'articolo 29; le raccomandazioni e gli altri atti di quest'ultimo sono comunque tutt'oggi validi (quando non sostituiti da altre *opinions* successive sullo stesso tema[28]) e costituiscono ancora un importante punto di riferimento negli studi in materia di protezione dei dati personali[29]. Nell'opinione numero 8 del 2014 (ad oggi l'unico parere sul tema) il gruppo di lavoro definiva l'*IoT*:

> «*an infrastructure in which billions of sensors embedded in common, everyday devices – "things" as such, or things linked to other objects or individuals – are*

[26] Evans D., Cisco, *The Internet of things How the Next Evolution of the Internet Is Changing Everything*, 2011.

[27] «La difficoltà di definire l'Internet degli oggetti è alimentata dal fatto che essa si evolve man mano che emergono nuovi paradigmi come cloud computing, big data, social networking…», Pascuzzi G., *Il diritto dell'era digitale*, 2020, pag. 254.

[28] Passaglia P., *Il sistema delle fonti normative in materia di tutela dei dati* personali, in Cuffaro V., D'Orazio R., Ricciuto V.*, I dati personali nel diritto europeo*, Giappichelli, Torino, 2019, pag. 108.

29 Il valore degli atti del Gruppo di lavoro è inquadrabile nella categoria del *soft law*: Ibidem, pag. 108.

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».[30]

Sempre in ambito unionale, si è avvertita la necessità di affiancare al GDPR una regolamentazione indirizzata in maniera specifica alle comunicazioni elettroniche, sfociata nella proposta di regolamento sul rispetto della vita privata e sulla protezione dei dati personali nelle comunicazioni elettroniche[31]. In questa proposta, al Considerando 12[32], l'Internet delle cose viene menzionato espressamente, e definito come «*services involving an automated transfer of data and information between devices or software-based applications with limited or no human interaction*». Al momento, nell'ordinamento giuridico europeo, non è possibile trovare una definizione legislativa di *IoT*, e questo, come anticipato, in virtù dell'inopportunità di definire un fenomeno particolarmente complesso ed estremamente soggetto a cambiamenti repentini. Un approccio simile, ossia senza una espressa definizione, lo si ha negli Stati

[30] Opinione 8/2014 del Gruppo di lavoro *ex* articolo 29. Disponibile online al seguente link:https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf.

[31] Proposta di regolamento del Parlamento europeo e del Consiglio relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche e che abroga la direttiva 2002/58/CE (regolamento sulla vita privata e le comunicazioni elettroniche), disponibile online al seguente link: https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf

[32] Considerando 12: «*The use of machine-to-machine and Internet of things services, that is to say services involving an automated transfer of data and information between devices or software-based applications with limited or no human interaction, is emerging. In order to ensure full protection of the rights to privacy and confidentiality of communications, and to promote a trusted and secure Internet of things in the digital single market, this Regulation, in particular the requirements relating to the confidentiality of communications, should apply to the transmission of such services. The transmission of machine-to-machine or Internet of things services regularly involves the conveyance of signals via an electronic communications network and, hence, constitutes an electronic communications service. This Regulation should apply to the provider of the transmission service if that transmission is carried out via a publicly available electronic communications service or network. Conversely, where the transmission of machine-to-machine or Internet of things services is carried out via a private or closed network such as a closed factory network, this Regulation should not apply. Typically, providers of machine-to-machine or Internet of things services operate at the application layer (on top of electronic communications services). These service providers and their customers who use IoT services are in this respect end-users, and not providers of the electronic communication service and therefore benefit from the protection of confidentiality of their electronic communications data. Specific safeguards could also be adopted under sectorial legislation, as for instance Directive 2014/53/EU*».

Uniti, che considerano il California Consumers Privacy Act[33] (in seguito CCPA), unitamente al SB-327[34], gli atti di legge di riferimento in materia di protezione dei dati personali in tema di Internet delle cose.

Alla luce di quanto appena visto è possibile affermare che per quanto la soluzione definitoria sia importante, questa non sia imprescindibile. In alcuni casi è possibile ed opportuno definire un concetto, in altri invece non lo è. É possibile accogliere tutte le proposte definitorie finora esposte tentando di tracciare gli elementi in comune. Ai fini della presente tesi si tratterà l'*Internet of Things* come un insieme di oggetti intelligenti (*smart objects*), ossia capaci di identificare e/o essere identificati in modo univoco, interconnessi tra loro attraverso Internet (o senza Internet), capaci di percepire la realtà fisica in molteplici modi, sia attraverso un *input* umano sia autonomamente.

1.3 Profili applicativi

1.3.1 Ambiti e casi applicativi, i vantaggi di un sistema *IoT*

La tecnica definitoria, quando possibile e opportuna, viene considerata l'opzione migliore per l'inquadramento di una questione; in alcuni casi, tuttavia, ciò non risulta possibile e diviene necessario chiarire la tematica in altro modo. In queste situazioni il metodo più semplice e intuitivo è l'esemplificazione: offrire un contesto che consenta all'uditore o al lettore la ricostruzione, attraverso l'immaginazione, del problema in esame. L'*IoT*, come visto nei paragrafi precedenti, è un fenomeno tecnologico poco opportuno da definire. Lo stato dell'arte degli studi sul tema, nella maggior parte dei casi, mostra come si preferisca prescindere dal definire con puntualità l'Internet delle cose, e come invece si opti per l'esemplificazione, anche attraverso l'utilizzo di immagini e grafici. Nel presente paragrafo si procederà all'illustrazione di alcuni settori tipici dell'*IoT*. I settori che verranno evidenziati non esauriscono gli ambiti nei quali è possibile rinvenire architetture *IoT*[35], in quanto, come già evidenziato (cfr. 1.1.2.), la rapida evoluzione di queste tecnologie rende impossibile la previsione delle future applicazioni.

[33] California Consumer Privacy Act (CCPA): *Ex multis* si vedano l'articolo 1798.140, lettere E n.8, J e X.

[34] Senate Bill 327: si veda l'articolo 1798.91.05 lettera B.

[35] Per una lista delle possibili applicazioni vedasi Geng H., *The internet of things and data analytics handbook*, John Wiley & Sons, Inc.,, New Jersey (Hoboken) e Canada, 2017, pag. 12.

A. Smart city

Un (macro)settore rilevante nel mondo dell'*IoT* è quello delle città intelligenti, o *smart cities*. In Italia se ne hanno già alcuni esempi importanti, quali Milano, Firenze o Bologna, e nei prossimi anni, visto il progetto di transizione digitale intrapreso dall'Italia, questo fenomeno è destinato a divenire sempre più diffuso. Così come per l'Internet delle cose, anche per le città intelligenti non si ha una definizione legale; soccorrono dunque gli studi protratti in seno ad altre discipline. Per *smart city*, può dunque intendersi «*a place where traditional networks and services are made more efficient with the use of digital solutions for the benefit of its inhabitants and business*»[36]; benefici che si sostanziano, ad esempio, in trasporti urbani più intelligenti, in infrastrutture in grado di gestire al meglio le riserve idriche evitando sprechi, capaci di illuminare e riscaldare edifici in maniera efficiente.

L'intelligenza di queste città è data dalla loro capacità di relazionarsi autonomamente all'ambiente circostante, dalla loro abilità di sentire cosa accade all'esterno. Ciò è possibile attraverso la raccolta dati effettuati da sensori atti a monitorare le infrastrutture pubbliche (ponti, edifici, strade ecc.), in quanto ciò elimina l'esigenza di fissare regolari ispezioni e controlli, riducendo così i costi[37]. In quest'ultima citazione si ritrovano le parole di Kevin Ashton[38], che nel 1999 si riferivano a singoli computer, mentre oggi possono essere riportate in relazione ad un'intera città. Quest'ultima, attraverso sensori e dispositivi, percepisce l'ambiente circostante e i cittadini nell'ottica di una vasta fornitura di servizi. La capacità di avvertire, di sentire quanto avviene, si deve alla possibilità di acquisire una enorme mole di informazioni. Il passaggio da una normale città ad una *smart city* «è, pertanto, rappresentato dall'avvento dei c.d. *Big data*»[39] e «il connubio *Big*

[36] Portale ufficiale della Commissione europea. Disponibile online al seguente link: https://ec.europa.eu/info/eu-regional-and-urban-development/topics/cities-and-urban-development/city-initiatives/smart-cities_en

[37] Hancke G. P., De Carvalho B., Hancke G. P. Jr, *The Role of Advanced Sensing in Smart Cities*, Dicembre 2012. Disponibile online al seguente link: https://www.mdpi.com/1424-8220/13/1/393/htm

[38] Ashton K., 1999: «*If we had computers that knew everything there was to know about things—using data they gathered without any help from us — we would be able to track and count everything, and greatly reduce waste, loss and cost. We would know when things needed replacing, repairing or recalling, and whether they were fresh or past their best. We need to empower computers with their own means of gathering information, so they can see, hear and smell the world for themselves, in all its random glory. RFID and sensor technology enable computers to observe, identify and understand the world—without the limitations of human-entered data*».

[39] Ferrari G. F. (a cura di), *La prossima città*, Milano, 2017. Disponibile online al seguente link:
https://www.academia.edu/49346537/LA_PROSSIMA_CITT%C3%80

Data e *Internet of Things* (*IoT*) trova nel modello *smart city* la sua ideale trasposizione pratica»[40].

Le definizioni sono molteplici[41], ma convergenti: la *smart city* è dunque un contesto in cui utenti e città (nelle sue specifiche articolazioni) interagiscono attraverso tecnologie intelligenti. Per offrire una rappresentazione più concreta di come avvenga questa interazione tra città e persone si proporranno alcuni esempi: wi-fi pubblici, *smart mobility* e *smart surveillance*, ricordando che con questi non si intende esaurire gli ambiti applicativi dell'*IoT* in una città.

Partendo dal *wi-fi* pubblico (o *hotspot*) e dalla sua definizione (non legale), esso può essere inteso come: «un luogo fisico in cui le persone possono accedere a Internet, in genere tramite *wi fi*, sfruttando una rete locale senza fili (*WLAN*) con un *router* collegato a un provider Internet»[42]. Gli *hotspot* sono già molto diffusi ed in crescente aumento: li si trova nelle strade, nei parchi, nelle biblioteche, nei cimiteri, negli aeroporti, nei treni, nelle università ecc. I vantaggi consistono, quando si usa lo *smartphone*, nella possibilità di accedere ad Internet senza necessità di utilizzare le proprie tariffe personali; quando invece si utilizzano *tablets* o *pc*, nell'avere accesso ad Internet che altrimenti (nella maggior parte dei casi) risulterebbe impossibile. Oggigiorno moltissime attività, sia professionali che ludiche, e la maggior parte delle comunicazioni (messaggistica istantanea, e-mail, videochiamate ecc.) si svolgono online, dunque, gli *hotspot* consentono di non interrompere diversi aspetti importanti della quotidianità.

Proseguendo, quando si parla di *smart mobility*, si fa riferimento ad una serie di servizi *IoT* che perseguono obiettivi di diversa natura: «*to reducing pollution, traffic congestion (citizens' quality of life), pedestrian and driver safety as well as making the transport network more efficient and easier to manage*[43]», grazie all'accesso informatico ai mezzi di trasporto pubblici, alla gestione intelligente dei parcheggi e allo *sharing* dei mezzi di trasporto privati. La definizione del concetto di mobilità intelligente risulta molto complesso perché particolarmente composito, difatti spesso si preferisce procedere attraverso l'esemplificazione di casi che ne denotano

---

[40] Ibidem.

[41] *Ex multis*: Weber M., Lučić D., Lovrek I., *Internet of things context of the smart city,* 2017 International Conference on Smart Systems and Technologies (SST), 2017, pag. 187 - 193. Disponibile online al seguente link:
https://ieeexplore.ieee.org/abstract/document/8188693?casa_token=r6Z-zARk7ksAAAAA:eur-03Gv3z6s4Mk7Shu5jBpXIMv3yV0zvrjYU0uqFNfjIN55urU57aYW_dGK4rjBzIsI4myDag

[42] Intel. Disponibile online al seguente link: https://www.intel.it/content/www/it/it/tech-tips-and-tricks/what-is-a-hotspot.html#:~:text=In%20poche%20parole%2C%20gli%20hotspot,o%20persino%20in%20un%20aereo

[43] Paiva S., Ahad M.A., Zafar S., Tripathi G., Khalique a., Hussain I., *Privacy and security challenges in smart and sustainable mobility*. SN Applied Science 2, articolo numero 1175, 2020. Disponibile online al seguente link:
https://doi.org/10.1007/s42452-020-2984-9

le principali caratteristiche. Un primo tratto primario è rappresentato dal passaggio verso la *Mobility as a Service* (*MaaS*), dove i diritti di proprietà sui mezzi vengono progressivamente sostituiti con altri diritti di godimento (*usership*) attraverso i quali è possibile accedere a diversi servizi di mobilità, quali bus, taxi, treni, bici e macchine. E ciò si deve al trattamento massiccio di *Big Data* in modo da poter rispondere in tempo reale alle esigenze di chi fruisce dei servizi[44].

Per osservare più concretamente alcune applicazioni della mobilità intelligente si propongono tre esempi: quello della gestione del traffico, dei parcheggi intelligenti e della *sharing mobility.* Per quanto concerne la gestione del traffico, attraverso dei sensori posizionabili su semafori o cartelli stradali è possibile ottenere informazioni sul livello di traffico nelle strade: un esempio lo offre la città di Granada, che ha sviluppato e installato su strada il sistema MOBYWIT[45] (*Mobility by Wireless Tracking*) che attraverso dei sensori installati sui segnali stradali è in grado di rilevare i segnali *bluetooth* e *wi-fi* emessi da dispositivi come *smartphones* o *tablets*. In base a quanto tempo i segnali rilevati impiegano per giungere da un punto A ad un punto B, è stato possibile calcolare il tempo medio di percorrenza di quel tratto di strada ad una determinata ora di un determinato giorno, e quindi di prevedere quando si creeranno ingorghi. Sulla base di queste informazioni le autorità competenti della città di Granada hanno potuto pianificare al meglio la viabilità della città, almeno nei luoghi dove era stato installato il sistema. Un altro esempio in quest'ultima direzione è rappresentato dai sensori acustici installati a Santander (ES): qui, in un incrocio molto affollato, nel caso in cui i veicoli di emergenza trovino difficoltà di passaggio, i sensori dislocati lungo le strade (comunicanti tra loro), riconoscendo il suono delle sirene e calcolandone la provenienza e la direzione, intervengono cambiando automaticamente i semafori in modo da facilitare il passaggio del veicolo d'emergenza[46]. Una migliore viabilità inoltre riduce l'impatto ambientale dei veicoli, in quanto queste ultime, se bloccate a motore acceso, emettono Co2 per un tempo maggiore rispetto a quello richiesto per il naturale precorrimento della tratta.

Inoltre, neppure i parcheggi sfuggono all'innovazione, difatti tradizionalmente gli autisti provano a cercarne di liberi senza sapere dove trovarne uno, continuando a girare, contando solo sulla loro esperienza e

---

[44] Docherty I., Marsden G., Anable J., *The governance of smart mobility, transportation research part A*, volume 115, 2008, pag. 114. Disponibile online al seguente link:

https://www.sciencedirect.com/science/article/pii/S096585641731090X

[45] Musso M., *I software che sfrutta lo smartphone per evitare il traffico*, Wired, 2017. Disponibile online al seguente link:

https://www.wired.it/scienza/lab/2017/03/03/software-evitare-traffico/

[46] Napolitano D., *Le orecchie della smart city. Riconoscimento vocale e ascolto operazionale nella "città senziente"*, rivista trimestrale di scienza dell'amministrazione, Aprile 2020. Disponibile online al seguente link:

http://www.rtsa.eu/RTSA_4_2020_Napolitano.pdf

fortuna. Tutto ciò consuma una considerevole quantità di tempo e carburante[47]. Ecco che per rispondere a questa problematica nasce una sensoristica che tiene conto dei veicoli di passaggio, dei parcheggi liberi e dei relativi pagamenti. Quando si parla di *smart parking s*i fa riferimento ad un «*automated smart parking management system that would not only help a driver to locate a suitable parking space for his/her vehicle, but also it would reduce fuel consumption as well as air pollution*»[48], in quanto fornisce anche la rotta più agevole per il posto libero. Uno sfruttamento intelligente dei parcheggi soccorre anche all'obiettivo di decongestionamento del traffico, difatti si potrebbe ridurre il numero di veicoli in costante ricerca di posto libero in quanto un piccolo sensore, facilmente posizionabile, può rilevare e comunicare informazioni in merito alla disponibilità del posto auto, sicché che il sistema centrale possa elaborare una mappa dei posti liberi e renderla disponibile per i gestori dei parcheggi o per gli automobilisti dotati di apposita app[49]. Un esempio è rappresentato dal sistema di parcheggio intelligente in sperimentazione a Piacenza[50], che permette a chi scarica l'apposita applicazione di conoscere non solo quali parcheggi per diversamente abili sono liberi ma anche la strada più semplice da percorrere (la più veloce o la meno trafficata).

Proseguendo, per *sharing mobility* si intende invece una varietà di servizi alternativi, sia all'utilizzo dei mezzi di proprietà che pubblici (bus, treni ecc.), basati sulla possibilità di accedere temporaneamente ai mezzi messi a disposizione attraverso piattaforme digitali, che consentano anche il pagamento online[51]. Gli esempi classici sono quelli del *car sharing*, *car pooling*, condivisione di biciclette, scooter e monopattini. La *sharing mobility* risponde a diversi obiettivi quali la qualità il miglioramento della mobilità, la riduzione di emissioni inquinanti e la riduzione del traffico.

Abbandonando l'ambito della *sharing mobility*, una delle funzioni fondamentali di una città è difendere sé stessa e i propri cittadini. I pericoli possono essere di diversa natura, sia umani che non: dalla criminalità predatoria da strada ai terremoti, dalla scomparsa di persone a possibili

---

[47] Shaikh Y. S., *Privacy preserving internet of things recommender systems for smart cities*, Networking and Internet Architecture, Institut Polytechnique de Paris, Marzo 2020. Disponibile online al seguente link: https://tel.archives-ouvertes.fr/tel-02500640/document

[48] Sadhukhan P., *An IoT-based E-parking system for smart cities*, International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2017, pag 1062. Disponibile online al seguente link:
https://ieeexplore.ieee.org/document/8125982

[49] Tava N., *Smart City: i mille utilizzi della sensoristica IoT*, 17 Novembre 2020. Disponibile online al seguente link: https://www.invisiblefarm.it/smart-city-i-mille-utilizzi-della-sensoristica-IoT/

[50] Pagina ufficiale del comune di Piacenza, disponibile online al seguente link: https://www.comune.piacenza.it/novita/notizie/i-quaderni-degli-stati-generali-della-ricerca

[51] Smorto G., *Verso una disciplina giuridica della sharing mobility nell'Unione europea*, Diritto e Questioni pubbliche, questione numero 17, 2020.

inondazioni ecc. In tutti questi casi le città predispongono misure organizzative di sicurezza preventiva. Talvolta queste prevedono l'utilizzo di capitale umano, talaltra invece un ruolo molto importante è rivestito dalla tecnologia. In alcuni di questi casi è possibile parlare di *smart surveillance* (o sorveglianza intelligente). La questione della sicurezza è di particolare rilevanza nel mondo *IoT*: i dispositivi che oggi vengono utilizzati sono innumerevoli: si è già visto l'esempio dei semafori e dei cartelli stradali, ma ve ne sono di altri tipi, quali telecamere, *smartphone*s, tessere per i trasporti o qualsiasi altro dispositivo in grado di operare un tracciamento puntuale, di analizzare e prendere decisioni. La sorveglianza è di norma preposta alla prevenzione dei crimini, ma risulta di grande importanza anche in altri contesti[52]. Alla luce di quanto detto è possibile affermare che «*the keywords that define smart surveillance networks are: effective data aggregation, seamless integration/transmission across wired and wireless channels and meaningful data analytics*».[53]

Lo strumento di sorveglianza intelligente più utilizzato nelle *smart cities* è la videocamera e i motivi sono molteplici: dalla deterrenza, ossia la strategia diretta a disincentivare i crimini, alla grande capacità identificativa, e infine alla possibilità di migliorare la percezione, il sentimento diffuso nella comunità in merito alla sicurezza collettiva[54]. La lotta al crimine, tuttavia, non è l'unica funzione della videosorveglianza, tant'è che i sistemi a circuito chiuso (*closed circuit television*, in seguito CCTV) vengono spesso utilizzati anche per il monitoraggio di canali di trasporto pubblico, di strade, di aeroporti e altre infrastrutture. Queste fungono da «*workforce multiplier*», capaci di estendere il raggio d'azione del governo e ridurre così i tempi di risposta agli allarmi[55].

Un esempio è dato da quanto fatto dalla polizia del Galles qualche anno fa, che ha portato all'importante pronuncia nel caso *R. (Bridges)* contro

---

[52] «*For example, the chemical products storage and the surrounding environment where risk of explosion exists. In addition, trace data of individuals or communities are also very useful for «epidemics dissemination control, abnormal illegal events detection and even early alarm for terrorism activity. In urban surveillance, un-interrupted dynamic data sensing, real-time massive data analysis and instant accurate decision making for sudden disasters are quite critical and significant*», Chen N., Chen Y., Ye X., Ling H., Song S., Huang, *Advances in Mobile Cloud Computing and Big Data in the 5G Era*, Studies in Big Data, Springer, volume 22, 2017, pag. 209. Disponibile online al seguente link:

https://link.springer.com/book/10.1007/978-3-319-45145-9

[53] Kashef M., Visvizi A., Troisi O., *Smart city as a smart service system: Human-computer interaction and smart city surveillance systems*, computers in Human Behavior, volume 124, Novembre 2021. Disponibile al link:

https://www.sciencedirect.com/science/article/pii/S0747563221002466

[54] Paliotta A. P., *Le politiche innovative di sicurezza nelle città tra tecnologie di riconoscimento e smart cities*, SINAPPSI – Connessioni tra ricerca e politiche pubbliche, numero 2, 2020. Disponibile online al seguente link:

https://oa.inapp.org/handle/123456789/744

[55] Kashef M., Visvizi A., Troisi O., *Smart city as a smart service system: Human-computer interaction and smart city surveillance systems*, computers in Human Behavior, 2021.

Chief Constable Of South Wales Police & Information Commissioner del 2020[56]. Il caso verte sull'utilizzo da parte della polizia di telecamere a circuito chiuso con un sistema di riconoscimento facciale automatico incorporato, volto a rilevare il volto di persone ricercate o scomparse; i visi di queste persone erano inseriti in un *database* in dote alla polizia al quale era connesso il sistema di riconoscimento facciale. Queste telecamere erano installate sulle auto della polizia, e quando percorrevano le strade da pattugliare, il sistema rilevava i volti delle persone che entravano nello spettro visivo delle telecamere; a quel punto, in una frazione di secondo, il *software* elaborava le immagini isolando i volti delle persone e le confrontava con quelli delle persone inserite nel *database*. Automaticamente, il *software* di riconoscimento facciale segnalava all'ufficiale di polizia addetto al controllo l'eventuale *match* tra il volto della persona rilevata dalla telecamera e quello di una delle persone inserite nel *database* della polizia. In Italia qualcosa di simile lo si ha avuto a Como, anche se in quel caso è più corretto parlare di tentativo fallito[57]. Nel nostro paese questi sistemi sono stati di recente vietati fino al Dicembre 2023[58], salvo non intervenga prima una apposita disciplina giuridica. Nel mondo il numero delle telecamere è notevolmente aumentato durante la pandemia da Covid-19: le nuove telecamere sono state progettate per essere in grado di misurare la temperatura corporea ed identificare i soggetti sottoposti a quarantena, che vengono riconosciuti anche se indossano una mascherina[59]. Nel 2020 In Italia le città con più telecamere erano Roma e Milano[60]; ad oggi, non esistono ancora dati certi sul numero di telecamere nel paese, ma è altamente probabile ritenere che siano aumentate di molto a causa della pandemia (basti pensare a quelle installate negli aeroporti per la misurazione della temperatura dei viaggiatori). Il crescente numero di videocamere si deve negli ultimi due anni certamente alla pandemia ma anche, come si vedrà nel paragrafo 1.4, allo sviluppo del c.d. *fog computing* ed *edge computing*[61].

---

[56] R. (Bridges) contro Chief Constable Of South Wales Police & Information Commissioner. Disponibile online al seguente link: https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf

[57] Carrer L., *Il Comune di Como ha scoperto che il suo sistema di riconoscimento facciale non è quello che aveva comprato*, Wired, Settembre 2020. Disponibile online al seguente link: https://www.wired.it/attualita/tech/2020/09/28/como-riconoscimento-facciale-collaudo/

[58] Il divieto si deve all'articolo 1 della legge 205/2021 del 3 Dicembre. Disponibile online al seguente link:

https://www.gazzettaufficiale.it/eli/id/2021/12/07/21G00228/sg

[59] Paliotta A, *Le politiche innovative di sicurezza nelle città tra tecnologie di riconoscimento e smart cities*, 2020.

[60] Ibidem, «la capitale dispone di 8.300 telecamere con una media di 1,96 per 1.000 abitanti, mentre il capoluogo lombardo ha 4.143 dispositivi e una media pari a 1,32».

[61] Ibidem, «la videosorveglianza attuale e sempre più quella prossima ventura si baseranno anche su altre innovazioni tecnologiche quali l'elaborazione al 'margine' (edge computing) e la computazione nella 'nube'. Oggigiorno, difatti, l'analisi video, guidata dalle

Un ruolo di fondamentale e crescente importanza nella *smart surveillance* viene riservato all'ascolto «sotto forma di monitoraggio sonoro del traffico, dell'inquinamento acustico e dei suoni di arma da fuoco. Sensori acustici sono impiegati per rilevare colpi di pistola e attivare automaticamente risposte d'emergenza quali il lampeggiamento delle luci stradali circostanti»[62]. Un esempio è costituito dal già richiamato sistema EAR-IT, che riesce a veicolare il traffico grazie a sensori acustici[63]. L'espansione di questi apparecchi audio-ricettivi è anche dovuta alla loro apparente minore intrusività, in quanto nella stragrande maggior parte dei casi non sono visibili.

B. Smart health

Un settore ad oggi ricco di applicazioni tipiche dell'*Internet of Things* è quello della sanità, e in questi casi si parla di *Internet of Medical Things* (*IoMT*). Per *internet of Medical Things* si intende «*the interconnection between not only numerous personal medical devices but also between devices and health care providers, such as hospitals, medical researchers, or private companies*»[64]. I dispositivi che compongono l'*IoMT* sono molto eterogenei; esempi sono: «strumenti per il monitoraggio remoto dei pazienti, letti ospedalieri, pompe di infusione, sistemi di tracciamento dei farmaci e strumenti per il monitoraggio delle scorte mediche e delle

reti neurali, è già stata implementata nei dispositivi messi in commercio, e i principali venditori commercializzano appositi chips di intelligenza artificiale (AI) per supportare l'analisi del contenuto video, al 'bordo' della rete. Ciascuna telecamera, dotata di protocollo internet (IP), ha un circuito integrato in grado di elaborare i dati video che vengono successivamente trasmessi a un videoregistratore di rete. La capacità di analizzare automaticamente i video, ai fini della rilevazione e classificazione degli eventi temporali e spaziali, favorisce, evidentemente, lo spostamento progressivo da situazioni reattive a quelle predittive. Se il trattamento dei dati e la loro analisi possono avvenire all'interno della telecamera stessa, vi sono sostanzialmente due vantaggi: 1. minor consumo della larghezza di banda, in quanto è necessario inviare ai server solo eventi specifici e brevi sequenze di video (l'identificazione di una persona indesiderata o sospetta oppure di un veicolo derubato). In molte installazioni, tuttavia, la larghezza di banda può porre una seria limitazione poiché il video viene fortemente compresso e se si devono compiere analisi avanzate, ad esempio, con le reti neurali, è evidente che ciò riduce l'accuratezza delle identificazioni; 2. minore latenza, la quale consente soluzioni che utilizzano risposte locali, anziché richiedere un continuo round trip ai server in back-end: i dati impiegano dai 150 ai 200 millisecondi per viaggiare dai punti di ingresso alla 'nube', mentre ne bastano solo 10 per passare da questi all'elaborazione al 'bordo'».

[62] Napolitano D., *Le orecchie della smart city. Riconoscimento vocale e ascolto operazionale nella "città senziente*, 2020.

[63] Ibidem.

[64] Gatouillat A., Badr Y., Massot B, Sejdić E., *Internet of Medical Things: A Review of Recent Contributions Dealing With Cyber-Physical Systems in Medicine*, in IEEE Internet of things Journal, volume 5, pag. 3810, Ottobre 2018. Disponibile online al seguente link: https://ieeexplore.ieee.org/document/8388188

apparecchiature»[65]. Generalmente, si distingue tra dispositivi *in-body*, *in-home* e *in-clinic*, tutti sono caratterizzati dalla capacità di prendere delle decisioni in autonomia[66].

I vantaggi sono molteplici: il continuo flusso di informazioni relativo allo stato di salute del paziente può sostituire i ciclici controlli degli operatori sanitari, evitando così un monitoraggio intervallato in favore di uno continuo; l'*IoMT* ha anche la virtù di abbattere i costi relativi a visite *una tantum*. Tutto ciò grazie alla varietà di sensori applicabili ed ai nuovi algoritmi in grado di elaborare la grande quantità di dati raccolti, discernendo tra le informazioni rilevanti e quelle superflue, restituendo in tempo reale agli operatori sanitari (grazie alla connettività senza fili) importanti dati inerenti allo stato di salute dei pazienti[67].

Inoltre, nell'ottica di un miglior monitoraggio della salute «*numerous fitness trackers and bands are available that track daily activities, such as steps, exercise, sleep, and heart rate, which also connect to the cloud to store and analyze the data they collect*»[68]. I dispositivi che caratterizzano l'*IoMT* sono capaci di acquisire diversissimi tipi di informazioni, dal battito cardiaco alla pressione sanguigna, dal livello di glucosio nel sangue alla temperatura corporea[69].

c. Smart cars

[65] Lorenza, *Internet of Medical Things (IoMT): cos'è, come si fa e quali vantaggi porta alla sanità e ai cittadini*, Internet 4 Things, Gennaio 2021.

Disponibile online al seguente link: https://www.internet4things.it/IoT-library/internet-of-medical-things-iomt-cose-come-si-fa-e-quali-vantaggi-porta-alla-sanita-e-ai-cittadini/

[66] «*The medical things which have the facility to transfer data over a network without demanding human to human or human to computer interaction are termed as Internet of Medical Things (IoMT)*». Vishnu S., Ramson S. R. J. , Jegan R., *Internet of Medical Things (IoMT) - An overview*, 5th International Conference on Devices, Circuits and Systems (ICDCS), 2020, pag. 101. Disponibile online al seguente link: https://ieeexplore.ieee.org/document/9075733

[67] Mohammeda Z.., Ahmedb E., *Internet of things Applications, Challenges and Related Future Technologies*, Gennaio 2017, disponibile online al seguente link: https://www.researchgate.net/publication/313651150_Internet_of_Things_Applications_Challenges_and_Related_Future_Technologies/link/58a6e9b64585150402f27785/download

[68] Chen D., Bovornkeeratiroj P., Irwin D., Shenoy P., *Private Memoirs of IoT Devices: Safeguarding User Privacy in the IoT Era*, IEEE 38th International Conference on Distributed Computing Systems (ICDCS), 2018, pag. 1327. Disponibile online al seguente link: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8416396

[69] S. Vishnu, S. R. J. Ramson e R. Jegan, *Internet of Medical Things (IoMT) - An overview*, 2020 5th International Conference on Devices, Circuits and Systems (ICDCS), pag. 101: «*vital parameters such as heart rate, heart rate variability, pulse rate, respiration rate, systolic blood pressure, diastolic blood pressure, oxygen saturation, body temperature, body mass index, level of consciousness, muscular activation, total lung volume, height, blood glucose level, urine report*». Disponibile online al seguente link: https://ieeexplore.ieee.org/document/9075733

Altro settore dell'*Internet of Things* molto importante è poi quello delle *smart cars*, per le quali si intende vetture dotate di tecnologie *IoT* capaci di eseguire delle azioni a prescindere dall'*input* umano. In questi casi si fa riferimento ad un misto tra auto a giuda autonoma e auto connesse. Esse sono in grado di avere autonome connessioni ad Internet, che possono condividere con i passeggeri, sia se si trovano dentro la vettura, sia da remote[70]. Grazie alla sua connettività, la *smart car* può comunicare con i sistemi di navigazione satellitare sia per ricevere che per inviare dati. Ad esempio, può ricevere informazioni sul traffico tracciando così una rotta meno congestionata (utile sia ad accorciare le tempistiche dei viaggi sia a ridurre le emissioni nocive). Può poi inviare le informazioni sul traffico di modo che gli altri autisti possano beneficiarne. L'auto intelligente è anche in grado di comunicare grazie alle apposite applicazioni installabili sugli *smartphones*, e rendere così possibili alcuni servizi, come ad esempio l'accensione dell'aria condizionata da remoto poco prima di recarsi in auto, o il lampeggiamento dei fari per individuare la vettura in un parcheggio affollato, o tracciarne la posizione in caso di furto. Addirittura, in alcuni casi è possibile, grazie alla *smart car*, prenotare hotel, parcheggi o ristoranti; importanti sono anche le comunicazioni che l'auto effettua al proprietario per avvisarlo di problemi tecnici del veicolo[71]. Sempre nell'ottica della sicurezza stradale, il Parlamento europeo nel 2015 ha emanato il c.d. Regolamento eCall[72], che impone la predisposizione di un sistema automatico progettato per chiamare autonomamente i soccorsi in caso di incidente.

In ultimo, da sottolineare è l'interoperabilità tra i *softwares* propri delle *smart cars* e gli *smartphones*. Un esempio è dato dall'app Mercedes Me[73] di Mercedes-Benz, attraverso la quale è possibile monitorare da remoto l'ubicazione della vettura o il suo stato di salute (ad esempio il livello della batteria); è anche possibile attivare il sistema di climatizzazione prima di entrare in macchina, ma la cosa fondamentale è che è l'auto stessa, attraverso l'app scaricata nello *smartphone*, ad avvisare il proprietario (ad es. della pressione troppo bassa degli pneumatici) con una notifica.

---

[70] Arena F., Pau G., Severino A., *An Overview on the Current Status and Future Perspectives of Smart Cars*, Giugno 2020. Disponibie online al link: https://www.mdpi.com/2412-3811/5/7/53/htm

[71] Ibidem.

[72] Regolamento (UE) 2015/758 del Parlamento europeo e del Consiglio del 29 Aprile 2015 relativo ai requisiti di omologazione per lo sviluppo del sistema eCall di bordo basato sul servizio 112 e che modifica la direttiva 2007/46/CE, articolo 3.

[73] Portale ufficiale di Mercedes-Benz, app smart EQ control. Disponibile online al seguente link:

https://www.smart.mercedes-benz.com/ch/it/connected-car/eq-control-app#messaggi-di-stato-app-smart-eq-control

D. Smart home

Innanzitutto, per *smart home* si intende «*a home embedded with information and communication infrastructure that collaborates to the need of the home occupants*»[74]. Nelle case intelligenti si trova un ambiente ibrido in cui si intersecano diversi sistemi, come quelli di *smart security* e *smart metering.* Negli ultimi anni si è assistito ad un'esplosione di *smart objects* per la casa che rendono possibile l'automazione, il controllo da remoto ed altre comodità per l'utente[75].

Di seguito alcuni esempi dei sistemi e degli oggetti che rendono una casa intelligente. Per quanto concerne la sicurezza nelle abitazioni private e negli uffici pubblici, le videocamere, con diverse tecnologie alla base[76], sono gli strumenti maggiormente diffusi. Queste sono per lo più rivolte al rilevamento di intrusioni quando gli abitanti della casa o i frequentatori degli uffici sono fuori. Negli ultimi anni si sono diffusi sensori anche molto diversi, ad esempio quelli antincendio, in grado di rilevare non solo la presenza di fuoco, ma anche una fuoriuscita di gas, di modo da comunicare immediatamente ed automaticamente con il proprietario del sistema di sicurezza. Anche le porte d'ingresso divengono oggigiorno intelligenti. Negli anni della pandemia, per ragioni di sicurezza legata al virus Covid-19, sono state progettate porte dotate di sensori in grado di processare determinate informazioni in modo da rendere più sicuro l'accesso nelle abitazioni o agli uffici, ad esempio: il sensore MLX90614 per la rilevazione della temperatura corporea, installato nella porta, la sblocca solo se la temperatura di chi vuole entrare non è alta; se è nella media il sensore aprirà la porta. Allo stesso modo il computer Raspberry Pi dotato di videocamera Rasberry Pi è in grado di distinguere se il soggetto che vuole entrare stia indossando la mascherina contro il virus Covid-19 oppure no, e in quest'ultimo caso la porta non verrà sbloccata[77].

---

[74] Abba B., Sulaiman M., N., Mustapha N., Perumal T, *HMM-Based Decision Model for Smart Home Environment*, International Journal of Smart Home, Gennaio 2014. Disponibile online al seguente link:
https://www.researchgate.net/publication/284351676_HMM-Based_Decision_Model_for_Smart_Home_Environment

[75] Chen D., Bovornkeeratiroj P., Irwin D., Shenoy P., *Private Memoirs of IoT Devices: Safeguarding User Privacy in the IoT Era*, 2018, pag. 1327.

[76] Per una panoramica su alcuni esempi di videocamere intelligenti: Tanwar S., Patel P., Patel K., Tyagi S., Kumar N., Obaidat M. S., *An advanced Internet of things based Security Alert System for Smart Home*, International Conference on Computer, Information and Telecommunication Systems (CITS), 2017, pag. 25. Disponibile online al seguente link:
https://ieeexplore.ieee.org/document/8035326

[77] Varshini B., Yogesh H.R., Pasha S. D., Suhail M., Madhumitha V., Sasi A*., IoT-Enabled smart doors for monitoring body temperature and face mask detection*, Global Transitions Proceedings, volume 2, Novembre 2021, pag. 246. Disponibile online al seguente link:
https://www.sciencedirect.com/science/article/pii/S2666285X21000996

Talvolta, l'obiettivo sicurezza è invece rivolto a monitorare lo stato di salute degli abitanti dell'abitazione, ad esempio l'Istituto Fraunhofer di Oldenburg ha brevettato il sistema SonicSentinel volto al monitoraggio della sicurezza e della salute degli anziani. I sensori di questo sistema sono infatti capaci di riconoscere suoni legati a situazioni emergenziali, quali urla, cadute, tosse ecc., comunicando in tempo reale ai familiari e agli operatori sanitari quanto rilevato[78].

Invece, nell'ottica di un efficientamento energetico, nelle *smart home* è individuabile il settore *IoT* definito *smart metering*, con il quale ci si riferisce ad un sistema elettronico capace di misurare la quantità di energia elettrica immessa nella rete, o quella consumata dalla stessa, fornendo informazioni dettagliate ed in tempo reale, nell'ottica di un efficientamento energetico, in quanto il proprietario della griglia potrà regolare le proprie abitudini in base ai consumi[79].

L'importanza di questi sistemi si deve al fatto che si pongono come soluzioni a problemi atavici come lo spreco di energia, le bollette inesatte o addirittura l'omissione della dichiarazione dell'energia utilizzata. La soluzione è fornita in quanto un sistema del genere permette di preimpostare ogni quanto questo dovrà raccogliere i dati, ad esempio ogni 5 minuti, 10 minuti o mezz'ora. In questo modo l'utente potrà consapevolmente gestire il proprio consumo di energia. Nelle case vengono installati anche dispositivi di rilevazione e monitoraggio della qualità dell'aria, della quantità di Co2, di altre forme di inquinamento, dell'umidità, della temperatura, del ricircolo dell'aria nei luoghi chiusi. Vi sono anche sensori che percepiscono l'inquinamento acustico.

Oggigiorno, potenzialmente tutto in una casa potrebbe essere *smart*, perfino i giocattoli che i genitori comprano ai propri piccoli, ed in questi casi si parla di *smart toys*. Secondo il Garante per la protezione dei dati personali gli *smart toys* sono dotati di vari sensori (quali microfoni, telecamere, sistemi di localizzazione ecc.) che permettono la percezione dell'ambiente circostante e la comunicazione con esso (sia con persone che con altri oggetti), grazie alla loro connettività. Si tratta di qualsiasi tipo di giocattolo, progettati con il precipuo scopo di relazionarsi con gli esseri umani, principalmente bambini, ed in grado di compiere azioni in autonomia, quali scattare foto, registrare suoni, registrare video e collegarsi a *social networks*[80]. Per offrire un'idea di quanto gli oggetti di una casa possano essere interconnessi basterebbe pensare che, in un'ottica di riduzione degli sprechi relativi a cibo e bevande, anche apparecchi come i frigoriferi

[78] Napolitano D., *Le orecchie della smart city. Riconoscimento vocale e ascolto operazionale nella "città senziente*, 2020.

[79] Commissione europea. Disponibie online al seguente link:

https://energy.ec.europa.eu/topics/markets-and-consumers/smart-grids-and-meters_en#smart-metering-benefits

[80] Garante per la protezione dei dati personali. Disponibile online al seguente link: https://www.garanteprivacy.it/temi/IoT/smarttoys

divengono intelligenti. Questi offrono servizi[81] in grado di supportare gli utenti nella gestione degli alimenti: i c.d. *smart fridges* sono oggi infatti in grado di avvertire i proprietari in merito alla scadenza degli alimenti attraverso una notifica allo *smartphone*, oppure possono soccorrere nel calcolo delle calorie del prodotto in questione, o anche aiutare a redigere una lista della spesa o addirittura fornire informazioni relative al produttore, alla filiera produttiva o al peso effettivo del prodotto (ad esempio il peso lordo o sgocciolato del tonno o le caratteristiche di un vino). Piuttosto conosciuto come *smart object* è la *smart tv*, che può essere brevemente definita come «*an Internet-connected TV that has apps for users to stream content, play games, and even browse the web*»[82]. Ciò che rende questi oggetti parte dell'*IoT* è la loro capacità di collegarsi ai monitor della tv, del *pc*, delle piattaforme da gioco ed altri dispositive elettronici insieme nello stesso *network* di casa, permettendo all'utente di condividere informazioni con questi dispositivi[83].

Gli oggetti intelligenti fondamentali in una *smart home* sono oggi gli *smartphones*, e in misura leggermente minore *tablets* e *pc*. La ragione risiede nel fatto che attraverso questi dispositivi il proprietario può controllare e monitorare i diversi *smart objects* della casa: i sistemi di sorveglianza, quelli energetici ecc., tutti insieme da un'unica stazione operativa. Gli *smartphones* possono avere differenti ruoli negli ambienti interconnessi, possono difatti parteciparvi o come semplici *nodes*[84], o come centrali dalle quali controllare l'intero sistema. Quando lo *smartphone* si comporta come centrale operativa accentra le funzioni dei vari sistemi *IoT* presenti in casa: attraverso esso il proprietario di casa potrebbe programmare i termostati, i sistemi di sorveglianza e tutti gli altri dispositivi *smart* presenti in casa, potendo così tenere le redini della casa anche quando è fuori. Già oggi (ma soprattutto nel prossimo futuro), è possibile trovare nelle abitazioni quelli che vengono definiti *smart personal assistance* (*spa*), «*defined as a computer system that interacts with the user using varying*

---

[81] Per una panoramica vedasi: Rouillard J. *The Pervasive Fridge. A smart computer system against uneaten food loss.* Seventh International Conference on Systems (ICONS2012), Febbraio 2012. Disponibile online al seguente link: https://hal.archives-ouvertes.fr/hal-00825886/document

[82] Varmarken J., Le H., Shuba A., Markopoulou A., Shafiq Z., *The TV is Smart and Full of Trackers: Measuring Smart TV Advertising and Tracking*, Proceedings on Privacy Enhancing Technologies, Aprile 2020. Disponibile online al seguente link: https://par.nsf.gov/biblio/10205759

[83] Jalal L., Anedda M., Popescu V., Murroni M., *QoE Assessment for IoT-Based Multi Sensorial Media Broadcasting*, in IEEE Transactions on Broadcasting, volume 64, numero 2, pag. 552, Giugno 2018. Disponibile online al seguente link: https://ieeexplore.ieee.org/document/8344559

[84] Enciclopedia Treccani, alla voce "nodo": «In una rete informatica, ciascuno degli elaboratori (detti nodi di elaborazione) interconnessi tra loro». Disponibile online al seguente link:

https://www.treccani.it/vocabolario/nodo/#:~:text=8.,di%20elaborazione)%20interconnessi%20tra%20loro

levels of artificial intelligence to perform tasks and services for the user»[85], i cui esempi più famosi sono Alexa e Google assistant.
I compiti che gli *spa*, presi singolarmente o connettendosi ad altri dispositivi, aiutano a compiere sono diversissimi[86].

Da tenere a mente è l'interoperabilità di questi sistemi: per esempio è possibile attraverso lo *smartphone*, ordinare ad un *spa* di attivare l'impianto di riscaldamento prima di tornare a casa, o magari impartirgli l'ordine di accendere in determinati intervalli le luci durante la notte quando non si è in casa, di modo da tenere lontani potenziali malintenzionati, dando l'idea che ci sia qualcuno nell'abitazione; o addirittura far suonare una sveglia da remoto in caso di emergenza per capire se vi è qualcuno che dorme. Si pensi, ancora, al caso in cui un sensore in grado di rilevare fughe di gas invii una notifica al proprietario di casa, il quale trovandosi altrove e non riuscendo a contattare i familiari, faccia suonare una sveglia attraverso lo *spa* per svegliare gli occupanti dell'abitazione.

Gli oggetti appena menzionati: *smartphones*, *pc* portatili, *tablets* e *smartwatches* costituiscono oggi i principali *smart objects* dell'*Internet of Things*, e ciò si deve appunto alla loro capacità di connettersi a quasi qualsiasi *software* e di essere coadiuvate da tecnologie che ne ampliano le capacità (come si vedrà nel paragrafo 1.4). Occorre ricordare che gli esempi appena forniti, non esauriscono il novero di applicazioni di tecnologie *IoT* nell'ambito delle abitazioni.

1.4 Le tecnologie alla base dell'*IoT*

L'*Internet of Things*, come già accennato nel paragrafo 1.1.1, è il risultato di una serie di diversi fattori e tecnologie. In questo paragrafo si offre una sintetica visione di questi ultimi, che oggi rendono l'*IoT* come lo conosciamo. Innanzitutto, si evidenzierà il fenomeno dei *Big Data*; successivamente le tecnologie del *cloud computing*, *edge computing* e *fog*

[85] Valtteri S., *Work-based use of Smart Personal Assistants and their impact on technostress*, 2021. Disponibile online al seguente link:
https://jyx.jyu.fi/handle/123456789/76156

[86] Edu J. S., Such J. M., Suarez-Tangil G., *Smart Home Personal Assistants: A Security and Privacy Review*, ACM Computing. volume 53, Dicembre 2020, pag. 36: «*to maintain shopping and to-dos lists, purchase goods, and food, play audio-books, play games, stream music, radio and news, set timers, alarms and reminders, get recipe ideas, control large appliances, send messages, make calls [59], and many more depending on their usage context. With the continuous proliferation and the rapid growth of SPA, we are now approaching an era when SPA will not only be maneuvering our devices at home but also replacing them in many cases. For instance, many SPA are now able to make phone calls, which positions them as a communicating device, and a likely alternative to landlines phones in the future, and some SPA are also equipped with display interface for watching videos/movies and smart home cameras directly in the SPA devices*». Disponibile online al seguente link: https://doi.org/10.1145/3412383

computing. Infine, nell'ambito degli algoritmi di intelligenza artificiale, il c.d. *machine learning*.

1.4.1 *Big Data*

L'*Internet of Things* è un fenomeno che si basa fondamentalmente su due fattori: i dati e le informazioni che da questi possono essere estratte. Negli ultimi 15 anni si è assistito ad un fenomeno comunemente chiamato *Big Data*, per i quali si intende «un set di dati estesi (le cui caratteristiche principali sono volume, varietà, velocità e/o variabilità) che richiedono una tecnologia scalabile per poter essere archiviati, manipolati, gestiti e analizzati in modo efficiente»[87]. Questo particolare set di dati si è a sua volta definito con lo sviluppo di nuove tecnologie[88]. Le caratteristiche principali di questi dati sono comunemente indicate con termini che iniziano con la lettera 'V', quindi come appena detto volume, varietà, velocità, variabilità e secondo alcuni anche valore, veridicità, validità, volatilità, visualizzazione o vulnerabilità (si fa un generico richiamo al numero di "v", quindi *Big Data* 5V, *Big Data* 6V, a seconda di quante e quali di queste caratteristiche si accolgono nella propria definizione). Un approccio definitorio siffatto, che inquadra il tema in base a tutte le sue caratteristiche, ha certamente il pregio di descrivere quanto più esaustivamente possibile l'argomento, ma reca con se il rischio di estenderne eccessivamente i contorni, rendendoli meno chiari[89].

Si fa riferimento al volume per offrire un criterio quantitativo: non si parla di *Big Data* se si tratta di 500 megabyte di dati (tuttavia manca uno standard di volume minimo). Come si vedrà a breve, l'enorme quantità tipica dei *Big Data* ha condotto a significative innovazioni tecnologiche. Per quanto concerne il richiamo alla varietà di questi set di dati, si fa riferimento ai diversi formati di questi (file audio, file video, file *GPS*). Il riferimento alla variabilità è invece dato dal fatto che questi dati possono variare di significato se analizzati insieme ad alcuni o altri dati, in questo o in quel

[87] Pascuzzi G., *Il diritto dell'era digitale*, 2020.

[88] Ibidem, «ad alimentare il fenomeno big data contribuisce, ovviamente, la tecnologia. Negli ultimi anni sono cresciute in maniera esponenziale: la velocità di calcolo dei microprocessori; la capacità delle schede di memorie (oggi il più piccolo computer immagazzina giga di dati, si pensi al volume di stoccaggio che serve per memorizzare tutte le pagine web su cui opera il motore di ricerca di Google); la velocità delle connessioni di Internet; la velocità di scambio di dati tra smartphone. Ma sotto il profilo tecnologico, lo si è detto prima, grande rilievo acquistano altri due ingredienti: il calcolo distribuito, ovvero la possibilità di dividere un carico di lavoro tra più computer che operano in parallelo al fine di scambiarsi i risultati intermedi per giungere al prodotto finale6; e il cloud computing, ovvero l'architettura che consente di scambiare risorse informatiche (ad esempio, potenza computazionale e spazio di memorizzazione) tra organizzazioni diverse».

[89] Guarda P., Il regime giuridico dei dati della ricerca, Università degli Studi di Trento, 2020, pag. 30. Disponibile anche in accesso aperto al seguente link: https://iris.unitn.it/handle/11572/315657

contesto, in un momento o in un altro. Si parla di velocità in quanto i dati tipici dei *Big Data* sono raccolti, elaborati trasmessi ed archiviati ad una grande velocità. L'aggettivo relativo alla veridicità è uno dei più dibattuti in quanto, sebbene attraverso i *Big Data* possano ottenersi dei risultati sorprendentemente accurati, può anche succedere, e succede, che si giunga a risultati estremamente inesatti. Si ha inoltre un riferimento al valore, in quanto i *Big Data*, vengono oggi considerati il nuovo petrolio[90] per via della molteplicità di sfruttamenti commerciali (e non solo[91]) possibili. Dati ed informazioni non sono la medesima cosa. Per dato si intende infatti una «rappresentazione reinterpretabile di informazioni in modo formalizzato e idoneo per la comunicazione, l'interpretazione o l'elaborazione (i dati possono essere elaborati da persone o con mezzi automatici)»[92]. Da ciò si evince che il dato è il punto di partenza, mentre l'informazione è il risultato ottenuto attraverso il completamento di un'operazione di interpretazione di quel dato.

I processi di estrazione di informazioni dai dati grezzi vengono generalmente ricondotti all'espressione *data mining*, che si riferisce ad un «processo computazionale che crea modelli analizzando i dati quantitativi da diverse prospettive e dimensioni, classificandoli ed enucleando potenziali relazioni e impatti»[93]. Per offrire un esempio più chiaro delle questioni che ruotano intorno ai *Big Data* si pensi al fatto che una auto Tesla produce in media 80 gb di dati al minuto; a questo punto le questioni diventano: quante informazioni è possibile ricavare da questi dati? Con quali tecniche è possibile elaborarli? Che valore hanno queste informazioni? Alla prima domanda non può darsi una risposta a monte, in quanto non si ha una standardizzata correlazione tra *n* dati e *n* informazioni che da questa possono essere estratte; un singolo dato può offrire diverse informazioni in base al contesto nel quale si trova, in base al momento nel quale si analizza, in base agli altri dati con il quale viene analizzato, ecc. Per quanto riguarda invece le tecniche di elaborazione dei *Big Data*, in questi casi si parla di *analytics*, che vengono definite come un

> «concetto composito costituito da acquisizione, raccolta, convalida, elaborazione, quantificazione, visualizzazione e interpretazione dei dati (l'analisi dei dati viene utilizzata per comprendere gli oggetti rappresentati dai dati, per fare previsioni per una determinata situazione e consigliare sui passi da fare per raggiungere gli obiettivi»[94].

---

[90] The Economist, *The world's most valuable resource is no longer oil, but data*, Maggio 2017. Disponibile online al seguente link:
https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data

[91] Per i vari utilizzi dei *Big Data* vedasi Delmastro M., Nicita A., *Big data Come stanno cambiando il nostro mondo*, Il Mulino, Bologna, 2019.

[92] Pascuzzi, *Il diritto dell'era digitale*, 2020, pag. 265.

[93] Ibidem, pag. 299.

[94] Ibidem, pag. 265.

Le *analytics* sono molteplici ed in costante sviluppo: secondo l'Osservatorio *big data* & *analytics* del Politecnico di Milano il mercato delle *Big Data analytics* nel 2021 si è attestato intorno al valore di 2 miliardi e gli investimenti sono in costante aumento. Il motivo è chiaro: estrarre più informazioni possibili dai dati raccolti, farlo più velocemente, ed aumentare la precisione e quindi l'esattezza delle informazioni ricavate. L'ultima questione, relativa al valore delle informazioni rimane irrisolta[95] in quanto la medesima informazione può avere diverso valore in base alla quantità di dati posseduta, alle capacità di analizzarli (se si hanno algoritmi ecc.), in base alle finalità, alla capacità di diffondere i dati raccolti ecc.[96].

1.4.2 *Cloud computing*

La tecnologia che nell'ultimo decennio si è dimostrata fondamentale nell'architettura *IoT* è sicuramente il *cloud computing* (o *cloud*, o nuvola), ma prima di descriverlo occorre rappresentare lo scenario precedente, e quindi su quali tecnologie poggiava l'*IoT* prima di esso. Fino ai primi anni 2000, i dati raccolti dalle varie imprese venivano gestiti nelle relative sedi: si parlava infatti di *softwares on-premise*. Queste imprese erano dunque dotate di *servers* proprietari.
La creazione di infrastrutture in grado di raccogliere, salvare e elaborare grandi quantitativi di dati impattava in maniera importante la vita di queste imprese: il numero di *servers*, l'energia da questi consumata, la commissione ad imprese esterne dei servizi di manutenzione degli stessi (o addirittura impiegare un team interno all'impresa) e la ridotta scalabilità, rendevano particolarmente onerosa la scelta di modelli di business basati sulla raccolta di *Big Data*.
É in questo contesto che il *cloud* emerge e si impone.
Il National Institute of standards and technology nel 2011 definiva il *Cloud computing* come: «*a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction*»[97].

---

[95] Da segnalare il tentativo del Financial Times di calcolare oggettivamente il valore dei dati. Il calcolatore è disponibile online al seguente link: https://ig.ft.com/how-much-is-your-personal-data-worth/

[96] Pizzetti F., *Privacy e il diritto europeo alla protezione dei dati personali*, Giappichelli, Torino, 2016, pag. 256.

[97] Mell P., Timothy Grance T., *The NIST Definition of Cloud Computing, R*ecommendations of the National Institute of Standards and Technology, Settembre 2011, pag. 2. Disponibile online al seguente link:
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

Inquadrare con precisione il *cloud* non è cosa semplice, infatti «tale vocabolo 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»[98]; più in generale si tratta di «un complesso e variegato ecosistema di servizi, applicazioni, metodologie e pratiche che presentano tante differenze e peculiarità quanto sono i caratteri in comune»[99]. I vantaggi principali che questo offre sono: facilità di gestione, efficienza dei costi, interruzioni e aggiornamenti a basso impatto, preparazione ai disastri, pianificazione semplificata. Per facilità di gestione si fa riferimento alla maggiore agevolezza con cui è possibile manutenere i *softwares*, gli *hardware* e l'infrastruttura in generale grazie ai servizi del *cloud,* rispetto a quelli *in-premise*. Al cliente basta infatti l'accesso al *web* e richiedere il servizio in questione, al quale penserà il fornitore del servizio. Per efficienza dei costi, o economicità, si intende invece l'abbattimento dell'onere economico dovuto per sostenere i sistemi ed il personale addetto alla manutenzione, o per effettuare *upgrade* di scalabilità. Preparazione ai disastri: grazie al fatto che lo *storage* avviene fuori sede, eventuali disastri (*black out*, incendi ecc.) non intaccano i dati, che grazie alle funzioni di *backup* automatico vengono salvati di continuo. Per pianificazione semplificata si intende invece il fatto che un'archiviazione su *cloud* sgrava i responsabili IT dalla necessità di effettuare una pianificazione delle necessità, delle capacità del sistema, in quanto grazie alla grande flessibilità delle soluzioni basate sul *cloud* è possibile adeguare i servizi alle proprie esigenze in ogni momento[100].

Negli ultimi anni l'*Internet of Things* si è diffuso ampiamente, grazie al ruolo della nuvola nella raccolta, nell'elaborazione, nella gestione e nella trasmissione dei dati. Ciò che ha reso il *cloud* una risorsa fondamentale per l'*Internet of Things* è la sua scalabilità, ossia la capacità di un sistema di crescere. Per chiarire il ruolo del *cloud* all'interno dell'*IoT*, si pensi all'*Internet of Things* come al sistema nervoso, dove i sensori e le connessioni costituiscono il sistema nervoso periferico, e gli *smart objects* sono invece gli organi e i tessuti resi attivi grazie al sistema nervoso. Il *cloud computing* in questa metafora è il sistema nervoso centrale, in quanto ad esso sono riservate le funzioni di ricezione, trasmissione ed analisi delle informazioni che vengono recepite dal sistema nervoso periferico (gli *smart objects*)[101].

---

[98] Pascuzzi, *Il diritto dell'era digitale*, 2020, pag. 259.

[99] Boncinelli V., *Modelli tecnici e disciplina giuridica del c.d. cloud computing*, Rivista italiana di informatica e diritto, fascicolo 1, 2021, pag. 32. Disponibile online al seguente link:
http://eulero.ittig.cnr.it/www.rivistaitalianadiinformaticaediritto.it/index.php/RIID/article/view/71/53

[100] Wu J., Ping L., Ge X., Wang Y., Fu J*., Cloud Storage as the Infrastructure of Cloud Computing*, International Conference on Intelligent Computing and Cognitive Informatics, pag. 380, 2010. Disponibile online al seguente link:
https://ieeexplore.ieee.org/abstract/document/5565955

[101] Martelli S. (a cura di), *Internet of things (IoT) e Cloud Computing*, 2019.

Sempre per quanto concerne il rapporto tra *IoT* e *cloud*, *l'Internet of Things* può sfruttare i vantaggi del *cloud computing* per superare gli annosi problemi di conservazione ed elaborazione tipici dei sistemi *on-premise*, e il *cloud* a sua volta può estendere le proprie funzioni agli oggetti intelligenti tipici dell'*IoT*[102]. Secondo il Nist[103], il *cloud* ha 5 caratteristiche essenziali: *on-demand self-service*, accessibilità globale, condivisione delle risorse, rapida elasticità e misurabilità dei servizi[104]. I servizi offerti dai *cloud* sono in genere raggruppati attraverso tre etichette: *Software as a Service* (*SaaS*), *Platform*

[102] Geng H., *The internet of things and data analytics handbook*, 2017, pag. 688.

[103] Mell P., Grance T., *The NIST Definition of Cloud Computing*, 2011.

[104] Pascuzzi, *Il diritto dell'era digitale*, 2020, pag. 260: «on-demand self-service: l'utente può fruire di funzionalità di elaborazione, come il tempo del server e l'archiviazione di rete, in maniera automatica secondo necessità e senza richiedere l'interazione umana con ciascun fornitore di servizi; broad network access: le funzionalità sono disponibili sulla rete e sono accessibili tramite meccanismi standard che ne consentono l'uso da parte di piattaforme client eterogenee (ad esempio, telefoni cellulari, tablet, laptop e workstation); resource pooling: le risorse informatiche del provider sono raggruppate per servire più utenti contemporaneamente con diverse risorse fisiche e virtuali assegnate e riassegnate dinamicamente in base alla domanda degli stessi utenti. Il cliente generalmente non ha alcun controllo o conoscenza sulla posizione esatta delle risorse fornite; rapid elasticity: le capacità possono essere fornite e liberate elasticamente, in alcuni casi automaticamente, per ridimensionarsi rapidamente verso l'esterno e verso l'interno in ragione della domanda. Per l'utente le capacità disponibili sembrano spesso illimitate e risultano essere appropriate in qualsiasi quantità in qualsiasi momento; measured service: i sistemi cloud controllano e ottimizzano automaticamente l'uso delle risorse sfruttando una capacità di misurazione a un certo livello di astrazione adeguato al tipo di servizio (ad esempio, archiviazione, elaborazione, larghezza di banda e account utente attivi). L'utilizzo delle risorse può essere monitorato, controllato e segnalato, garantendo trasparenza sia per il fornitore sia per l'utente del servizio utilizzato».

Per un diverso inquadramento delle caratteristiche essenziali del *cloud computing* vedasi S., Pradhan A., K., *Internet of Things. Security and Privacy in Cyberspace*, Transactions on Computer Systems and Networks, Springer, Singapore, 2022, pag. 25.

as a Service (*PaaS*) *Infrastructure as a Service* (*IaaS*)[105]: in tutti questi casi «l'utente non gestisce o controlla l'infrastruttura *cloud* ma ha il controllo sui sistemi operativi, sull'archiviazione e sulle applicazioni distribuite, e, se del caso, un controllo limitato di determinati componenti di rete (ad esempio, firewall host)»[106].Negli ultimi anni il *cloud computing* si è in parte trasformato divenendo ciò che viene da alcuni chiamato *mobile cloud computing*:

> «*Mobile cloud computing is a model for transparent elastic augmentation of mobile device capabilities via ubiquitous wireless access to cloud storage and computing resources, with context-aware dynamic adjusting of offloading in respect to change in operating conditions, while preserving available sensing and interactivity capabilities of mobile devices*»[107].

In termini più generici il *mobile cloud computing* consiste nel far funzionare un'applicazione (ad esempio Gmail di Google) installata in un dispositivo mobile, come uno *smartphone*, su un *server* da remoto (in questo caso i *servers* di Google)[108]. L'impressione è che il funzionamento stia

---

[105] Ibidem, pag. 260. «Software as a Service (SaaS). L'utente può utilizzare le applicazioni del provider che vengono eseguite sull'infrastruttura cloud. Le applicazioni sono accessibili da vari dispositivi client tramite un'interfaccia, ad esempio, un browser web o una e-mail fruibile via web. L'utente non gestisce né controlla l'infrastruttura cloud sottostante, inclusi rete, server, sistemi operativi, spazio di archiviazione o persino singole funzionalità dell'applicazione, con la possibile eccezione di impostazioni di configurazione dell'applicazione e specifiche dell'utente. Platform as a Service (PaaS). L'utente può eseguire sull'infrastruttura cloud applicazioni create o acquisite dallo stesso utente utilizzando linguaggi di programmazione, librerie, servizi e strumenti supportati dal provider. L'utente, anche in questo caso, non gestisce né controlla l'infrastruttura cloud ma ha il controllo sulle applicazioni distribuite e possibilmente sulle impostazioni di configurazione per l'ambiente di hosting delle applicazioni. Infrastructure as a Service (IaaS). All'utente vengono fornite capacità di elaborazione, archiviazione, reti e altre risorse informatiche grazie alle quali egli è in grado di distribuire ed eseguire software di qualsiasi tipo, inclusi sistemi operativi e applicazioni. L'utente non gestisce o controlla l'infrastruttura cloud ma ha il controllo sui sistemi operativi, sull'archiviazione e sulle applicazioni distribuite, e, se del caso, un controllo limitato di determinati componenti di rete (ad esempio, firewall host)».

Nello stesso senso Cirani S., Ferrari G., Picone M., Veltri L., *Internet of Things: Architectures, Protocols and Standards*, John Wiley & Sons, Inc, 12 Novembre 2018, pag. 237.

[106] Ibidem, pag. 260.

[107] Kovachev D., Cao Y., Klamma R., *Mobile Cloud Computing: A Comparison of Application Models*, Information Systems & Database Technologies, 2011.

Disponibile online al seguente link:

https://arxiv.org/ftp/arxiv/papers/1107/1107.4940.pdf

[108] «*Some other examples of this type are Facebook's location aware services, Twitter for mobile, mobile weather widgets etc*». Niroshinie F., Seng W. L., Wenny R., *Mobile cloud computing: A survey, Future Generation Computer Systems*, volume 29, 2013. Disponibile online al seguente link:

avvenendo nello *smartphone*, quando invece avviene nel *server,* il quale invia i dati elaborati direttamente allo *smartphone.*

Le applicazioni installate su dispositivi mobili che si servono di questa tecnologia spesso funzionano attraverso collegamenti a *softwares* archiviati nei *cloud*, quindi, non raccolgono direttamente le informazioni, o non le elaborano autonomamente ma lo fanno attraverso programmi di calcolo installati sui *servers* dei *cloud*. Ciò avviene in quanto:

> «*As mobile phones and tablets are getting "smarter," their usage and preference over traditional desktops and laptops has increased dramatically. At the same time, the availability of a huge number of intelligent mobile applications has attracted more people to use smart mobile devices. Some of these applications, such as speech recognition, image processing, video analysis, and augmented reality are computing intensive and their implementation in portable devices is still impractical due to the mobile device resource limitations. In contrast, the high-rate and highly-reliable air interface allows to run computing services of mobile devices at remote cloud data centres. Hence the combination of mobile computing with cloud computing has resulted in the emergence of what is called mobile cloud computing (MCC) technology. In MCC computing and communications-intensive application workloads, also as storage, are moved from the mobile device to powerful and centralised computing platforms located in clouds*»[109].

Tuttavia, sebbene questo tipo di tecnologia abbia diversi vantaggi, soffre comunque di una rilevante bassa latenza, dovuta alla distanza di propagazione elevata tra i centri del *cloud* e l'utente finale[110], e questo ha portato nel corso degli ultimi anni allo sviluppo di tecnologie diverse dal *cloud*, in particolare l'*edge* e il *fog computing*[111].

1.4.3 *Edge computing*

Se il *cloud* ha rappresentato un'innovazione in quanto ha spostato la gestione dei dati dalla sede dell'impresa ad una nuvola esterna abbattendo costi e semplificando i processi, esso non costituisce comunque il punto di

---

https://didattica-2000.archived.uniroma2.it//infomob/deposito/MobileCloudComputing-Survey_FGCS2013.pdf

[109] Maldonado Y., Trujillo L., Schütze O., Riccardi A., Vasile M., *Results of the Numerical and Evolutionary Optimization Workshop NEO 2016 and the NEO Cities 2016 Workshop Held on September 20–24, 2016 in Tlalnepantla, Mexico*, Studies in Computational Intelligence, Springer, volume 731, 2018. Disponibile online al seguente link: https://link.springer.com/content/pdf/10.1007/978-3-319-64063-1.pdf

[110] Ibidem.

[111] Mastorakis G., Mavromoustakis C. X., Batalla J., M., Pallis E., (edito da), *Convergence of Artificial Intelligence and the Internet of things*, Springer, 2020, pag. 1. Disponibile online al seguente link: https://link.springer.com/book/10.1007/978-3-030-44907-0

arrivo in termini di tecnologie sfruttate oggi dall'*IoT*. Questo strumento infatti è stato portato al limite dalle necessità (raccolta, elaborazione, trasmissione) dei servizi che offre e le applicazioni che supporta. Il limite del *cloud computing* si incontra quando si è alla ricerca di risposte in *real time*, che in molti casi, per via di carenze tecniche, non risulta possibile. Più in particolare, la velocità e la qualità di elaborazione richieste dai miliardi di dispositivi *IoT* hanno spinto il *cloud* al limite, in particolare per quanto concerne la latenza, la larghezza di banda, la sicurezza dei dati, la connettività e l'IA[112]. Ciò ha condotto all'invenzione di tecnologie in grado di assistere il *cloud* attraverso la decentralizzazione di una parte (anche consistente) delle sue funzioni computazionali (si parla in questo caso di modello distribuito).

Una delle tecnologie più importanti a questo proposito è l'*edge computing* (o margine), la quale «si sostanzia nel posizionamento della capacità di elaborazione e di archiviazione vicino o nei luoghi in cui tali sistemi interagiscono con il mondo fisico («*edge*» vuol dire «bordo», «margine»)»[113]. Di recente, infatti, si è assistito all'incremento degli *smart objects*, sia nel numero che nel modello, e ciò ha portato all'aumento dei dati generati. Per gestire tali novità si è optato per spostare la memorizzazione e l'elaborazione dei dati il più vicino possibile al luogo fisico in cui i dati vengono generati. Così alcuni servizi tipici del *cloud* vengono avvicinati alla fonte dei dati (nell'*edge*, nel margine) per sfruttare una ridotta latenza e senza incappare in bande di larghezza limitata, in modo tale da

[112] «Latenza. Più settori stanno implementando applicazioni che richiedono analisi e risposta rapida. Il cloud computing da solo non è in grado di soddisfare queste esigenze a causa della latenza dovuta dalla distanza di rete dalla fonte dei dati, con conseguenti inefficienze, ritardi e customer experience scadenti. Larghezza di banda. Aumentando larghezza di banda di trasmissione o la potenza di elaborazione si potrebbero superare i problemi di latenza. Tuttavia, poiché le aziende continuano ad aumentare il numero di dispositivi edge nella loro rete e la quantità di dati che generano, l'invio dei dati al cloud può raggiungere costi insostenibili, che però potrebbero essere abbattuti se i dati potessero essere elaborati, archiviati e analizzati nell'edge. Sicurezza e privacy. La protezione nell'edge dei dati sensibili, come la documentazione medica privata e la trasmissione di meno dati via Internet potrebbero contribuire a migliorare la sicurezza riducendo il rischio di intercettazione. Inoltre, alcune amministrazioni o clienti potrebbero richiedere che i dati rimangano nella giurisdizione in cui sono stato creati. In campo sanitario, ad esempio, potrebbero esserci anche requisiti locali o regionali a limitare l'archiviazione o la trasmissione di dati personali. Connettività. L'assenza di connettività Internet costante può compromettere il cloud computing, ma una varietà di opzioni di connettività di rete rende possibile il computing edge-to-cloud. Ad esempio, il 5G offre una connessione con ampia larghezza di banda e bassa latenza, consentendo un trasferimento rapido dei dati e l'erogazione dei servizi direttamente dall'edge. Con la necessità di informazioni fruibili quasi in tempo reale, le aziende hanno bisogno dell'IA alla fonte dei dati per consentire un'elaborazione più veloce e sfruttare il potenziale dei dati precedentemente inespresso». Intel. Disponibile online al seguente link:

https://www.intel.it/content/www/it/it/edge-computing/what-is-edge-computing.html

[113] Pascuzzi G., *Il diritto dell'era digitale*, 2020, pag. 261.

processare anche grandi moli di dati e fornire risposte in tempo reale[114]. Il vantaggio che offre questo tipo di architettura risiede nel fatto che «spostando l'elaborazione e l'analisi dei dati nell' *edge* si contribuisce a velocizzare la risposta del sistema, consentendo transazioni più rapide ed esperienze migliori che potrebbero essere fondamentali nelle applicazioni quasi in tempo reale, come la guida autonoma»[115]. A ciò si aggiunge una migliore gestione del traffico di rete, una maggiore affidabilità e una maggiore sicurezza[116].

Quanto appena visto non mette in ombra l'odierno ruolo del *cloud*, bensì lo esalta: *l'edge computing*, infatti, non sostituisce la nuvola, ma la sostiene, la alleggerisce. *Cloud computing* ed *edge computing* non sono sostitutivi, bensì complementari: «sebbene l'edge computing possa offrire alle aziende un'opportunità senza precedenti per sfruttare appieno il valore dei dati, il cloud rimane essenziale come deposito dati centralizzato e centro di elaborazione»[117]. L'alleggerimento della nuvola si deve al fatto che questi dispositivi effettuano una parte (anche importante) delle operazioni di norma deputate al *cloud*. Ad esempio, si potrebbe pensare ad un sensore in grado di raccogliere una grande mole di dati, e dotato di una capacità computazionale che gli consente di discernere quali di questi dati inviare al *cloud* per effettuare analisi approfondite e quali invece eliminare perché inutili, così concentrando il lavoro della nuvola sui soli dati importanti. La diffusione dei dispositivi che sfruttano tecnologie di *edge computing* (videocamere intelligenti, sensori medici ecc.) sta favorendo la crescita della quantità dei dati generati, ma soprattutto la prontezza di risposta, che permette di attivare funzioni in tempo reale[118].

1.4.4 *Fog computing*

Il *Fog computing* (o *fog*, o nube) è una tecnologia che, esattamente come l'*edge computing*, mira a sopperire ai succitati limiti del *cloud computing*. Il *Fog computing* viene definito come «*a highly virtualized platform that provides compute, storage, and networking services between*

[114] Ibidem.

[115] Nota numero 112.

[116] Ibidem: «migliore gestione del traffico di rete. Riducendo al minimo la quantità di dati inviati tramite la rete al cloud si possono ridurre larghezza di banda e costi di trasmissione e archiviazione di grandi volumi di dati». Si ottiene inoltre una «maggiore affidabilità. La quantità di dati che le reti possono trasmettere simultaneamente è limitata. Per gli ambienti con connettività Internet di qualità inferiore alla media, la capacità di archiviare ed elaborare i dati nell'edge aumenta anche l'affidabilità in caso di interruzione della connessione con il cloud». Infine, si ha una «maggiore sicurezza. Con una corretta implementazione, una soluzione di edge computing può contribuire ad aumentare la sicurezza dei dati limitando la trasmissione dei dati tramite Internet».

[117] Ibidem.

[118] Ibidem.

end devices and traditional Cloud computing Data Centers, typically, but not exclusively located at the edge of network».[119] Esattamente come nell'*edge computing*, anche qui si ha una decentralizzazione di alcune delle operazioni che di norma vengono svolte nel *cloud*, e ciò risulta conveniente soprattutto in termini di bassa latenza e quindi prontezza delle risposte per i servizi *real time*.

Grazie a questo tipo di tecnologia le funzioni tipiche del *cloud* vengono spostate più vicino a dove avviene la raccolta dei dati riguardanti il mondo fisico. A differenza di quanto avviene nell'*edge computing* però, queste funzioni non vengono svolte direttamente negli *smart objects* che raccolgono i dati, bensì nei c.d. *fog nodes* (come, ad esempio, i *routers*[120]), posti nelle vicinanze degli *smart objects*.

Ciò che si cerca di ottenere con il *Fog computing* è «*the exact balance of capacity among the three basic capabilities, computational, networking, and storage, at the precise level of the network where they are the most optimally located*»[121]. Per quanto invece concerne il rapporto con il *cloud*: «*fog computing should be considered not as replacement of the cloud, but as a supplement to the cloud for the most critical aspects of network operations*»[122].

Alla luce di quanto esposto è possibile notare come le moderne tecnologie *IoT* partano da un approccio *cloud-based* per poi passare ad una progressiva decentralizzazione parziale delle funzioni dello stesso attraverso le tecnologie di *edge* e *fog computing*, che non sostituiscono il *cloud* bensì lo assistono e completano. Come già detto, avvicinare le funzioni computazionali alle fonti di raccolta dei dati è molto utile per fornire risposte in *real time* (nell'ordine di decimi di secondo); allo stesso modo però, per le analisi più approfondite, la potenza di calcolo propria del *cloud* risulta più appropriata e rimane dunque la prima scelta.

1.4.5 Intelligenza artificiale: il *machine learning*

Una volta immagazzinati nella nuvola, nei dispositivi a margine o nella nube, i dati grezzi vengono lavorati al fine di estrarre informazioni di valore.

---

[119] Bonomi F., Milito R., Zhu J., Addepalli S., *Fog Computing and Its Role in the Internet of things*, Cisco Systems In. Disponibile online al seguente link:
https://dl.acm.org/doi/pdf/10.1145/2342509.2342513

[120] Tordera E. M., Masip-Bruin X., García-Almiñana J., Jukan A., Ren G., Zhu J., Farré J., *What is a Fog Node? A Tutorial on Current Concepts towards a Common Definition*, Novembre 2016. Disponibile online al seguente link:
https://arxiv.org/ftp/arxiv/papers/1611/1611.09193.pdf#:~:text=Fog%20nodes%20are%20distributed%20fog,%2C%20temperature%20sensors%2C%20etc)

[121] Maldonado Y., Trujillo L., Schütze O., Riccardi A., Vasile M, *Results of the Numerical and Evolutionary Optimization Workshop NEO 2016 and the NEO Cities 2016 Workshop Held on September 20–24, 2016 in Tlalnepantla*, 2016.

[122] Ibidem.

Si è detto che queste operazioni rientrano nel novero delle *analytics* o delle tecniche di *data mining*[123]. Negli ultimi anni, per implementare la capacità di estrazione di informazioni, si è diffusa l'applicazione di sistemi di intelligenza artificiale (o IA), in primis nel *cloud*, ma anche nell'*edge* e nel *fog computing.* Il gruppo di esperti di alto livello sull'Intelligenza Artificiale della Commissione Europea ha definito l'intelligenza artificiale come:

> «*systems designed by humans that, given a complex goal, act in the physical or digital world by perceiving their environment, interpreting the collected structured or unstructured data, reasoning on the knowledge derived from this data and deciding the best action(s) to take (according to pre-defined parameters) to achieve the given goal. AI systems can also be designed to learn to adapt their behaviour by analysing how the environment is affected by their previous actions. As a scientific discipline, AI includes several approaches and techniques, such as machine learning (of which deep learning and reinforcement learning are specific examples), machine reasoning (which includes planning, scheduling, knowledge representation and reasoning, search, and optimization), and robotics (which includes control, perception, sensors and actuators, as well as the integration of all other techniques into cyber-physical systems)*».[124]

Dunque, l'intelligenza artificiale è una disciplina scientifica che caso per caso si articola in diverso modo in base al processo computazionale che si sceglie. Il *machine learning* citato poc'anzi, costituisce una delle tecniche con cui si manifesta l'intelligenza artificiale, e a sua volta questo può esternarsi sotto forma (tra le altre) di *deep learning* o *reinforcement learning*. Innanzitutto, per *machine learning* si intende «quel processo mediante il quale un'unità funzionale migliora le sue prestazioni acquisendo nuove conoscenze o abilità o riorganizzando le conoscenze o le abilità esistenti»[125].

Il *deep learning* invece è «un insieme di tecniche basate su reti neurali artificiali organizzate in diversi strati: ogni strato calcola i valori per quello successivo, in modo da elaborare l'informazione in maniera sempre più completa»[126]. Ciò ha rappresentato una rivoluzione nel mondo

---

[123] Per *data mining* si intende il processo di identificazione di modelli utili nei dati grezzi con l'obiettivo di trarre conoscenza da grandi quantità di dati. In altre parole, il data mining è una delle attività nell'analisi dei dati che implica la comprensione del complesso mondo dei dati. L'analisi dei dati (*data analytics*) invece è un campo diversificato che comprende un set completo di attività, incluso il *data mining*, che si occupa di tutto, dalla raccolta dei dati alla preparazione, alla modellazione dei dati e all'estrazione delle informazioni utili che contengono, utilizzando tecniche statistiche, *software* del sistema informativo e metodologie di ricerca operativa.

[124] The European Commission's high-level expert group on artificial intelligence, *A definition of AI: main capabilities and scientific disciplines*, Dicembre 2018. Disponibile online al seguente link:

https://ec.europa.eu/futurium/en/system/files/ged/ai_hleg_definition_of_ai_18_december_1.pdf

[125] Pascuzzi G., *Il diritto dell'era digitale*, 2020, pag. 300.

[126] Redazione Osservatori Digital Innovation, *Alla scoperta del Deep Learning: significato, esempi e applicazioni*, Febbraio 2021. Disponibile online al seguente link:

dell'intelligenza artificiale, in quanto per determinati compiti le prestazioni sono aumentate notevolmente (ad esempio per il riconoscimento di immagini o suoni). Grazie ad un addestramento mirato questi sistemi possono identificare e classificare correttamente oggetti che non avevano mai visto, con grandissima precisione. Tutto ciò è stato possibile grazie alla grande mole di dati prodotta oggigiorno e in virtù dell'elevata capacità computazionale moderna[127]. Il *reinforcement learning* «*can be described as the discrete, stochastic control process in which future states depend on the current states and taken actions…*»[128]. In altre parole, la macchina viene istruita con regole, azioni consentite e potenziali risultati finali. Questa, esercitando le azioni possibili secondo le regole che le sono state date, apprende come giungere ai risultati designati[129]. In ultimo vanno menzionati anche i sistemi di c.d. *cognitive computing*, che «cercano di comprendere ed emulare il comportamento umano utilizzando anche il linguaggio naturale (si pensi agli assistenti vocali come Alexa di Amazon, Siri di Apple o l'assistente vocale di Google»[130]. La quantità dei dati prodotti oggi dai dispositivi *IoT* è talmente grande da sconsigliare (se non escludere) un'analisi estesa protratta senza l'ausilio di sistemi intelligenti, ed è qui che i *softwares* di IA divengono di fondamentale importanza (soprattutto quando le soluzioni ad un problema cambiano velocemente e richiedono una veloce capacità di adattamento[131]); a testimonianza di ciò, la proposta di regolamento dell'Ue sull'intelligenza artificiale[132].

Questi programmi dove vengono applicati? Si è visto infatti che la raccolta e l'elaborazione dei dati può avvenire in luoghi diversi, sulla nuvola, sul dispositivo a margine o sulla nube a seconda delle varie necessità. Nei casi in cui vi sarà necessità di una pronta risposta si opterà per un'applicazione di sistemi di IA a margine o nella nube, altrimenti per le elaborazioni più complesse e che non richiedono particolare urgenza si opterà per le maggiori risorse computazionali offerte dal *cloud*. Ad esempio, grazie al *fog computing*, è possibile elaborare la grande quantità di dati prodotti a livello locale dall'erogazione di servizi sanitari, di modo da

---

https://blog.osservatori.net/it_it/deep-learning-significato-esempi-applicazioni

[127] The European Commission's high-level expert group on artificial intelligence, 2018.

[128] Greguric M., Vujic M., Alexopoulos C., Miletic M., *Application of Deep Reinforcement Learning in Traffic Signal Control: An Overview and Impact of Open Traffic Data*, 2020. Disponibile online al seguente link: https://www.mdpi.com/2076-3417/10/11/4011

[129] «È come insegnare a qualcuno le regole del gioco: infatti è la tecnica usata nella robotica ovvero per permettere ai computer di giocare a scacchi», Pascuzzi G., *Il diritto dell'era digitale*, 2020, pag. 301.

[130] Ibidem.

[131] Arora J. B.*, IoT and Machine Learning- A Technological Combination for Smart Application*, International Conference on Innovative Advancement in Engineering and Technology, 21 Febbraio 2020, pag. 2.

132 Proposta disponibile online al seguente link: https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A52021PC0206

aumentare la prontezza di risposta e diminuire i consumi energetici. Nello specifico, i dati raccolti dai sensori (ad esempio il battito cardiaco) vengono inviati nei nodi del *fog computing*, dove possono essere istallati algoritmi di apprendimento automatico capaci di captare i segnali di allarme dei sistemi di monitoraggio dei pazienti. Questi stessi algoritmi potrebbero ben essere istallati nel *cloud*, ma se posti nei nodi *fog*, più vicini al luogo di rilevamento e produzione dei dati, migliorano la prontezza nel rilevamento dei segnali d'allarme, migliorando il servizio sanitario in questione[133].Nel presente capitolo si è cercato di introdurre gli elementi caratterizzanti l'*IoT*, partendo dalle sue radici, fino ad arrivare ad oggi, passando per alcune delle innovazioni più importanti, quali il *cloud computing*. Questo primo capitolo ha l'obiettivo di fornire un'introduttiva disamina del sostrato tecnologico che negli ultimi 50 anni ha cambiato radicalmente quella porzione di diritto che oggi prende il nome di protezione dei dati personali.

Nel capitolo 2 si evidenzierà il rapporto intercorrente tra l'*IoT* e i dati personali, mentre nel quinto capitolo, dapprima si mostrerà come l'*IoT* incide sulla materia in generale, ed in un secondo momento come questa particolare relazione impatta sul regime di responsabilità civile da illecito trattamento previsto dall'articolo 82 del GDPR.

[133] Mastorakis G., Mavromoustakis C. X., Batalla J., M., Pallis E., (edito da), *Convergence of Artificial Intelligence and the Internet of things*, 2020.

Capitolo 2 - L'*Internet of Things* e i dati personali

2.1 Diritto e tecnologia: il rapporto

Secondo alcuni[134] il diritto è una tecnologia, ossia uno strumento creato dagli uomini per perseguire i loro scopi. Come tutte le tecnologie, anche il diritto muta, evolve e alle volte involve. Man mano che mutano i contesti sociali o i fini che le comunità si prefissano, muta anche il diritto. Per forza di cose esso si modifica ad una velocità molto inferiore rispetto agli avvenimenti che determinano variazioni di contesto o di obiettivi. Si prendano come esempio i sistemi democratici occidentali, in cui la produzione di norme è affidata primariamente ai vari parlamenti, ai congressi o alle assemblee, e secondariamente ai giudici: quanto tempo è necessario per creare una norma che copra una novità tecnologica introdotta nella società, qualora sia considerato opportuno?

Innanzitutto, per essere prese in considerazione dai legislatori, le novità devono essere sufficientemente estese e presenti nella società, e ciò richiede tempo; oltre a questo serve l'attenzione dell'opinione pubblica o di esperti che riescano a riportare ai legislatori o ai giudici di ultima istanza la data questione, di modo che questi possano normare. Quanto tempo intercorre tra una data invenzione tecnologica e il momento in cui, eventualmente, questa viene coperta da norme giuridiche? E cosa succede nel frattempo?

Il diritto è lento e neutro[135] e, anche provandoci, non riesce a stare al passo delle innovazioni della tecnica[136]. Si pensi ad esempio all'invenzione degli aerei: il diritto internazionale ha adottato per questi le medesime norme che da secoli erano state applicate alle imbarcazioni; ci sono voluti anni prima che fossero varate norme apposite per gli aeromobili.

---

[134] Pascuzzi G., *Has comparative law in Italy lost its driving force?*, Trento Law and Technology Research Group Research, Paper numero 31, Marzo 2017, pag. 33. Disponibile online al seguente link:

https://iris.unitn.it/retrieve/handle/11572/171785/127415/Pascuzzi_LawTech_31.pdf

[135] Ad esempio, il GDPR, come stabilisce il considerando 15, è tecnologicamente neutro: «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».

[136] «[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». Rodotà S., Tecnologie e diritti, Il Mulino, Bologna, 1995.

Continuando, la tecnologia, attraverso i suoi sviluppi, produce mutamenti sociali. Questi cambiamenti, nel momento in cui si verificano, sono fautori di interessi nuovi e socialmente rilevanti, ma ovviamente privi di tutela giuridica.
Quest'ultima arriva quando la richiesta di protezione di quegli interessi è già diffusa. Secondo chi scrive, per descrivere il rapporto tra diritto e tecnologia possono distinguersi quattro fasi. La prima è quella dell'innovazione tecnologica; la seconda è rappresentata dalla diffusione di interessi ritenuti meritevoli di tutela da parte della collettività; la terza è una fase in cui, nell'attesa di una introduzione legislativa (sempre e solo eventuale), gli operatori del diritto tentano di offrire una protezione a quegli interessi (solitamente questo si deve al ricorso a strumenti come l'interpretazione estensiva o l'analogia, che possono portare in ogni caso solo a delle sentenze, che sono atti puntuali, vincolanti solo per le parti in causa e non per la collettività). Durante questa fase, i legislatori e gli apparati collaterali discutono in merito all'opportunità di legiferare sul punto; nella quarta fase, solo eventuale, approvano quegli interventi legislativi che apprestano una tutela giuridica agli interessi sorti a causa dell'innovazione tecnologica. La tecnologia è dunque un motore per il diritto: se uno sviluppo tecnologico introduce un cambiamento nella società, questo sprigiona la diffusione di nuovi interessi, che richiedono tutela da parte dell'ordinamento giuridico. Da qui, dalle richieste di tutela, prendono avvio studi multidisciplinari che cercano di adattare le categorie classiche del diritto alle novità della tecnica, in attesa di un intervento dei legislatori. Alla luce di quanto esposto è possibile evidenziare un rapporto particolare tra il diritto e la tecnologia, che sfocia nel campo e metodo di studi comunemente definito *Law & Technology*. Questo viene definito anche come metodo, poiché si serve della multidisciplinarietà come tecnica di approccio allo studio.
Per esempio: l'informatica e Internet hanno polarizzato l'attenzione dei giuristi ormai da circa quarant'anni; tuttavia, le questioni sono molto complesse da analizzare. Lo studioso deve prima conoscere adeguatamente il fenomeno (in questo caso l'informatica ed Internet) sottostante la pretesa giuridica. I giuristi hanno dunque dovuto dapprima approcciarsi agli studi sull'informatica e Internet, avviando un dialogo con gli esperti delle relative discipline, talvolta creando dei veri e propri *pool* di professionisti con percorsi accademici differenti.

Law & Technology è un ambito di studi composito che include, oltre il diritto e l'informatica, anche la medicina, la biologia, l'economia, l'etica e la sociologia.

La materia della protezione dei dati personali è un esempio di incontro tra tecnologia e diritto. Basti pensare che in questo caso l'invenzione delle fotocamere portatili della seconda metà del diciannovesimo secolo ha portato non solo all'introduzione di nuove norme, ma ha persino sancito la nascita di un nuovo ambito giuridico, quello appunto della protezione dei dati personali. Nella seconda metà del '800 negli Stati Uniti si erano diffuse

le cosiddette *snap cameras*, ossia le prime fotocamere portatili[137]. Queste venivano utilizzate dalla stampa che si occupava di *yellow journalism*, ossia servizi scandalistici. Con tali fotocamere si realizzavano intrusioni indesiderate nella sfera privata mai verificatesi prima: si poteva infatti scattare l'istantanea di una persona all'interno della sua abitazione, o al di fuori ma comunque in un momento particolarmente intimo, ad esempio durante i funerali. Queste intrusioni indesiderate crearono dei malcontenti, e da questi si generò l'interesse ad essere lasciati da soli all'interno della propria sfera privata; tuttavia come si è detto non esisteva ancora una normativa posta a tutela della riservatezza. Si era in quella terza fase di cui si è parlato poc'anzi in cui gli operatori affrontano le sfide generate dalle tecnologie (in questo caso le *snap cameras*) con gli strumenti classici del diritto. Celeberrimo è l'articolo del 1890 intitolato "*The Right to Privacy*"[138] di Warren (avvocato) e Brandeis (futuro giudice della Corte Suprema degli Stati Uniti), che segna l'avvio degli studi su quella materia che oggi chiamiamo privacy. I mutamenti tecnologici hanno più tardi portato all'emersione della cd. protezione dei dati personali. L'equivalente inglese è *data protection*, mentre negli Stati Uniti si utilizza l'espressione *informational privacy* o *data* privacy.

L'articolo inizia con la descrizione dell'evento scatenante la questione giuridica principale:

> «*Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right «to be let alone». Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that «what is whispered in the closet shall be proclaimed from the house-tops*»[139].

Una volta esposto il substrato tecnologico e l'interesse da questo leso (il *right to be let alone*), gli autori proseguono partendo dal presupposto della mancanza di una tutela giuridica, superabile attraverso la fluidità del *common law*: «*Political, social and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society*»[140].

L'istituto classico che gli autori ritrovano nelle radici del *common law* utile a tutelare il *right to be let alone*, e che secondo questi andrebbe

[137] Solove D. J., Schwartz P., *Information Privacy Law*, Wolters Kluwer, New York, 2021, pag. 11.

[138] Warren S.D., Brandeis L.D., *The Right to Privacy*, in Harvard Law Review, volume. 4, numero 5, Dicembre 1890, pag. 193.

[139] Ibidem, pag.195.

[140] Ibidem, pag. 193.

applicato attraverso l'analogia, è il diritto d'autore, presente negli Stati Uniti già da molto prima[141].

Il *right to privacy* è oggi regolato negli Stati Uniti anche dal formante legislativo a livello sia federale che statale, attraverso specifici *acts* e *statutes*, un esempio ne è il California Consumers Privacy Act. A livello costituzionale invece la giurisprudenza statunitense ha ricollegato il diritto in esame all'interpretazione degli emendamenti, tra cui il quarto[142] relativo alle ispezioni e alle perquisizioni.

Attraverso la ricostruzione della nascita e del riconoscimento del *right to privacy* statunitense è possibile ricostruire le quattro fasi che caratterizzano il rapporto tra tecnologia e diritto: dapprima l'innovazione tecnologica (*snap cameras*); subito dopo si ha la nascita di interessi ritenuti rilevanti dalla collettività (*right to be let alone*); successivamente vi è l'attività non legislativa degli operatori del diritto utile a fornire una tutela giuridica in assenza di leggi (l'operato di Warren e Brandeis); infine si ha, eventualmente, una quarta fase in cui il legislatore riconosce tutela legislativa a quell'interesse. Negli Stati Uniti la tutela legislativa si riscontra sia a livello costituzionale nazionale (un esempio ne sono le costituzioni di California[143] e Florida[144]), sia in alcune leggi federali (come il USA-Patrioct Act o il Children's Online Privacy Act), ed anche in leggi statali (come il già citato California Consumer Privacy Act o il Virginia's Consumer Data Protection Act).

In questo paragrafo si è riassunto brevemente il rapporto tra diritto e tecnologia, e si è indicato il metodo interdisciplinare che comporta.

Alla luce di tutto quanto detto finora su questa relazione appare d'uopo concludere ricordando che:

---

[141] Ibidem, pag. 198: «*for the legal doctrines relating to infractions of what is ordinarily termed the common-law right to intellectual and artistic property are, it is believed, but instances and applications of general right to privacy, which properly understood afford a remedy for the evils under consideration. The common law secures to each individual the right of determing, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others*».

[142] Sulla protezione costituzionale del diritto alla privacy negli Stati Uniti vedasi Solove D. J., Schwartz P., *Information Privacy Law*, 2021, pag. 34: «*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*». Costituzione americana disponibile online al seguente link: https://www.senate.gov/civics/constitution_item/constitution.htm#amendments

[143] All'articolo 1 recita: «*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*».

[144] Florida, art. 1, § 23 «*Right of privacy—Every natural person has the right to be let alone and free from governmental intrusion into the person's private life except as otherwise provided herein. This section shall not be construed to limit the public's right of access to public records and meetings as provided by law*».

«la scienza giuridica e le scienze dalle quali discendono le applicazioni tecnologiche (computer science, biologia ecc.) parlano linguaggi differenti. Tra questi linguaggi occorre gettare ponti (è un aspetto centrale degli studi interdisciplinari)»[145].

2.2 Protezione dei dati personali: le fonti

Ad oggi in Europa si studia la protezione (e circolazione) dei dati personali. Tale diritto si radica in una materia, quella della privacy, che origina dall'articolo di Warren e Brandeis di più di 120 anni fa. In questo paragrafo si prospetta brevemente e a scopo introduttivo l'evoluzione storica della disciplina della protezione dei dati personali applicabile ai paesi dell'Unione europea, attraverso la cronistoria delle fonti tutt'oggi vincolanti.

A seguito della Seconda guerra mondiale, nel 1948 le Nazioni Unite si riunirono e adottarono la Dichiarazione Universale dei diritti dell'Uomo (o Dichiarazione). L'Unione europea ha oggi lo status di membro osservatore permanente, e proprio in quanto membro, è soggetta agli obblighi previsti dalla Dichiarazione.

Questa, all'articolo 12, prevede il diritto al rispetto della vita privata, secondo cui:

«Nessun individuo potrà essere sottoposto ad interferenze arbitrarie nella sua vita privata, nella sua famiglia, nella sua casa, nella sua corrispondenza, né a lesione del suo onore e della sua reputazione. Ogni individuo ha diritto ad essere tutelato dalla legge contro tali interferenze o lesioni»[146].

La locuzione «vita privata» della traduzione italiana si ritrova anche nella traduzione francese[147], con l'espressione «*vie privèe*». Diversa invece la versione inglese[148], in cui non si parla di *private life* ma di «privacy». Il diritto al rispetto della vita privata, o della privacy stando alla traduzione inglese, viene inserito in una disposizione concernente diversi altri diritti,

[145] Caso R., *La società della mercificazione e della sorveglianza: dalla persona ai dati. Casi e problemi di diritto civile*, 2021, pag. 71.

[146] Dichiarazione Universale dei Diritti Umani, disponibile online al seguente link: https://www.ohchr.org/sites/default/files/UDHR/Documents/UDHR_Translations/itn.pdf

[147] «*Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes*».

[148] «*No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks*».

come inviolabilità della corrispondenza, del domicilio ecc., e ciò poiché veniva considerato come una sorta di «*gateway*» per gli altri diritti[149].

In seno al Consiglio d'Europa, di cui fanno parte anche gli Stati membri dell'Unione Europea, nel 1950 è stata approvata la Convenzione europea dei diritti dell'uomo (o Cedu), la quale, all'articolo 8 prevede, quasi pedissequamente rispetto alla Dichiarazione[150], il diritto al rispetto della vita privata e familiare:

> «Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui»[151].

In questa disposizione, al contrario di quanto avvenuto con l'articolo 12 della Dichiarazione, è possibile notare un'uniformità di traduzioni, in quanto sia la versione italiana, quanto quella francese ed inglese si esprimono in termini di vita privata («*private and family life*» e «*vie privèe*»); scompare così il termine «privacy».

Come si evince dalla norma, il diritto alla vita privata e familiare ricomprende anche i correlati diritti relativi al domicilio e alla corrispondenza, e sono previste anche le condizioni alle quali questo diritto può essere soggetto a limitazioni[152].

A tutela dei diritti previsti dalla Cedu, e quindi anche del diritto alla vita privata e familiare, è stata istituita la Corte europea dei diritti dell'uomo (o Corte Edu, o Corte di Strasburgo), la quale vigila a che gli Stati firmatari rispettino gli obblighi previsti dalla convenzione. Questa, in diverse pronunce[153], ha stabilito che il cuore della tutela apprestata dall'articolo 8 risiede nel proteggere gli individui da interferenze arbitrarie da parte delle autorità pubbliche nella propria sfera privata; tuttavia, è bene precisare, come al momento della sua approvazione la Convenzione non mirava a garantire la protezione dei dati personali, e questo in quanto non era ancora

---

[149] «*Privacy is often asserted as a "gateway" right that reinforces other rights*». Ufficio dell'Alto Commissario per i Diritti Umani, *Universal Declaration of Human Rights at 70: 30 Articles on 30 Articles - Article 12*, 14 Novembre 2018.

[150] Schabas W. A., *The European Convention on Human Rights*, Oxford University Press, New York, 2015, pag. 359.

[151] Convenzione Europea dei Diritti dell'Uomo, disponibile online al seguente link: https://www.echr.coe.int/documents/convention_ita.pdf

[152] Non è facile distinguere sempre tra questi diritti, tant'è che talvolta si sovrappongono: Grabenwarter C., *European Convention on Human Rights*, Verlag C. H. Beck oHG, Monaco di Baviera, 2014, pag. 184.

[153] Vedasi P. e S. contro Polonia - 57375/08 e Nunez contro Norvegia - 55597/09.

presente un contesto tecnologico in grado di porre a rischio i diritti degli individui[154].

Nei primi anni dopo l'approvazione della Cedu, al termine «privacy» si iniziò ad attribuire una dimensione differente rispetto a quella di vita privata[155]. In quegli anni si stavano difatti rendendo evidenti le violazioni di alcuni diritti umani ad opera dei nuovi sviluppi tecnologici, e ci si chiedeva se l'articolo 8 della Convenzione fosse idoneo a tutelare la privacy degli individui, e non la vita privata. Così nel 1968 l'Assemblea parlamentare del Consiglio d'Europa indirizza agli Stati Membri una raccomandazione in cui si afferma l'importanza di proteggere il diritto alla privacy (*informational self-determination*[156]*)* dai nuovi sviluppi tecnologici, e che questo è tutelato, autonomamente rispetto alla vita privata e familiare, dall'articolo 8 della Convenzione[157].

I diritti previsti dalla Cedu sono inoltre considerati principi dell'Unione europea, in virtù dell'articolo 6 del Trattato di Lisbona, che ai commi 2 e 3 così recita:

> «L'Unione aderisce alla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali. Tale adesione non modifica le competenze dell'Unione definite nei trattati. I diritti fondamentali, garantiti dalla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali e risultanti dalle tradizioni costituzionali comuni agli Stati membri, fanno parte del diritto dell'Unione in quanto principi generali»[158].

---

[154] Castellaneta M., in D'Orazio R., Finocchiaro G., Pollicino O., Resta G., *Codice della privacy e data protection*, Giuffrè, Milano, 2021, pag. 4.

[155] Fuster G., *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Springer, Dordrecht, 2014, pag. 83.

[156] Nella specie non si discute di diritto alla privacy: *«The ECtHR has considered that Article 8 of the ECHR provides for the right to a 'form of informational self-determination', allowing individuals to rely on their right to privacy as regards data which, albeit neutral, are collected, processed and disseminated collectively and in such a form or manner that their Article 8 rights may be engaged*», Peers S., Hervey T., Kenner J., Ward a. (edito da), *The EU Charter of Fundamental Rights*, Hart/Beck, Londra, 2021, pag. 239.

Nello stesso senso Castellaneta M., *Codice della privacy e data protection*, 2021, pag. 6, e, Consiglio d'Europa e Corte Europea dei diritti dell'uomo, *Guide on Article 8 of the European Convention on Human Rights*, 31 Agosto 2022 (ultima versione aggiornata), pag. 56.

[157] «*Believing that newly developed techniques such as phone-tapping, eavesdropping, surreptitious observation, the illegitimate use of official statistical and similar surveys to obtain private information, and subliminal advertising and propaganda are a threat to the rights and freedoms of individuals and, in particular, to the right to privacy which is protected by Article 8 of the European Convention on Human Rights». Raccomandazione numero 509 del 1968. Disponibile online al seguente link: https://pace.coe.int/en/files/14546/html*

[158] Trattato di Lisbona, disponibile online al seguente link: https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0017.02/DOC_1&format=PDF

Gli anni sessanta e settanta sono cruciali per lo sviluppo della materia della protezione dei dati personali[159]. Sulla spinta dell'opera del Consiglio d'Europa e della Corte Edu nascono le prime legislazioni nazionali. Il primo paese a dotarsene fu la Svezia, nel 1973, quando adottò il Data Act (*Datalagen*); successivamente anche Germania e Francia approvano delle normative apposite. In Germania lo stato federato dell'Assia già nel 1970 aveva adottato una prima legislazione sulla protezione dei dati personali, ma una legge a livello federale arriva solo nel 1977 con il *Bundesdatenschutzgesetz* (*Federal Data Protection Act*). L'anno successivo, nel 1978, la Francia adotta una legge relativa a *l'informatique, aux fichiers et aux libertés*. Come visto poc'anzi Il Consiglio d'Europa nel 1950 aveva previsto il diritto al rispetto della vita privata e familiare nell'ambito di una convenzione avente ad oggetto una pletora di diritti fondamentali.

La medesima istituzione, nel 1981, apre alla stipula di un nuovo accordo: la Convenzione 108, incentrata interamente sulla protezione dei dati personali. Essa è stata sottoscritta da tutti gli Stati membri dell'UE. Fu la risposta al crescente trattamento di dati personali verificatosi dagli anni sessanta in poi[160], giudicato non regolabile adeguatamente dal solo articolo 8 della Cedu[161]. Il Consiglio d'Europa, durante gli anni settanta, aveva adottato diverse risoluzioni in materia di protezione dei dati personali, sempre ponendo come base l'articolo 8 della Cedu[162].

La Cedu ha rappresentato dunque il punto di partenza dal quale il Consiglio d'Europa ha preso spunto per creare un intero accordo incentrato esclusivamente sulla protezione dei dati personali, la Convenzione 108. Essa, inoltre, rimane ad oggi l'unico strumento giuridicamente vincolante a livello internazionale in materia di privacy[163], in quanto, la stessa convenzione, all'articolo 23[164], stabilisce che vi possono aderire anche paesi non facenti parte il Consiglio d'Europa.

---

[159] Agenzia dell'Unione europea per i diritti fondamentali e Consiglio d'Europa, *Manuale sul diritto europeo in materia di protezione dei dati*, 2018. pag. 21.

[160] Ibidem, pag. 27. Nello stesso senso Peers S., Hervey T., Kenner J., Ward a. (edito da), *The EU Charter of Fundamental Rights*, 2021, pag. 238.

[161] Fuster G., *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, 2014, pag. 84.

[162] Ibidem.

[163] González G., Van Brakel R., De Hert P. (edito da*), Research Handbook on Privacy and Data Protection Law*, Edward Elgar Publishing Limited, Northampton, 15 Marzo 2022, pag. 11.

[164] L'articolo 23 stabilisce che «dopo l'entrata in vigore della presente Convenzione, il Comitato dei Ministri del Consiglio d'Europa potrà invitare qualsiasi Stato non membro del Consiglio d'Europa ad aderire alla presente Convenzione mediante una decisione presa con la maggioranza prevista dall'articolo 20 lettera d dello Statuto del Consiglio d'Europa ed all'unanimità dei rappresentanti degli Stati contraenti aventi diritto di sedere al Comitato. 2 Per ogni Stato che aderisce, la Convenzione entrerà in vigore il primo giorno del mese successivo alla scadenza di un periodo di tre mesi dopo la data del deposito dello strumento di adesione presso il Segretario Generale del Consiglio d'Europa».

L'ambito applicativo è molto ampio: si riferisce difatti a tutti i trattamenti di dati personali effettuati nel settore privato, nelle pubbliche amministrazioni e nelle attività dell'autorità giudiziaria.

La Convenzione 108 introduce inoltre i principi del trattamento[165], nella specie i principi di correttezza, di liceità, di finalità e di qualità dei dati, e si vieta il trattamento di quei dati che venivano definiti sensibili, come la razza, la salute, le opinioni politiche, l'orientamento sessuale, ecc.

Sul rapporto tra tale convenzione e la Corte Edu, è da segnalare come essa non sia soggetta al controllo giudiziario della Corte Europea dei diritti dell'Uomo, ma quest'ultima la abbia sempre tenuta in considerazione nella sua giurisprudenza in merito all'articolo 8 della Cedu, ispirandosi ai principi previsti dalla Convenzione 108 per stabilire se vi fosse o meno una violazione del diritto alla privacy[166].

L'impatto della Convenzione 108 fu evidente, e già nei primissimi anni successivi alla sua approvazione diversi Stati Membri dell'Unione europea iniziarono ad adottare legislazioni nazionali *ad hoc*. Il Regno Unito nel 1984 approva il *Data Protection Act*; nel 1987 la Finlandia si dota del *Data File Act*; nel 1988 l'Irlanda adotta il *Data Protection Act*. Nel 1989 i Paesi Bassi pubblicano il *Wet persoonsregistraties* (Legge sulla protezione dei dati); nel 1992 il Belgio promulga il *Wet tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens* (Legge sulla tutela della privacy in relazione al trattamento dei dati personali). Queste legislazioni, sebbene ispirate dal lavoro fatto in merito all'articolo 8 della Cedu e dalla Convenzione 108, presentavano chiaramente delle differenze.

Proseguendo, nel 1993 venne firmato l'accordo che sancisce la nascita dell'Unione europea, ossia il Trattato di Maastricht. Uno degli effetti principali fu l'abbattimento delle frontiere materiali.
Per quanto riguarda quelle immateriali invece il discorso era diverso: ogni paese (quando lo faceva) disciplinava a modo proprio il trasferimento dei dati personali connesso alla compravendita o fornitura di beni e servizi negli altri paesi. Consapevoli di ciò, i paesi dell'allora comunità economica europea (o CEE) avviarono negoziazioni per giungere ad un accordo che agevolasse i trasferimenti di dati personali tra paesi europei[167].

---

[165] Gruppo di lavoro *ex* articolo 29, parere 06/2014 sulla nozione del legittimo interesse e del titolare del trattamento.ai sensi dell'articolo 7 della Direttiva 95/46/CE, 9 Aprile 2014, pag. 7. Disponibile online al seguente link:
https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf

[166] Agenzia dell'Unione europea per i diritti fondamentali e Consiglio d'europa, *Manuale sul diritto europeo in materia di protezione dei dati*, 2018, pag. 28.

[167] «La libera circolazione delle merci, dei capitali, dei servizi e delle persone nel mercato interno ha richiesto la libera circolazione dei dati, che non poteva essere realizzata se gli Stati membri non avessero potuto contare su un livello elevato e uniforme di protezione dei dati», Agenzia dell'Unione europea per i diritti fondamentali e Consiglio d'Europa, *Manuale sul diritto europeo in materia di protezione dei dati*, 2018, pag. 32.

Il risultato fu la Direttiva 95/46/CE[168] (detta anche Direttiva madre). Il ruolo della direttiva, tra le varie fonti di diritto dell'ordinamento giuridico europeo, è quello di armonizzare gli ordinamenti dei paesi membri, stabilendo dei principi, degli obiettivi, che i suddetti paesi dovranno raggiungere potendo scegliere in autonomia i migliori strumenti per farlo. Le direttive dovrebbero dunque essere sempre accompagnate da norme nazionali applicative, e sono sempre vincolanti, ma non direttamente operative.

Le uniche direttive direttamente operative sono quelle le cui disposizioni sono incondizionate e sufficientemente chiare e precise da essere applicate direttamente nei vari paesi; si richiede però anche che lo stato membro non le abbia recepite con apposita normativa applicativa nel termine previsto dalla direttiva stessa (questa efficacia ha effetto solo verticale)[169]. La Direttiva madre, tuttavia, fallì nel tentativo di creare un compiuto spazio libero di scambio di dati personali, era difatti previsto il meccanismo del mutuo riconoscimento: «la conseguenza del mutuo riconoscimento consiste nel fatto che in ogni Paese dell'Unione si applica la legge di protezione dati del Paese in cui ha sede lo stabilimento principale del titolare del trattamento»[170].
Alla luce di ciò si applicavano ancora le differenti normative nazionali, seppur orientate ai principi della Direttiva madre.

Sul rapporto tra la direttiva 95/46/CE e la Convenzione 108, è bene sottolineare come la prima riflettesse i principi di quest'ultima, spesso ampliandoli. Ad esempio, vennero introdotte le autorità di controllo indipendenti in materia di protezione dei dati personali per monitorare l'osservanza delle norme della Direttiva madre. Questa novità verrà poi tradotta anche nella Convenzione 108 grazie al Protocollo addizionale, a dimostrazione di una reciproca, positiva, influenza tra i due strumenti normativi[171].

La Direttiva abbracciava i principi di base della protezione dei dati personali.

Andando avanti nel novero delle fonti rilevanti in materia di protezione dei dati personali, nel 2001 viene adottato il Regolamento 45/2001/CE, volto ad introdurre i principi espressi dalla Direttiva madre nell'ambito dei trattamenti di dati personali effettuati dalle istituzioni e dagli organismi europei nell'esercizio delle loro funzioni. Altro fattore importante di tale

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

[169] Mengozzi P., Morviducci C. *Istituzioni di diritto dell'Unione Europea*, Wolters Kluwer, Milano, 2018, pag. 131.

[170] Pizzetti F., *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Giappichelli, Torino, 2016, pag. 66.

[171] Agenzia dell'Unione europea per i diritti fondamentali e Consiglio d'Europa, *Manuale sul diritto europeo in materia di protezione dei dati*, 2018, pag. 32.

regolamento è l'istituzione un'autorità garante indipendente per monitorare l'applicazione delle sue disposizioni, il Garante europeo della protezione dei dati personali.

Nel 2000 l'UE adotta la Carta dei diritti fondamentali dell'Unione europea (o Carta). L'obiettivo era raggruppare «la totalità dei diritti civili, politici, economici e sociali dei cittadini europei, sintetizzando le tradizioni costituzionali e gli obblighi internazionali comuni agli Stati membri. I diritti descritti nella Carta sono suddivisi in sei titoli: dignità, libertà, uguaglianza, solidarietà, cittadinanza e giustizia»[172]. Inizialmente la Carta era solo un documento politico. Essa diviene vincolante solo nel 2009, dopo l'approvazione del Trattato di Lisbona, che al paragrafo 1 dell'articolo 6 prevede:

> «L'Unione riconosce i diritti, le libertà e i principi sanciti nella Carta dei diritti fondamentali dell'Unione europea del 7 dicembre 2000, adattata il 12 dicembre 2007 a Strasburgo, che ha lo stesso valore giuridico dei trattati. Le disposizioni della Carta non estendono in alcun modo le competenze dell'Unione definite nei trattati. I diritti, le libertà e i principi della Carta sono interpretati in conformità delle disposizioni generali del titolo VII della Carta che disciplinano la sua interpretazione e applicazione e tenendo in debito conto le spiegazioni cui si fa riferimento nella Carta, che indicano le fonti di tali disposizioni»[173].

Le norme della Carta rilevanti ai fini della presente tesi sono gli articoli 7[174] e 8[175]. Specialmente quest'ultimo, rubricato «diritto alla protezione dei dati di carattere personale», innalza tale diritto a diritto fondamentale dell'Unione. Gli articoli 7 e 8 della Carta vengono spesso considerati unitamente in virtù della loro connessione[176], anche se è proprio grazie alla

[172] Ibidem, pag. 31.

[173] Trattato di Lisbona, disponibile online al seguente link: https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0017.02/DOC_1&format=PDF

[174] Articolo 7. rispetto della vita privata e della vita familiare.

«Ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni».

[175] Articolo 8. Protezione dei dati di carattere personale.

«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».

[176] Tale collegamento emerge negli atti delle istituzioni europee: ad esempio nella sentenza Volker-Schecke e Eifert v. Hessen (procedimenti riuniti C-92/09 e C-93/09) o nelle *Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data* (12 Dicembre 2019).

Carta che il diritto alla protezione dei dati personali diviene un diritto fondamentale autonomo[177].

La Carta, pur rigettando il concetto di *information self-determination* fatto proprio dalla Corte Edu in merito all'articolo 8 della Cedu, basa il suo diritto alla protezione dei dati personali proprio sui risultati ottenuti in seno all'articolo 8 della Convenzione, così come anche sulla Convenzione 108 e sulla Direttiva madre[178].

La novità dell'articolo 8 consiste nel sistema di «*check and balances»*[179] introdotto al fine di tutelare i dati personali: si è preferito abbandonare il concetto di *information self-determination*, che vedeva il consenso dell'interessato come elemento cardine della liceità del trattamento, in virtù di una serie di diritti, obblighi e limitazioni di entrambi, anche in casi in cui il trattamento non avveniva in base al consenso. In quanto questo non era più l'unica base prevista[180].

Nel 2002 viene adottata la direttiva 2002/58 del Parlamento europeo e del Consiglio del 12 luglio relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche. Così come modificata dalla direttiva 2009/136, deve intendersi una precisazione ed integrazione della Direttiva madre per il settore delle comunicazioni elettroniche, che richiede una disciplina speciale. Lo si evince dall'art. 1 paragrafo 2, che recita: «ai fini di cui al paragrafo 1, le disposizioni della presente direttiva precisano e integrano la direttiva 95/46/CE»[181].

Nel 1997 era stata emanata la direttiva 97/66/CE. Questa è stata però abrogata dalla direttiva 2002/58/CE, la quale, al quarto considerando, ne riporta i motivi:

> «la direttiva 97/66/CE deve essere adeguata agli sviluppi verificatisi nei mercati e nelle tecnologie dei servizi di comunicazione elettronica, in guisa da fornire

[177] Peers S., Hervey T., Kenner J., Ward a. (edito da), *The EU Charter of Fundamental Rights*, 2021, pag. 177.

Sulla distinzione tra privacy e protezione dei dati personali vedasi: Hijmans H., *The European Union as Guardian of Internet Privacy*, Springer, pag. 62 e ss; Lynskey O., *The Foundations of EU Data Protection Law*, Springer, Oxford University Press, Ney York, 2019, pag. 89 e ss., e Bieker F., *The Right to Data Protection*, T.M.C. Asser press, Springer-Verlag GmbH, L'Aia, 2022, pag. 258 e ss.

[178] Peers S., Hervey T., Kenner J., Ward a. (edito da), *The EU Charter of Fundamental Rights*, 2021, pag. 239; Castellaneta M*., Codice della privacy e data protection, 2021, pag.* 12.

[179] Ibidem, pag. 239; vedasi anche Bieker F, *The Right to Data Protection*, 2022, pag. 162.

[180] Peers S., Hervey T., Kenner J., Ward a. (edito da), *The EU Charter of Fundamental Rights*, 2021, pag. 239.

[181] Direttiva del Parlamento europeo e del Consiglio del 12 luglio 2002 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche). Disponibile online al seguente link: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32002L0058&from=IT

un pari livello di tutela dei dati personali e della vita privata agli utenti dei servizi di comunicazione elettronica accessibili al pubblico, indipendentemente dalle tecnologie utilizzate. Tale direttiva dovrebbe pertanto essere abrogata e sostituita dalla presente direttiva»[182].

La direttiva 2002/58/CE arriva dunque soltanto cinque anni dopo la prima disciplina relativa alle comunicazioni elettroniche, eppure, quando si tratta di normare le tecnologie, anche pochi anni possono rappresentare un'eternità. La direttiva 2002/58 infatti, recepì i cambiamenti e gli sviluppi relativi alle tecnologie usate nell'ambito delle comunicazioni elettroniche, in quanto in queste il Legislatore europeo vedeva un anello debole per quanto concerne la tutela dei dati personali. Tra le norme della direttiva si notino l'articolo 5 paragrafo 3[183], che prevede l'obbligatorietà del consenso informato per poter utilizzare le reti di comunicazione elettronica al fine di archiviare informazioni o accedere a informazioni archiviate nell'apparecchio terminale dell'utente, e l'articolo 6 paragrafo 1[184] che impone l'anonimizzazione o cancellazione dei dati di traffico quando non più necessari per il fine per il quale sono stati trattati. Su questo punto, c'è chi ritiene che l'aspetto più importante della norma sia quello di essere imperniata sull'utente, con la conseguenza che tutte le attività da questi svolte nell'ambito delle comunicazioni elettroniche rientrano nella sua sfera privata, nella quale vi si può accedere solo con il consenso dell'utente (con consequenziale divieto di utilizzo di *cookies* o *fingerprint* senza il consenso dell'interessato)[185].

Altra norma rilevante è l'articolo 9, secondo cui i dati relativi all'ubicazione della comunicazione, se diversi dai dati relativi al traffico, possono essere trattati solo se anonimizzati o se gli interessati ne hanno fornito il consenso.

---

[182] Ibidem.

[183] Ibidem: «Gli Stati membri assicurano che l'uso di reti di comunicazione elettronica per archiviare informazioni o per avere accesso a informazioni archiviate nell'apparecchio terminale di un abbonato o di un utente sia consentito unicamente a condizione che l'abbonato o l'utente interessato sia stato informato in modo chiaro e completo, tra l'altro, sugli scopi del trattamento in conformità della direttiva 95/46/CE e che gli sia offerta la possibilità di rifiutare tale trattamento da parte del responsabile del trattamento. Ciò non impedisce l'eventuale memorizzazione tecnica o l'accesso al solo fine di effettuare o facilitare la trasmissione di una comunicazione su una rete di comunicazione elettronica, o nella misura strettamente necessaria a fornire un servizio della società dell'informazione esplicitamente richiesto dall'abbonato o dall'utente».

[184] Ibidem: «I dati sul traffico relativi agli abbonati ed agli utenti, trattati e memorizzati dal fornitore di una rete pubblica o di un servizio pubblico di comunicazione elettronica devono essere cancellati o resi anonimi quando non sono più necessari ai fini della trasmissione di una comunicazione, fatti salvi i paragrafi 2, 3 e 5 del presente articolo e l'articolo 15, paragrafo 1».

[185] Pizzetti F., *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, 2016, pag. 133.

Il diritto primario dell'Ue prevede il diritto alla protezione dei dati personali nell'ambito della Carta, ma anche all'articolo 16 del Trattato sul funzionamento dell'Unione europea[186] (o TFUE), il quale al primo paragrafo recita: «ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano»[187]. Esiste dunque anche qui una previsione esplicita. Questa disposizione, congiuntamente agli articoli 7 e 8 della Carta, costituisce la base del diritto alla protezione dei dati personali in Europa[188], ed infatti costituirà la base normativa sulla quale si poggerà il Regolamento 2016/679, legittimando interventi legislativi in materia.

Nel 2016 viene approvato il Regolamento generale sulla protezione dei dati personali[189] (in seguito GDPR o Regolamento). Il Regolamento, entrato in vigore nel 2016, ma applicativo dal 25 maggio 2018, rappresenta un punto di svolta rispetto al passato per parecchi motivi. L'*iter* di approvazione fu parecchio lungo: il punto di partenza fu una consultazione pubblica della Commissione europea nel 2009, che portò alla proposta di regolamento nel 2012. Solo dopo 4 anni di negoziazioni tra Parlamento e Consiglio, nel 2016, si arrivò all'approvazione; si stabilì anche un periodo di transizione di 2 anni, in modo da permettere a tutti gli attori di adeguarsi alle nuove prescrizioni.

Il GDPR si pone l'obiettivo di modernizzare la disciplina della tutela dei dati personali. In dottrina il passaggio di testimone tra Direttiva madre e Regolamento è stato visto come un importante punto di svolta[190]. La differenza più evidente con la Direttiva madre è la natura dell'atto: il regolamento, essendo sempre *self-executing*, lascia molto meno spazio di manovra agli stati nazionali dell'Unione (seppur rimanga comunque un

---

[186] Trattato sul funzionamento dell'Unione europea, disponibile online al seguente link:
https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:12012E/TXT:it:PDF

[187] Ibidem.

[188] Hijmans H., *The European Union as Guardian of Internet Privacy*, 2016, pag. 4; Pizzetti F., *Privacy e il diritto europeo alla protezione dei dati personali*, pag. 8.

[189] Regolamento (Ue) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). Disponibile online al seguente link:
https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=celex:32016R0679

[190] «Il GDPR introduce grandi novità a partire dal raggiungimento dell'obiettivo di assicurare una disciplina di protezione dati uniforme ed armonizzata tra tutti gli Stati membri dell'Unione europea. Invero, la nuova normativa europea in materia di protezione dati ha una portata di immense dimensioni: non è solo la tanto attesa risposta all'esigenza di predisporre una disciplina unitaria sul trattamento dei dati che si adegui al sempre più esteso processo di digitalizzazione globale - ruolo che l'ormai superata dir. 95/46/CE non era più in grado di garantire – ma è innanzitutto il mezzo con cui il legislatore europeo, mutando completamente impostazione rispetto al passato, ha realizzato un articolato puzzle normativo prevalentemente incentrato sul processo di rendere responsabili i titolari ed i responsabili del trattamento sancito dall'art. 24 del GDPR. La dir. 95/46/CE, infatti, era tutta focalizzata sui diritti dell'interessato, mentre il testo del nuovo Regolamento si sviluppa essenzialmente su processi, attività, misure tecniche ed organizzative, sanzioni e obblighi rivolti a titolare e responsabile del trattamento», Riccio G. M., Scorza G., Belisario E. (a cura di), *GDPR e normativa privacy*, Wolters Kluwer, Milano, 2018, pag. 237.

margine, ad esempio, per quanto concerne i codici di condotta)[191]. Se la direttiva risponde ad esigenze di armonizzazione, i regolamenti dell'Unione servono invece ad uniformare i vari ordinamenti. Quanto appena detto si evince dal Regolamento stesso, che al considerando 9 recita:

> «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»[192].

La frammentazione della tutela dei dati personali non è ovviamente l'unico fattore che ha condotto all'adozione del Regolamento. Nel 1996 le tecnologie che avevano portato all'introduzione della Direttiva madre non erano certo quelle del 2016[193], infatti in quegli anni non vi erano gli *smartphones*, o i *social networks* o i motori di ricerca. La Direttiva fotografava una realtà in cui i dati circolavano dall'interessato al titolare del

---

[191] Lo stesso Regolamento lo prevede al considerando 10: «…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».

Sobolewski M., Mazur J., Paliński M., *The European Digital Single Market*, volume 52, Luglio/Agosto 2017, numero 4. Disponibile online al seguente link: https://www.intereconomics.eu/pdf-download/year/2017/number/4/article/the-european-digital-single-market.html

[192] Sulle ragioni della scelta della forma del regolamento vedasi Pizzetti F., *Privacy e il diritto europeo alla protezione dei dati personali*, 2016, pag. 7.

[193] Kedzior M., *GDPR and beyond—a year of changes in the data protection landscape of the European Union*, Europäische Rechtsakademie (ERA), 14 Febbraio 2019. pag. 506. Disponibile online al seguente link;

https://link-springer-com.ezp.biblio.unitn.it/content/pdf/10.1007/s12027-019-00549-x.pdf

trattamento, ma le innovazioni tecnologiche di cui sopra hanno stravolto questo paradigma, creando un modello di circolazione globale dei dati che non prevede solo l'interessato e il titolare come protagonisti del trattamento[194].

Si è evidenziato (cfr. 1.4.2.) come tecnologie quali il *cloud computing* abbiano aumentato enormemente la circolazione dei dati personali. A questo aumento del traffico dati si aggiunge anche una moltiplicazione degli attori in campo, visto che questi vengono trattati ora da nuove entità, come appunto i fornitori di servizi di *cloud computing*.

Come detto poc'anzi, la base normativa sulla quale poggia il Regolamento è l'articolo 16 del TFUE, al quale è riservato, non a caso, il primo considerando, il quale recita:

> «La protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale. L'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea («Carta») e l'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea («Tfue») stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano"»[195].

La modernizzazione della disciplina passa attraverso la creazione di nuovi istituti o la modernizzazione di altri già esistenti. Grazie all'articolo 3 per esempio, è stato aumentato l'ambito di applicazione territoriale del regolamento[196].

Mutamenti importanti sono poi quelli relativi ai principi di *accountability*[197], di *privacy by design* e *by default*[198], ma anche

---

[194] Finocchiaro G., *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Zanichelli, Torino, 2019, pag. 4. Vi erano anche ragioni di natura strettamene economica, come aumentare la fiducia nelle transazioni elettroniche nel mercato interno: Ibidem, pag. 9.

[195] GDPR.

[196] Pizzetti F., *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, 2016, pag. 159; Finocchiaro G., *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, 2019, pag. 19.

[197] Bolognini L., Pelino E., *Codice della disciplina privacy*, Giuffrè, Milano, 2019, pag. 201; Riccio G. M., Scorza G., Belisario E. (a cura di), *GDPR e normativa privacy*, Wolters Kluwer, Milano, 2018, pag. 237. Sul punto anche Pizzetti F., *Privacy e il diritto europeo alla protezione dei dati personali*, 2016, pag.4.

Si distingue chi sostiene che l'innovazione sia solo apparente, in quanto che la gestione del rischio fosse prassi già conosciuta ed applicata anche in seno alla Direttiva madre: vedasi Mantelero A., *La gestione del* rischio, in Finocchiaro G., *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, 2019, pag. 476.

[198] Pizzetti F., *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, 2016, pag. 153; Panetta R. *Privacy is not*

l'introduzione del registro dei trattamenti[199], o la valutazione di impatto del trattamento[200]. Particolare rilevanza è stata assegnata al principio di responsabilizzazione, che informa l'intero Regolamento, orientandolo ad un approccio dinamico di prevenzione del rischio[201]; se prima del GDPR infatti l'attenzione era riposta sull'esercizio dei diritti dell'interessato sulla base del principio del consenso e il relativo controllo dei dati, adesso si è dinanzi ad una regolamentazione volta alla responsabilizzazione di alcune figure tipizzate (principalmente titolare e responsabile del trattamento) attraverso l'imposizione di doveri tipici, ed altri da valutarsi in base alle circostanze del trattamento *de quo* [202].

Inoltre, grazie alle attività delle autorità garanti nazionali, del Garante europeo e della Corte di Giustizia, i singoli istituti vengono reinterpretati alla luce dei casi più importanti, o degli sviluppi tecnologici più rilevanti.

Il Regolamento abbraccia e garantisce tutti i diritti fondamentali, le libertà e i principi sanciti dalla Carta e dai Trattati[203].

Nello stesso pacchetto legislativo[204] sui dati è stata adottata anche la Direttiva 2016/680[205] 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».

La direttiva in questione ha come unico ambito applicativo quello della cooperazione giudiziaria in materia penale e della cooperazione di polizia. In

---

dead: it's hiring!, in Panetta R. (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, Giuffrè, Milano, 15 Giugno 2019, pag. 28.

[199] Chauvenet R., in D'Orazio R., Finocchiaro G., Pollicino O., Resta G., *Codice della privacy e data protection*, 2021, pag. 489.

[200] Ibidem, pag. 534.

[201] Mantelero A., *La gestione del rischio*, 2019, pag. 476.

[202] Tosi E., *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale*, Giuffrè, Milano, 2019, pag. 34; vedasi anche Bilotta F., *La responsabilità civile nel trattamento dei dati personali*, in Panetta R., *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, 2019, pag. 446.

[203] Polini M., *Privacy e protezione dei dati personali nell'ordinamento europeo e italiano*, in Maglio M., Polini M., Tilli N., *Manuale di diritto alla protezione dei dati personali*, Maggioli, Santarcangelo di Romagna, Giugno 2019, pag. 64.

[204] Sul Data Protection Package vedasi Passaglia P., *Il sistema delle fonti normative in materia di tutela dei dati personali*, 2019, pag. 91.

[205] 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, Disponibile online al seguente link:

https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32016L0680&rid=5

questi settori non si applica il GDPR[206], bensì la direttiva stessa, quale normativa speciale, come nel caso delle comunicazioni elettroniche. L'articolo 1 invece indica gli obiettivi della stessa: innanzitutto la regolamentazione del trattamento di dati personali nell'ambito delle attività «a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia e la prevenzione di minacce alla sicurezza pubblica». In secondo luogo, dotare i Paesi membri di una normativa di riferimento per i casi di scambio di dati tra le varie autorità. La direttiva 2016/680 inoltre, tenta di affrontare le conseguenze degli sviluppi tecnologici più rilevanti, capaci di incidere sensibilmente sugli individui, come la profilazione operata dalle autorità di contrasto[207]. D'altro canto, Internet offre nuove possibilità di indagine, ad esempio seguendo le tracce dei criminali disseminate in rete; le relative attività di contrasto non dovranno però mettere a rischio i diritti e le libertà delle persone fisiche[208].

Nel 2018, viene anche approvato[209] il protocollo di ammodernamento della Convenzione 108 di cui si è detto in precedenza; in virtù di tale aggiornamento si parla oggi di Convenzione 108+[210].

L'aggiornamento si deve al fatto che la Convenzione 108 era e rimane l'unico strumento giuridicamente vincolante a livello internazionale per quanto riguarda la protezione dei dati personali. La realtà fotografata dalla Convenzione 108 era molto differente rispetto a quella odierna: non c'era Internet, non c'erano i *social networks*, non si poteva parlare di *Big Data* o oggetti interconnessi come accade oggi. La disciplina apprestata dal vecchio documento si è rivelata negli anni insufficiente, inidonea a confrontarsi con le nuove sfide del mondo digitale[211]. Dunque, la Convenzione 108+ si pone l'obiettivo di affrontare le sfide risultanti dalle nuove tecnologie digitali attraverso il rafforzamento dei meccanismi apprestati dal vecchio documento del 1981[212]. Il processo di ammodernamento della Convenzione 108 è iniziato prima dell'approvazione del GDPR, ma si è preferito attendere

---

[206] Sajfert J., Quintel T., *Data protection Directive (Eu) 2016/680 for police and criminal justice authorities*, 1 Dicembre 2017, pag. 3.

[207] Agenzia dell'Unione europea per i diritti fondamentali e Consiglio d'Europa, *Manuale sul diritto europeo in materia di protezione dei dati*, 2018, pag. 36.

[208] Sajfert J., Quintel T., *Data protection Directive (Eu) 2016/680 for police and criminal justice authorities*, 2017, pag. 1.

[209] La Convenzione 108+ entrerà in vigore l'11 Ottobre 2023, ma solo qualora almeno 38 paesi la ratifichino.

[210] Ratificata in Italia attraverso la legge numero 60 del 2021.

[211] «*The changes that have emerged during these decades relate to the volume of data processed, the variety of actors, the scale of operations on data, the economic value attached to data, the threats to data, the overall availability of data in time and space, etc.*». De Terwangne C., *Council of Europe convention 108 +: A modernised international treaty for the protection of personal data*, Computer Law & Security Review, volume 40, Aprile 2021, pag. 1. Disponibile online al seguente link:

https://www.sciencedirect.com/science/article/pii/S0267364920301023

[212] A tal proposito si esprime il Garante con apposito comunicato stampa, disponibile online al seguente link: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9585156

che lo stesso fosse adottato, in modo da evitare discrasie tra la nuova convenzione e il Regolamento. Le ragioni sottostanti all'importanza data alla coerenza tra GDPR e nuova convenzione risiedono nella questione relativa al trasferimento transfrontaliero dei dati, già preso in considerazione dal Regolamento agli articoli 44 e seguenti[213]. Il Regolamento statuisce che un trasferimento siffatto può aversi solo se la Commissione ha stabilito che il paese terzo garantisce un'adeguata protezione dei dati. Il considerando numero 105[214] aggiunge poi che la Commissione, nel valutare la suddetta adeguatezza, dovrebbe tenere in considerazione, tra diverse cose, l'adesione alla Convenzione 108 e al relativo protocollo addizionale. La Convenzione 108, nella sua vecchia e nuova formulazione, costituisce dunque un importante elemento ai fini di una continuità nella circolazione transazionale dei dati. Grazie ad essa sono state poste le basi per una futura globalizzazione della disciplina, che detta solamente degli standard minimi di tutela, eventualmente rivedibili al rialzo dalle singole parti contraenti[215].

Attraverso degli emendamenti al testo originale, la Convenzione 108 è stata avvicinata allo standard stabilito dal GDPR (non essendo comunque le due discipline perfettamente sovrapponibili[216]).

Tra le modifiche più importanti si evidenzia quella al principio di proporzionalità, che dev'essere rispettato in ogni fase del trattamento. Tra i diritti implementati vi è quello relativo alle decisioni automatizzate (diritto a chiedere un intervento umano, a conoscere la logica del processo decisionale e ad opporsi) e all'oblio. Introdotti i principi di *privacy by design* e *by default* ecc.[217]. Qualora fosse ratificata da un significativo numero di

---

[213] Karadogan B., *Modernized Convention 108 And GDPR*, Ottobre 2019, pag. 3. Disponibile online al seguente link:

https://www.researchgate.net/publication/336512782_GDPR_and_COnvention_108_Article

[214] Il considerando numero 105 afferma che «al di là degli impegni internazionali che il paese terzo o l'organizzazione internazionale hanno assunto, la Commissione dovrebbe tenere in considerazione gli obblighi derivanti dalla partecipazione del paese terzo o dell'organizzazione internazionale a sistemi multilaterali o regionali, soprattutto in relazione alla protezione dei dati personali, nonché all'attuazione di tali obblighi. In particolare si dovrebbe tenere in considerazione l'adesione dei paesi terzi alla convenzione del Consiglio d'Europa, del 28 gennaio 1981, sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale e relativo protocollo addizionale. La Commissione, nel valutare l'adeguatezza del livello di protezione nei paesi terzi o nelle organizzazioni internazionali, dovrebbe consultare il comitato».

[215] Greanleaf G., *How far can Convention 108+ 'globalise'? Prospects for Asian accessions*, Computer Law & Security Review, volume 40, Maggio 2021, pag. 2. Disponibile online al seguente link:

https://www.researchgate.net/publication/341316791_How_far_can_Convention_108_'globalise'_Prospects_for_Asian_accessions

[216] Greenleaf G., *'Modernised' Data Protection Convention 108 and the GDPR,* Privacy Laws & Business International Report, 13 Novembre 2018, pag. 2. Disponibile online al seguente link:

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3279984

[217] González G., Van Brakel R., De Hert P. (edito da), *Research Handbook on Privacy and Data Protection Law*, 2018, pag. 33; in tal senso anche il Garante, alla pagina:

paesi, la Convenzione 108+ rappresenterebbe una miglior base comune per la circolazione transfrontaliera dei dati personali, specialmente alla luce della decisione sul caso Schrems II[218].

Essendo stata menzionata la direttiva 2002/58 sulle comunicazioni elettroniche, occorre precisare che è in discussione una proposta di regolamento (detto Regolamento e-privacy[219]) che dovrebbe sostituire la succitata direttiva. Essendo trascorsi ormai molti anni dal 2002, si ritiene necessario un aggiornamento della disciplina (visto lo sviluppo delle tecnologie delle comunicazioni) sulle comunicazioni elettroniche; l'obiettivo è anche quello di uniformare gli ordinamenti europei optando per la forma del regolamento a discapito di quella della direttiva.

Per quanto riguarda l'impianto normativo italiano in materia di protezione dei dati personali, la prima fonte in ordine cronologico è stata la legge n. 675 del 1996. Questa serviva ad applicare internamente la Direttiva madre emanata l'anno prima dal legislatore europeo. La legge n. 675 del 1996 era dunque un atto dovuto. La seconda fonte emanata in ordine cronologico è stata poi il c.d. Codice privacy (d.lgs. 196/2003) che recepiva ed applicava non solo la Direttiva madre ma anche la direttiva 2002/58/CE relativa alle comunicazioni elettroniche. Questo è stato più volte modificato dalla sua emanazione sino a giungere alla sua formulazione odierna. Le modifiche si devono a due ordini di ragioni: innanzitutto, come già detto, una fonte emanata in applicazione di una direttiva può scegliere autonomamente gli strumenti attraverso i quali perseguire l'obiettivo scelto dalla fonte europea; ciò ha condotto il legislatore italiano a modificare più volte il Codice privacy, cambiando appunto le vie per perseguire lo scopo fissato dalla Direttiva madre. La seconda ragione si deve invece all'emanazione del Regolamento numero 679 del 2016. Seppur la fonte del regolamento europeo sia più stringente per gli Stati unionali (in virtù della sua funzione di uniformazione degli ordinamenti), questo non può prescindere da una disciplina di dettaglio. Invero il GDPR è molto preciso, tant'è che si spinge fino alla normazione di procedure (si veda ad esempio quella prevista dall'articolo 33 sulla notifica all'autorità di controllo); purtuttavia non sufficientemente dettagliato per essere applicato senza normative che lo integrino. A riprova di ciò, dopo l'emanazione del Regolamento, il legislatore italiano ha approvato delle importanti modifiche al Codice privacy attraverso il d.lgs. del 10 agosto 2018, n. 101 (decreto di armonizzazione), volte a recepire le modifiche apportate dal

https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9088792

[218] Decisione disponibile online al seguente link:
https://curia.europa.eu/juris/liste.jsf?language=it&num=C-311/18

[219] Proposta di Regolamento del Parlamento europeo e del Consiglio relativo al rispetto della vita privata e alla protezione dei dati personali nelle comunicazioni elettroniche e che abroga la direttiva 2002/58/CE (regolamento sulla privacy e le comunicazioni elettroniche). Bozza disponibile online al seguente link: https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf

Regolamento[220]. L'ultima modifica al Codice privacy si deve alla legge numero 205 del 3 Dicembre 2021, che in particolare ha ampliato i poteri di trattamento delle pubbliche amministrazioni[221].

Alla luce di ciò è possibile affermare che le disposizioni del Codice privacy vadano lette in combinato disposto con quelle del Regolamento. Per esigenze di semplificazione si farà riferimento al Codice privacy *post* decreto di armonizzazione chiamandolo «nuovo codice privacy», in contrapposizione al «vecchio codice privacy» (ossia il d.lgs. 196/2003).

In ultimo, non può esimersi dal menzionare il lavoro operato su queste fonti dalle autorità garanti dei dati personali dei singoli Stati dell'Unione, dal Garante europeo dei dati personali e dal Comitato europeo per la protezione dei dati.

Iniziando dalle autorità nazionali, queste sono istituite dall'articolo 51 del Regolamento, secondo cui: «ogni Stato membro dispone che una o più autorità pubbliche indipendenti siano incaricate di controllare l'applicazione del presente regolamento…»[222]. Queste vengono definite autorità di controllo, e giocano un ruolo fondamentale nell'attuazione del diritto europeo della protezione e circolazione dei dati personali.

Compito primario delle autorità di controllo è vigilare sulla corretta e coerente applicazione del Regolamento nel proprio paese di riferimento. Questo obiettivo viene conseguito attraverso i poteri conferiti ad esse dal GDPR.

Innanzitutto, l'art. 57 prevede poteri di tipo consultivo: le autorità devono difatti riportare le proprie opinioni ai Parlamenti, ai Governi e ad altri organismi e istituzioni. Importante è poi la relazione annuale che queste devono presentare, in cui esamina lo stato della protezione dei dati personali verificatasi nei trattamenti all'interno del proprio stato di riferimento. Per rendere effettivi i compiti di controllo di cui queste sono istituite sono stati disposti poteri di indagine azionabili d'ufficio. Nello specifico tali poteri sono finalizzati al controllo sull'effettiva applicazione delle disposizioni del Regolamento (ad esempio chiedendo informazioni al titolare o al responsabile del trattamento) e quindi al rilevamento di ipotetiche violazioni delle norme dello stesso.
Oltre a questi poteri ne sono previsti altri, di tipo correttivo, che si sostanziano nella possibilità di ingiungere al titolare o al responsabile del trattamento il compimento di determinate operazioni per garantire la protezione dei dati personali (*ex multis* la possibilità di ingiungere la rettifica dei dati personali come da richiesta dell'interessato).

[220] L'articolo 2 del Regolamento, rubricato «Finalità», stabilisce infatti: «il presente codice reca disposizioni per l'adeguamento dell'ordinamento nazionale alle disposizioni del regolamento».

[221] Legge 3 Dicembre 2021, n. 205. Disponibile online al seguente link: https://www.gazzettaufficiale.it/eli/id/2021/12/07/21G00228/sg

[222] GDPR.

Inoltre, l'articolo 83 del Regolamento attribuisce loro anche il potere di comminare sanzioni amministrative.

Per quanto concerne la natura di questi atti invece, è possibile affermare che abbiano natura vincolante. In dottrina è infatti condiviso che: «i predetti provvedimenti costituiscono una misura giuridicamente vincolante e che, proprio in ragione del vincolo giuridico che instaurano, rappresentano il fondamento del potere esercitato *ex* articolo 58»[223]. Infine occorre segnalare che ai sensi dell'ultimo paragrafo dell'articolo 58 i poteri di queste autorità possono essere ampliati tramite legge primaria.

Per quanto riguarda invece il Comitato europeo per la protezione dei dati[224] (o Comitato) è stato creato dal GDPR e prende il posto del Gruppo di lavoro *ex* articolo 29 (o Gruppo di lavoro, che ritornerà spesso nel proseguimento della trattazione) che era invece stato predisposto dalla Direttiva madre. Il Regolamento ha notevolmente ampliato il ruolo del Comitato e delle autorità garanti nazionali. Ai sensi dell'articolo 70 il Comitato «garantisce l'applicazione coerente del presente regolamento» e lo fa principalmente attraverso un'attività di consulenza nei confronti della Commissione europea, elaborazione di linee guida e raccomandazioni. Di particolare rilevanza è la funzione del Comitato in tema di trasferimento transfrontaliero di dati[225] o la valutazione annuale *ex* articolo 71, in merito allo stato dei trattamenti all'interno dell'Unione.

Oltre alla funzione consultiva di cui sopra, al Comitato è attribuito anche il potere di emettere decisioni vincolanti nell'ambito del meccanismo di coerenza. Il ruolo del Comitato è dunque diventato centrale all'interno dell'Unione. A causa degli sviluppi tecnologici citati nel corso dei paragrafi precedenti gli individui rischiano di perdere la consapevolezza e la libertà in gran parte delle loro decisioni, e di essere orientati da terzi nel compimento di certe scelte. Il Comitato, attraverso la sua attività consultiva ed i suoi poteri vincolanti, è chiamato dunque a difendere i valori della libertà e della democrazia, attraverso la regolamentazione degli sviluppi tecnologici maggiormente impattanti (senza ovviamente fermare totalmente il progresso tecnologico[226].

---

[223] Bolognini L., Pelino E., Bistolfi C., *Il Regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Giuffrè Editore, Milano, 2016, pag. 624.

[224] Pagina ufficiale disponibile al seguente link: https://edpb.europa.eu/edpb_it

[225] L'articolo 70 paragrafo 1, lettera s, prevede che il Comitato «fornisce alla Commissione un parere per valutare l'adeguatezza del livello di protezione in un paese terzo o in un'organizzazione internazionale, così come per valutare se il paese terzo, il territorio o uno o più settori specifici all'interno di tale paese terzo, o l'organizzazione internazionale non assicurino più un livello adeguato di protezione. A tal fine, la Commissione fornisce al comitato tutta la documentazione necessaria, inclusa la corrispondenza con il governo del paese terzo, con riguardo a tale paese terzo, territorio o settore specifico, o con l'organizzazione internazionale».

[226] Zambrano V., *Il Comitato europeo per la protezione dei dati,* in Cuffaro V., D'Orazio R., Ricciuto V., *I dati personali nel diritto europeo*, 2019, pag. 999.

Infine, per quanto riguarda il Garante europeo dei dati personali, come si è detto è stato istituito attraverso il regolamento numero 45 del 2001.[227] L'ambito di intervento è più limitato rispetto ai due organismi analizzati poc'anzi. Ai sensi di questo regolamento, infatti, il Garante europeo «sorveglia l'applicazione delle disposizioni del presente regolamento a tutti i trattamenti dei dati personali eseguiti da un'istituzione o da un organismo comunitario»[228].

2.3 Il dato personale e l'identificazione

Il dato personale è l'oggetto di tutela della normativa sulla protezione dei dati personali. Definirlo è dunque il punto di partenza. Esso è caratterizzato da elementi che verranno illustrati nel presente paragrafo; oltre questi tipi di dati ve ne sono altri che, non presentando tali peculiarità, non possono essere definiti dati personali e in tal caso non si applicherà il GDPR. La qualifica di dato personale è tema strettamente inerente all'ambito di applicazione del Regolamento: i dati non personali non sono soggetti alla sua disciplina, potranno dunque essere raccolti senza il necessario adempimento degli obblighi previsti per i dati personali. Come si vedrà in seguito (cfr. paragrafo 2.4) i dati non personali sono spesso assimilati ai dati anonimi.

Il dato personale è definito dal GDPR all'articolo 4 (relativo alle definizioni). Il paragrafo 1, lettera 1 li definisce come:

> «qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale»[229].

Tale definizione non costituisce una rottura con quanto previsto dalle fonti precedenti al Regolamento, anzi, senza soluzione di continuità, si prosegue il percorso avviato dalla Convenzione 108 del 1981 e proseguito con la Direttiva madre[230]. Il dato personale, come si vedrà tra poco, è un

[227] Regolamento (CE) numero 45 del 2001, disponibile online al seguente link: https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32001R0045

[228] Articolo 1 paragrafo 2.

[229] GDPR.

[230] Bolognini L., Pelino E., *Codice della disciplina privacy*, 2019, pag. 29; Bygrave L. A., Tosoni L., *Article 4 (1). Personal data*, in Kuner C., Bygrave L. A., Docksey C., Drechsler L., *The EU General Data Protection Regulation (GDPR): A Commentary,* Oxford press, 13 Febbraio 2020, pag. 106; per le differenze ibidem pag. 108.

concetto parecchio ampio, che si è tentato di definire a più riprese: particolarmente rilevante[231] rimane l'opinione numero 4 del 2007 del Gruppo di lavoro[232]. Sebbene non recentissimo, questo documento è ancora in larga parte attuale[233], proprio in quanto adottato sulla base di una definizione molto simile, quella adottata dalla direttiva 95/46[234].

L'ampiezza del concetto di dato personale è una precisa scelta del Legislatore europeo. A testimonianza di ciò il Gruppo di lavoro *ex* articolo 29 sottolinea come questa scelta, condivisa dalla Commissione, dal Consiglio europeo e dal Parlamento, è la medesima operata nell'ambito della Convenzione 108, con l'obiettivo di includere qualsiasi informazione ricollegabile ad una persona identificabile[235](nello stesso senso anche la giurisprudenza della Corte di Giustizia[236]). Si precisa inoltre che «informazione» e «dato personale» non sono coincidenti. Il dato è la fonte dalla quale l'informazione viene estratta: l'informazione è l'elaborazione del dato[237].

Tornando alla definizione prevista nell'articolo 4, attualizzando quanto affermato dal Gruppo di lavoro, è possibile individuare quattro elementi caratteristici del dato personale. Il primo è individuabile nell'espressione «qualsiasi informazione»; il secondo nella parola «riguardante»; il terzo nella locuzione «identificata o identificabile» e infine nella condizione che si tratti di una «persona fisica».

Più approfonditamente, per informazione si intende il contenuto del dato, ossia il frutto della sua elaborazione. La persona fisica è il soggetto a cui il dato è riferibile grazie all'operazione del collegamento («riguardante»);

---

[231] Del Federico C., Popoli A. R., *Le definizioni*, in Finocchiaro G., *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Zanichelli, Torino, 2019, pag. 69.

[232] Parere 4/2007 sul concetto di dato personale. Disponibile online al seguente link: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1496512

[233] Bolognini L., Pelino E., *Codice della disciplina privacy*, 2019, pag. 29.

[234] La Direttiva madre definiva il dato personale come «qualsiasi informazione concernente una persona fisica identificata o identificabile («persona interessata»); si considera identificabile la persona che può essere identificata, direttamente o indirettamente, in particolare mediante riferimento ad un numero di identificazione o ad uno o più elementi specifici caratteristici della sua identità fisica, fisiologica, psichica, economica, culturale o sociale».

[235] Parere 4/2007 sul concetto di dato personale, pag.4. Sul punto anche Bolognini L., Pelino E., *Codice della disciplina privacy*, 2019, pag. 29.

[236] Caso C-434/16, Nowak, paragrafo 34: *«[T]he use of the expression 'any information' in the definition of the concept of 'personal data' ... reflects the aim of the EU legislature to assign a wide scope to that concept, which is not restricted to information that is sensitive or private, but potentially encompasses all kinds of information, not only objective but also subjective, in the form of opinions and assessments, provided that it 'relates' to the data subject*».
Per una lettura restrittiva del dato personale vedasi invece Joined Cases C-141/12 and C-372/12, YS.

[237] Del Federico C., Popoli A. R., *Le definizioni*, 2019, pag 66.

infine la persona fisica dev'essere singolarmente individuata o individuabile (altrimenti l'informazione sarà anonima) [238].

Nell'analisi dei quattro elementi di cui sopra, è preferibile iniziare dall'espressione «qualsiasi informazione».

Innanzitutto «l'informazione va intesa come una rappresentazione di cose, fatti, persone…» in quanto si ritiene applicabile l'articolo 2712 del codice civile[239]. La scelta dell'aggettivo indefinito collettivo «qualsiasi» rimarca la volontà del legislatore di non restringere in alcun modo il novero delle informazioni oggetto di tutela, da quelle oggettive (si riporta l'esempio di una sostanza nel sangue) a quelle soggettive. Queste ultime vengono utilizzate non di rado nel settore bancario per valutare chi richiede un prestito, così come in quello assicurativo o del mercato del lavoro[240].

Relativamente al contenuto invece non è richiesto che l'informazione sia vera o dimostrata. Tant'è che la normativa sulla protezione dei dati personali prevede la possibile inesattezza delle informazioni, e contro di essa pone appositi strumenti d'impugnazione[241]. Inoltre «un'informazione falsa o imprecisa produce tendenzialmente effetti pregiudizievoli ancor più che un'informazione corretta»[242].

Neppure il formato costituisce un limite al tipo di informazioni tutelabili: saranno dati personali a prescindere dal supporto utilizzato, carta, digitale ecc., e dalla forma, che sia essa alfabetica, numerica, acustica ecc. Ciò deriva dal fatto che si cerchi di tutelare i dati personali anche (e soprattutto) nell'ambito dei trattamenti automatizzati. Così, anche i dati in forma di suoni o immagini possono costituire dati personali qualora siano soddisfatti anche gli altri requisiti[243].

---

[238] «Giova un esempio. "Tizio ha una laurea in matematica" è un dato personale. Il nome "Tizio" soddisfa il (doppio) requisito dell'identificazione di una persona fisica. "Ha una laurea in matematica" è, nel suo complesso, il contenuto informativo. Esso non coincide necessariamente con un'unica unità informativa, ma può aggregarne molteplici, tre nel caso proposto: la laurea, la specifica materia di laurea e la titolarità della stessa, espressa dal verbo "avere". "ha" non costituisce il collegamento, ma è un elemento dell'informazione, sostituibile con qualsiasi altro appropriato ("sta conseguendo", "ha rinunciato a", "apprezza", "ritiene utile", ecc.). Il collegamento è nella sintassi della frase», Bolognini L., Pelino E., Bistolfi C., *Il Regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, 2016, pag. 44.

[239] Del Federico C., Popoli A. R, *Le definizioni*, 2019, pag. 70; Bolognini L., Pelino E., *Codice della disciplina privacy*, 2019, pag. 30.

[240] Parere 4/2007 sul concetto di dato personale, pag. 6; commento di De Franceschi A., in D'Orazio R., Finocchiaro G., Pollicino O., Resta G., *Codice della privacy e data protection*, 2021, pag. 158; Pizzetti F., *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Giappichelli, Torino, 2016, pag.184.

[241] Parere 4/2007 sul concetto di dato personale, pag. 6.

[242] Del Federico C., Popoli A. R, *Le definizioni*, 2019, pag. 70.

[243] Parere 4/2007 sul concetto di dato personale, pag. 8; commento di De Franceschi A., in D'Orazio R., Finocchiaro G., Pollicino O., Resta G., *Codice della privacy e data protection*, 2021, pag.158; Del Federico C., Popoli A. R, *Le definizioni*, 2019, pag. 70.

Per dare un'idea dell'ampiezza del concetto di dato personale, il gruppo di lavoro *ex* articolo 29 propone il seguente esempio:

> «Nell'ambito di un test neuropsichiatrico ai fini di un procedimento giudiziario per l'affidamento di una bambina, è stato presentato un suo disegno dei familiari. Il disegno dà informazioni sullo stato d'animo della bambina e sui suoi sentimenti per i diversi membri della famiglia. Queste informazioni possono di per sé costituire "dati personali" in quanto rivelano informazioni sulla bambina (la sua salute mentale), ma anche sul comportamento della madre o del padre. I genitori possono quindi, in questa fattispecie, esercitare il diritto di accesso a tale informazione specifica»[244].

Come già detto il dato personale è l'oggetto di tutela della materia dei dati personali, tutto ciò che non lo è rimane fuori dall'ambito applicativo della disciplina. Tuttavia vi sono casi in cui informazioni non classificabili come dati personali, qualora considerate unitamente ad identificativi, possono divenire dati personali: ad esempio i dati relativi allo stipendio potrebbero non essere dati personali se considerati singolarmente (si ponga il caso di un'offerta di lavoro pubblicizzata in cui si indica solo il tipo di lavoro e il salario offerto). Se invece quei dati sullo stipendio fossero collegati agli identificativi del soggetto che lo percepisce, essi diverranno dati personali, in quanto in grado di fornire informazioni su una persona fisica determinata[245].

Proseguendo, il secondo elemento caratterizzante il dato personale è il collegamento, il quale può essere definito come «un'operazione del pensiero. Come tale, è disomogeneo rispetto agli altri componenti. È cioè, un'operazione *sul* dato, ma tendenzialmente non fa parte della formulazione del dato»[246].

Il collegamento tra il contenuto informativo del dato e la persona fisica è anch'esso un concetto generico dall'ampia interpretabilità: secondo il Gruppo di lavoro un'informazione concerne una persona fisica quando la riguarda. Talvolta questo rapporto può essere individuato facilmente (si prenda come esempio il caso di un fascicolo del personale in cui vengono contenute ed abbinate le informazioni relative alle persone fisiche impiegate e alla loro situazione lavorativa). Vi sono casi invece in cui stabilire la relazione tra dati personali ed interessato non è così semplice, ad esempio quando le informazioni concernono oggetti e non persone. In questi casi,

---

[244] Parere 4/2007 sul concetto di dato personale, pag. 8.

[245] Information commissioner's office, *Determining what is personal data*, pag. 12. Disponibile online al seguente link:

https://ico.org.uk/media/for-organisations/documents/1554/determining-what-is-personal-data.pdf

Sul tema: Cherciu N., *Non-personal data processing – why should we take it personally?*, European Journal of Privacy Law & Technologies, volume 2, 2020.

[246] Bolognini L., Pelino E., Bistolfi C., *Il Regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, 2016, pag. 47.

infatti, la relazione tra informazione e persona fisica individuata o individuabile non è esclusa; gli oggetti possono appartenere ad una persona, o possono esercitare una particolare influenza su di esse, oppure hanno una vicinanza geografica o fisica ad altre persone fisiche o ad altri oggetti dalla quale è possibile desumere in via indiretta delle informazioni su persone fisiche individuate o individuabili[247].

A chiarimento di ciò il Gruppo di lavoro propone il seguente esempio:

> «Il valore di una casa specifica costituisce un'informazione su un oggetto. Beninteso, le norme sulla protezione dei dati non si applicano se l'informazione è usata soltanto per illustrare il livello dei prezzi immobiliari in un dato quartiere. Però, in alcune circostanze, tale informazione meriterebbe di essere considerata anche come dato personale: la casa è in effetti una proprietà e in quanto tale servirà per determinare in che misura il proprietario è tassabile. Da questo punto di vista l'informazione costituisce indiscutibilmente un dato personale»[248].

Nel prosieguo dell'analisi, il Gruppo di lavoro spiega come per stabilire se i dati «concernono» una persona, dovrebbe ricorrere un elemento di «contenuto», di «finalità», o di «risultato»[249].

Per quanto concerne l'elemento del contenuto, questo viene ritenuto il più intuitivo: un'informazione concerne una persona quando, in base alle circostanze *de quo*, la riguarda: è il caso dei risultati delle analisi mediche di un paziente, o del codice a barre incorporato nel documento d'identità di un individuo[250].

Relativamente all'elemento della finalità invece si osserva che: anche i dati non direttamente afferenti una persona fisica possono essere considerati dati personali qualora essi vengano utilizzati, tenendo conto delle circostanze del caso concreto, al fine di influire sul comportamento di un individuo, o per effettuare su questi delle valutazioni[251].

L'esempio riportato a riguardo concerne un registro chiamate di un telefono di una società:

> «Il registro chiamate di un telefono in una data società fornisce informazioni sulle chiamate effettuate da quel telefono collegato a una certa linea. Queste informazioni possono concernere diversi soggetti. Da un lato, la linea è a disposizione della società e questa è tenuta per contratto a pagare le chiamate. L'apparecchio telefonico è sotto il controllo di un impiegato negli orari di lavoro e si presume che le chiamate vengano effettuate da quell'impiegato. Il registro chiamate può anche

[247] Parere 4/2007 sul concetto di dato personale, pag. 9.

[248] Ibidem.

[249] Ibidem, pag. 10. Sul punto anche Pizzetti F., *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, 2016, pag. 185.

[250] Parere 4/2007 sul concetto di dato personale, pag. 10.

[251] Ibidem.

fornire informazioni sulla persona chiamata. Il telefono può essere usato pure da altro personale autorizzato in assenza dell'impiegato (ad esempio, addetti alle pulizie). Per scopi diversi, le informazioni sull'utilizzo di quell'apparecchio possono essere messe in relazione con la società, l'impiegato o il personale addetto alle pulizie (ad esempio, per verificare l'ora in cui l'addetto alle pulizie lascia il luogo di lavoro, poiché è tenuto a confermare per telefono a che ora lascia i locali prima di chiuderli a chiave). Si noti che il concetto di dati personali qui si estende sia alle chiamate in entrata che a quelle in uscita, nella misura in cui entrambe contengono informazioni sulla vita privata, sui rapporti sociali e sulle comunicazioni delle persone»[252].

L'ultimo elemento illustrato è quello del risultato: qualora dei dati, anche non relativi direttamente ad una persona fisica, se trattati, siano in grado di impattare sui diritti e gli interessi di una persona fisica individuata o individuabile, questi verranno considerati dati personali concernenti la persona su cui influiscono. Il Gruppo di lavoro precisa che non è importante che l'impatto sia importante, ma che da questa influenza ne derivi un trattamento diverso di quella persona rispetto ad altre[253].

L'esempio proposto in questo caso riguarda l'installazione di un sistema di localizzazione satellitare per individuare la posizione dei taxi disponibili in tempo reale:

«Obiettivo del trattamento è offrire un servizio migliore e risparmiare carburante, assegnando ad ogni cliente il veicolo che si trova più vicino al suo indirizzo. Strettamente parlando, i dati necessari al funzionamento del sistema sono dati relativi ad automobili, non ai conducenti. La finalità del trattamento non è valutare le prestazioni dei tassisti, ad esempio ottimizzandone gli itinerari. Eppure, il sistema permette di monitorare le prestazioni dei tassisti e di controllare se rispettano i limiti di velocità, se scelgono itinerari adeguati, se sono al volante o se stanno facendo una pausa, ecc. Il sistema quindi può esercitare un forte impatto su queste persone e si può considerare che i dati da quello elaborati concernono anche persone fisiche. Il loro trattamento dovrebbe essere quindi soggetto alle norme sulla protezione dei dati»[254].

In ultimo, il Gruppo di lavoro sottolinea come affinché si abbia dato personale sia sufficiente la sussistenza di anche uno soltanto dei suddetti requisiti del collegamento. Questi vengono dunque considerati condizioni alternative (e non cumulative) della personalità del dato. Oltre il contenuto informativo e l'operazione del collegamento vi è l'elemento della persona fisica. L'informazione estraibile dal dato è infatti collegata necessariamente ad una persona fisica (come si vedrà successivamente, individuata o individuabile). Innanzitutto, il fatto che l'articolo 4 del Regolamento

[252] Parere 4/2007 sul concetto di dato personale, pag. 11
[253] Ibidem.
[254] Ibidem.

specifichi che il dato personale si riferisca ad una persona fisica indica che la disciplina non si applica alle persone giuridiche. A conferma di ciò, lo stesso Regolamento, al considerando 14 stabilisce che:

> «è opportuno che la protezione prevista dal presente regolamento si applichi alle persone fisiche, a prescindere dalla nazionalità o dal luogo di residenza, in relazione al trattamento dei loro dati personali. Il presente regolamento non disciplina il trattamento dei dati personali relativi a persone giuridiche, in particolare imprese dotate di personalità giuridica, compresi il nome e la forma della persona giuridica e i suoi dati di contatto»[255].

Sempre in tal senso l'articolo 1 paragrafo 1 e 2:

> «il presente regolamento stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati. Il presente regolamento protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali»[256].

Il Regolamento sembra dunque chiaro nell'escludere le persone giuridiche dal suo ambito applicativo; tuttavia, il considerando citato richiede alcune riflessioni. É possibile, infatti, notare come si specifichi che «il presente regolamento non disciplina il trattamento dei dati personali relativi a persone giuridiche…»; i dati personali possono dunque anche essere riferibili a persone giuridiche, ma questo regolamento non se ne occupa. Viene riportato l'esempio del nome, della forma e dei dati di contatto della persona giuridica, che secondo il Legislatore europeo sono comunque dati personali, seppur relativi a persone giuridiche. Quanto appena evidenziato conduce alla conclusione che i dati personali possono essere relativi sia a persone fisiche che giuridiche, ma il regolamento 679/2016 disciplina soltanto in merito a quelli delle persone fisiche. A causa di ciò, i dati personali relativi alle persone giuridiche possono essere acquisiti e trattati senza che queste possano vantare i diritti previsti dal Regolamento. Non possono neppure ottenere un'informativa che li renda edotti sulle finalità e modalità del trattamento. Per lo stesso motivo, chi tratterà quei dati non sarà soggetto ai principi del trattamento previsti per dalla normativa relativa alla protezione dei dati personali. Detto questo preme sottolineare come attraverso l'opinione 04/2007 il Gruppo di lavoro sia andato oltre rispetto alla generale divisione tra persona fisica e giuridica. Lo si vede in particolare quando afferma che anche le informazioni sulle

[255] GDPR.
[256] GDPR.

persone giuridiche possono considerarsi relative a persone fisiche qualora, alla luce delle circostanze del caso concreto, e conformemente ai criteri sul collegamento di cui sopra, queste informazioni concernano delle persone fisiche. In questi casi queste informazioni saranno dati personali. Esemplificando, il nome della società "Diritto", pur essendo un dato personale della stessa, non sarà soggetto alla disciplina prevista dal Regolamento, in quanto neppure attraverso i tre criteri di contenuto, risultato e finalità è possibile individuare una persona fisica. Se la stessa società si chiamasse invece con il nome del suo titolare, ossia "Mario Rossi", allora questo nome-identificativo verrà considerato non già come dato personale afferente la società, ma come dato personale relativo alla persona fisica Mario Rossi[257]. É possibile dunque concludere che il Regolamento si applica soltanto ai dati personali delle persone fisiche.

Per quanto riguarda l'ordinamento giuridico nostrano, l'Italia è uno di quei paesi che per quanto riguarda la *quaestio* succitata ha intrapreso un percorso tutto suo, che il Garante ha descritto nel provvedimento n. 262 del 20 settembre 2012 in ordine all'applicabilità alle persone giuridiche del Codice in materia di protezione dei dati personali a seguito delle modifiche apportate dal d.l. n. 201/2011[258]. La Direttiva madre aveva previsto la protezione dei dati personali solo per le persone fisiche mentre sia la legge n. 675 del 1996 che il Codice privacy hanno optato per l'estensione anche alle persone giuridiche. Proprio il Codice privacy, nella sua formulazione originale, ricalcando la legge n. 675 del 1996, all'articolo 4 definiva i dati personali come: «qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale». Dunque, nel 1996 il nostro ordinamento ha previsto la disciplina sulla protezione dei dati personali anche per quelle informazioni riferibili alle persone giuridiche, mentre la Direttiva madre aveva delimitato l'ambito di applicazione alle sole persone fisiche. Questa differenza tra ordinamenti non costituiva comunque un contrasto in quanto era stata la medesima direttiva a concedere

[257] Parere 4/2007 sul concetto di dato personale, pag. 24: «le informazioni sulle persone giuridiche possono considerarsi "concernenti" persone fisiche in virtù della loro situazione specifica, conformemente ai criteri stabiliti nel presente documento. È quel che accade quando il nome di una persona giuridica deriva dal nome di una persona fisica, oppure nel caso dell'indirizzo e-mail di un'impresa di norma usato da un dato dipendente, o delle informazioni su una piccola impresa (giuridicamente un "oggetto" piuttosto che una persona giuridica) che possono descrivere il comportamento del suo titolare. In tutti questi casi, in cui i criteri di "contenuto", "finalità" o "risultato" fan sì che le informazioni su una persona giuridica o su un'impresa possano considerarsi come "concernenti" una persona fisica, è opportuno considerare tali informazioni come dati personali e si applicano le norme di protezione dei dati».

[258] Garante per la protezione dei dati personali. Provvedimento n. 262 del 20 settembre 2012. Disponibile online al seguente link:

https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2094932

discrezionalità agli stati in merito alla possibilità di estendere la tutela alle persone giuridiche[259].

Tale scelta ha condotto principalmente a due ordini di conseguenze. Il primo è relativo ai titolari del trattamento dei dati personali delle persone giuridiche, che divenivano soggetti ai principi e agli obblighi previsti per il trattamento. Il secondo invece è rappresentato da quei diritti e garanzie riconosciuti agli interessati ora anche persone giuridiche.

Nel 2011 però la situazione cambia. La legge 214/2011[260] (c.d. decreto "Salva Italia"), che converte in legge il d.l. 201/2011, nell'ottica di ridurre gli adempimenti amministrativi per le imprese, all'articolo 40 comma 2[261] stabilisce l'espunzione dei riferimenti alle persone giuridiche. In altre parole, si ha un ritorno all'originario ambito applicativo già disegnato dalla Direttiva madre, con i dati personali riferibili alle sole persone fisiche. Come già detto il Codice privacy ha recepito anche la direttiva 58/2002. Ciò significa che prevede la tutela preposta per i dati personali delle persone giuridiche nell'ambito delle comunicazioni elettroniche (articoli 121 e seguenti). Continuando sulla specificazione di chi sia una persona fisica, il Gruppo di lavoro prosegue affermando che, in virtù del fatto che per il diritto civile i defunti non sono più considerati persone fisiche, le informazioni ad essi relative non sono considerabili dati personali[262]. Quanto appena detto è tuttavia mitigato dal fatto che i singoli ordinamenti nazionali possono prevedere una protezione anche per i dati personali dei defunti che si riferiscano a persone in vita. Il Gruppo di lavoro riporta un esempio:

> «l'informazione che la defunta Gaia soffriva di emofilia indica che suo figlio Tizio soffre della stessa malattia, che è connessa a un gene presente nel cromosoma X. Pertanto, quando le informazioni costituenti dati di un defunto possono

[259] Confermato dal Gruppo di lavoro nell'opinione 04/2007: «La Corte di giustizia delle Comunità europee ha precisato che nulla impedisce che uno Stato membro estenda la portata della normativa nazionale di attuazione della direttiva 95/46 a settori non compresi nell'ambito di applicazione di quest'ultima, purché non vi osti alcuna altra disposizione del diritto comunitario. Di conseguenza, alcuni Stati membri come l'Italia, l'Austria e il Lussemburgo hanno esteso l'applicazione di alcune disposizioni della legislazione nazionale adottata in conformità della direttiva (come quelle sulle misure di sicurezza) al trattamento dei dati sulle persone giuridiche».

[260] Legge 214/2011, disponibile online al seguente link:
http://www.lexitalia.it/leggi/2011-214.pdf

[261] Articolo 40, legge 214/2011: «per la riduzione degli oneri in materia di privacy, sono apportate le seguenti modifiche al decreto legislativo 30 giugno 2003, n. 196: a) all'articolo 4, comma 1, alla lettera b), le parole «persona giuridica, ente od associazione» sono soppresse e le parole «identificati o identificabili» sono sostituite dalle parole «identificata o identificabile». b) All'articolo 4, comma 1, alla lettera i), le parole «la persona giuridica, l'ente o l'associazione» sono soppresse. c) Il comma 3-bis dell'articolo 5 è abrogato. d) Al comma 4, dell'articolo 9, l'ultimo periodo è soppresso. e) La lettera h) del comma i dell'articolo 43 è soppressa».

[262] Parere 4/2007 sul concetto di dato personale, pag. 22. Nello stesso senso Bygrave L. A., Tosoni L., *Article 4 (1). Personal data*, 2020, pag. 112.

considerarsi concernenti nel contempo anche persone viventi e configurare dati personali soggetti alla direttiva, i dati personali del defunto possono godere indirettamente della protezione delle norme della direttiva»[263].

Avendo definito cosa si intende per informazione concernente una persona fisica, rimane da illustrare il requisito della identificazione o identificabilità di quest'ultima. A tal proposito, sempre il Gruppo di lavoro afferma che una persona fisica si può considerare identificata quando è distinta all'interno di un gruppo. È invece identificabile quando, sebbene non ancora individuata, è possibile distinguerla tra altre persone[264].Secondo alcuni autori «"identificazione/identificabilità" vale allora nel senso di "individuazione/individuabilità" o di "riconoscimento/riconoscibilità", quando della persona fisica individuata o individuabile si abbia conoscenza pregressa»[265].
Tale impostazione sarebbe confermata dal considerando 26 che recita: «...per stabilire l'identificabilità di una persona è opportuno considerare tutti i mezzi, come l'individuazione, di cui il titolare del trattamento o un terzo può ragionevolmente avvalersi per identificare detta persona fisica direttamente o indirettamente»[266]. Nella formulazione originale appare ancora più evidente in quanto il suddetto considerando utilizza l'espressione «*singling out»*. Il processo di identificazione avviene attraverso almeno un identificativo, per il quale si intende un elemento del dato che consente il processo di identificazione della persona fisica. Questo elemento può essere di diverso tipo, ad esempio in un articolo di giornale l'identificativo potrebbe essere l'immagine di una persona, o il suo nome. Questi, dunque, non sono i dati personali, ma gli identificativi: Tizio non è la persona in sé, ma il nome anagrafico utilizzato per identificare quella persona[267]. Gli identificativi vengono generalmente suddivisi in diretti ed indiretti; nella prima categoria rientrano il nome, il cognome, la data di nascita ecc.; tra quelli indiretti invece il numero di telefono, il numero di targa, il codice fiscale, i dati relativi all'ubicazione, gli identificativi online, ecc. Tale ultima categoria permette l'identificazione della persona fisica solo se gli identificativi sono uniti ad altri dati (ad esempio, nella maggior parte dei casi il numero di targa porta all'individuazione del proprietario solo se si consulta l'apposito registro in cui il numero di targa è collegato al proprietario del mezzo).

Questa suddivisione costituisce tuttavia solo un punto di partenza in quanto volta per volta bisognerà valutare come può avvenire l'identificazione: ad esempio gli identificativi diretti "Mario Rossi" non costituiranno sempre e comunque dati personali. Ciò si deve al fatto che

[263] Parere 4/2007 sul concetto di dato personale, pag. 22.

[264] Ibidem, pag. 12.

[265] Bolognini L., Pelino E., Bistolfi C., *Il Regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, 2016, pag. 52.

[266] GDPR.

[267] Parere 4/2007 sul concetto di dato personale, pag. 48.

esistono molte persone fisiche individuabili attraverso essi, ma il requisito affinché si abbia dato personale secondo articolo 4 del Regolamento è che queste informazioni consentono l'identificazione/identificabilità di una persona fisica specifica. Se gli identificativi "Mario Rossi" vengono però attenzionati insieme ad altre informazioni, ad esempio il peso, l'altezza e la professione, potrebbe essere possibile individuare una persona fisica specifica e quindi si sarà dinanzi a dei dati personali.

Allo stesso modo, gli identificativi diretti più comuni, come il nome e il cognome, non sono necessari affinché si abbia l'identificazione di un soggetto, basti pensare al fatto che generalmente si è in grado di identificare i vicini di casa, anche se di questi non si conosce il nome. A proposito del nome, dunque, si può concludere sottolineando l'effettiva equipollenza tra questo e ogni altro tipo di identificativo[268]. Quanto appena detto vale anche per gli identificativi indiretti, ad esempio «rispetto a un familiare di un interessato intestatario di una targa automobilistica, la targa potrebbe costituire un identificativo diretto, ove il familiare l'associ direttamente all'interessato senza necessità di consultazione di registri»[269]. Proseguendo, da quanto emerge dal parere, è possibile affermare come l'identificabilità di una persona fisica possa dipendere anche dal soggetto in possesso dei dati e dalle finalità del suo trattamento: si pensi a due fotografi presenti ad una manifestazione di piazza, che scattano la medesima foto. Questi soggetti sono un fotografo di professione ed un agente di polizia. Il primo ha come finalità fotografare quel movimento della manifestazione, dunque, è improbabile che la foto contenga dati personali, in quanto non verrà utilizzata dal fotografo per identificare i manifestanti. Il caso del poliziotto invece è differente, in quanto è possibile presumere che utilizzerà quella foto per individuare determinati individui in caso di attività illegali perpetrate durante la manifestazione[270]. In quest'ultimo caso vengono in gioco anche i mezzi di identificazione ragionevolmente utilizzabili per l'individuazione dell'interessato. Il riferimento a questi mezzi lo si trova nel considerando 26, il quale statuisce che «per stabilire l'identificabilità di una persona è opportuno considerare tutti i mezzi, come l'individuazione, di cui il titolare del trattamento o un terzo può ragionevolmente avvalersi per identificare detta persona fisica direttamente o indirettamente»[271]. Se non è ragionevole ritenere che il soggetto in possesso dei dati abbia i mezzi necessari per identificare la persona fisica cui i dati si riferiscono, questi non potranno essere considerati dati personali (poiché viene meno il requisito fondamentale dell'identificabilità). Si richiede dunque un giudizio di ragionevolezza sui mezzi utilizzabili dal possessore dei dati per identificare

[268] Bolognini L., Pelino E., *Codice della disciplina privacy*, 2019, pag. 30.

[269] Bolognini L., Pelino E., Bistolfi C., *Il Regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, 2016, pag. 58.

[270] Parere 4/2007 sul concetto di dati personale, pag. 16.

[271] GDPR. Sul punto il provvedimento dell'autorità garante del 15 ottobre 2015 [doc. web n. 4541143].

l'interessato[272]. Tra gli elementi da considerare per operare tale giudizio, il Gruppo di lavoro segnala il costo dell'identificazione, sottolineando però come questo non sia l'unico[273]. Impossibile prefigurare i mezzi adoperabili, tant'è che in dottrina è stato opinato che: «la nozione di "strumenti", occorre subito chiarire, è la più ampia possibile e indica qualsiasi processo, anche meramente deduttivo, attraverso il quale è possibile approdare all'identificazione»[274].

Ci si è chiesto se questa valutazione dovesse essere *ex ante* o *ex post*; il Gruppo di lavoro a proposito della questione ha affermato che il test è dinamico: va presa in considerazione sia lo stato dell'arte della tecnologia al momento del trattamento, sia l'orizzonte di sviluppo della stessa nell'arco di conservazione dei dati. Ciò perché l'identificazione può non essere possibile per via di insufficienze tecnologiche, che però, nel tempo, vengono colmate, ed ecco che l'identificazione diviene possibile mentre prima non lo era. Al titolare si richiede dunque di valutare continuamente l'identificabilità dell'interessato, e non solo nella primissima fase della raccolta dei dati[275].Queste valutazioni non vanno certo rapportate all'uomo medio della strada. Caso per caso bisognerà tentare di prefigurare i mezzi di cui il soggetto in possesso dei dati potrà ragionevolmente disporre per identificare l'interessato. Ad esempio, non sarà ragionevole ritenere che un artista di strada utilizzi un sistema di intelligenza artificiale per analizzare i dati biometrici dei soggetti di cui ha creato dei ritratti con il fine di identificarli. Un simile ragionamento potrà invece farsi per i grandi attori del mercato digitale mondiale, che sono in possesso di algoritmi avanzatissimi, in grado di identificare una persona fisica con grande accuratezza anche partendo da informazioni apparentemente non classificabili come dati personali[276].

2.4 Anonimizzazione e pseudonimizzazione

[272] «*If the identification of the data subject was prohibited by law or practically impossible on account of the fact that it requires a disproportionate effort in terms of time, cost and man-power, so that the risk of identification appears in reality to be insignificant'*» Caso Breyer C-582/14, paragrafo 46.

[273] Pizzetti F., *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Giappichelli, Torino, 2016, pag. 186.

[274] Bolognini L., Pelino E., Bistolfi C., *Il Regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, 2016, pag. 60.

[275] Parere 4/2007 sul concetto di dato personale, pag. 15. A proposito anche Pizzetti F., *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, 2016, pag. 187.

[276] Quarta A., *Mercati senza scambi. La metamorfosi del contratto nel capitalismo della sorveglianza*, Edizioni Scientifiche Italiane, Napoli, 2020, pag. 43. Raso F., Hilligoss H., Krishnamurthy V., Bavitz C., Levin K., *Artificial Intelligence & Human Rights: Opportunities & Risks*, Berkman Klein Center for Internet & Society Research Publication, 2018, pag.18.

Come già detto nel paragrafo precedente, i dati anonimi, ai sensi di quanto disposto dal considerando 26 del GDPR, non sono soggetti alla disciplina sulla protezione dei dati personali. Nel presente paragrafo si definirà cosa si intenda per dato anonimo e le relative problematiche, partendo da quanto espresso dal Gruppo di lavoro nell'opinione 05/2014 sulle tecniche di anonimizzazione, che costituisce tutt'oggi la fonte basilare in merito al tema dei dati anonimi.

Innanzitutto, l'articolo 4 del GDPR dedicato alle definizioni non si occupa di questo tipo di dati, dunque la definizione va ricostruita a livello sistematico. Il Gruppo di lavoro trae spunto dal considerando 26 della Direttiva madre, il quale prevede:

> considerando che i principi della tutela si devono applicare ad ogni informazione concernente una persona identificata o identificabile; che, per determinare se una persona è identificabile, è opportuno prendere in considerazione l'insieme dei mezzi che possono essere ragionevolmente utilizzati dal responsabile del trattamento o da altri per identificare detta persona; che i principi della tutela non si applicano a dati resi anonimi in modo tale che la persona interessata non è più identificabile;…».

Da tal considerando il Gruppo di lavoro ha estrapolato una definizione concettuale di dati anonimi, asserendo che questi si ottengono nel momento in cui sono privati degli elementi che permettono l'identificazione dell'interessato. Tale definizione non è stata intaccata dal Regolamento, che al considerando 26 prosegue nel solco tracciato dalla Direttiva madre[277], stabilendo che:

> «…I principi di protezione dei dati non dovrebbero pertanto applicarsi a informazioni anonime, vale a dire informazioni che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato. Il presente regolamento non si applica pertanto al trattamento di tali informazioni anonime, anche per finalità statistiche o di ricerca».

Vista la sincronia del considerando 26 e dell'articolo 4 del Regolamento con le definizioni di dato personale e dato anonimo della

[277] Hintze M., *Viewing the GDPR through a de-identification lens: a tool for compliance, clarification and consistency*, Oxford University Press, volume 8, questione 1, Febbraio 2018, pag. 8; Stalla-Bourdillon S., Knight A., *Anonymous Data v. Personal Data — A False Debate: An EU Perspective on Anonymization, Pseudonymization and Personal Data*, Wisconsin International Law Journal, 6 Marzo 2017.

Direttiva madre, il parere fornito dal Gruppo di lavoro può ritenersi tutt'oggi pienamente efficace [278].

I dati anonimi possono quindi essere, o dati non personali, o dati personali resi anonimi[279]. Si crea allora una contrapposizione tra dati personali e dati anonimi[280]. Il dato personale anonimizzato, sempre stando al considerando 26, si ha nel momento in cui il dato personale originario viene privato degli elementi che consentono l'identificazione dell'interessato[281]. Il Gruppo di lavoro evidenziava che «la direttiva non specifica come si debba o si possa effettuare il processo di anonimizzazione. L'accento è posto sul risultato: i dati devono essere tali da non consentire l'identificazione della persona interessata mediante "l'insieme" dei mezzi che "possono" essere "ragionevolmente" utilizzati»[282] e che un siffatto trattamento debba essere irreversibile. Sempre il Gruppo di lavoro sottolineava come una anonimizzazione così descritta sia equipollente ad una cancellazione, poiché rende impossibile un trattamento dal quale possa discendere l'identificazione di una persona.

Il parere inoltre evidenziava come, qualora un dato personale fosse anonimizzato, questo risultato sarebbe da intendersi come la conseguenza di un trattamento di dati personali. Inizialmente questi devono dunque essere raccolti e trattati in conformità alla legislazione applicabile[283] e solo attraverso un successivo specifico trattamento essi diventano anonimi, pertanto, solo in un secondo momento non sono più soggetti alla disciplina sulla protezione dei dati personali.

Da collegare all'anonimizzazione è anche il principio di conservazione temporanea dei dati, previsto all'articolo 5, paragrafo 1, lettera e, del Regolamento secondo cui i dati personali sono:

---

[278] Foglia C., *Il dilemma (ancora aperto) dell'anonimizzazione e il ruolo della pseudonimizzazione*, in Panetta R., *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, 2019, pag 317.

279 Finck M., Pallas F., *They who must not be identified—distinguishing personal from non-personal data under the GDPR*, International Data Privacy Law, 1 Ottobre 2019, pag. 13; Vokinger K. N., Stekhoven D. J., Krauthammer M., *Lost in Anonymization — A Data Anonymization Reference Classification Merging Legal and Technical Considerations*, The Journal of Law Medicine & Ethics, volume 48, questione 1, Marzo 2020, pag. 28.

[280] Si accoglie in tal senso l'interpretazione secondo cui «qualsiasi informazione, ove non sia dato personale, deve essere considerata "anonima", terzium non datur», Bolognini L., Pelino E., Bistolfi C., *Il Regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, 2016, pag 75.

[281] Pizzetti F., *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, 2016, pag.190.

[282] Gruppo di lavoro *ex* articolo 29, parere 05/2014 sulle tecniche di anonimizzazione adottato il 10 aprile 2014, pag. 6. Disponibile online al seguente link: https://ronchilegal.eu/wp-content/uploads/2017/12/Anonimizzazione-secondo-il-WP29-del-2014_it-1.pdf

[283] D'Acquisto G., Naldi M*., Big data e privacy by design: anonimizzazione pseudonimizzazione sicurezza*, Giappichelli, Torino, 22 Febbraio 2017, pag. 35.

«conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»)»[284].

Alla fine del periodo di conservazione i dati devono essere cancellati, oppure possono essere anonimizzati (in virtù dell'equipollenza con la cancellazione richiesta dal Regolamento)[285]. Premesso, dunque, che il GDPR pone un obbligo di risultato (l'anonimizzazione totale ed irreversibile dei dati personali), si potrebbe ritenere che la procedura di anonimizzazione, ossia il metodo, non abbia alcuna rilevanza. Il parere succitato invece non verte sui dati anonimi, ma sulle tecniche di anonimizzazione; in altre parole, non verte sul risultato (il dato anonimo) ma sul metodo (le procedure di anonimizzazione).

Il motivo è cardinale: è generalmente riconosciuto che il dato personale completamente ed immutabilmente anonimizzato sia un obiettivo quasi irraggiungibile[286]. L'anonimia di un dato personale potrebbe anche ottenersi, ma come si evidenzierà a breve, questa potrebbe ad un certo punto venir meno, rendendo così l'informazione nuovamente in grado di identificare l'interessato (e dunque nuovamente un dato personale, così soggetto alla relativa disciplina). In virtù di ciò, il Gruppo di lavoro, e la dottrina[287] che si è formata sul tema, tendono a valorizzare maggiormente il metodo piuttosto che il risultato. Quanto appena detto si chiarirà a breve, quando verranno chiariti ulteriori elementi preliminari.

Il Gruppo di lavoro enunciava quattro caratteristiche proprie dell'anonimizzazione intesa come metodo. Innanzitutto, l'anonimizzazione può essere il risultato di un trattamento di dati personali volto ad impedire,

[284] GDPR.

[285] Pizzetti F., *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, 2016, pag. 190.

[286] Foglia C., *Il dilemma (ancora aperto) dell'anonimizzazione e il ruolo della pseudonimizzazione,* 2019, pag 315; parere 05/2014 sulle tecniche di anonimizzazione, pag. 7 e 25; commento di De Franceschi A., 2021, pag. 160; Brasher E., *Addressing the Failure of Anonymization: Guidance from the European Union's General Data Protection Regulation*, Columbia Business Law Review, 2018, pag. 226; Zibuschka J., Kurowski S., Roßnagel H., Schunck C., Zimmermann C., *Anonymization Is Dead – Long Live Privacy*, Open Identity Summit, Marzo 2019, pag. 76; Kolain M., Grafenauer C., Ebers M., *Anonymity Assessment – A Universal Tool for Measuring Anonymity of Data Sets under the GDPR with a Special Focus on Smart Robotics*, Rutgers University Computer & Technology Law Journal, volume 48, numero 2, 2022, pag. 29; Bale C., Fischer J. L., Schneider M. J., Weber S., Chang, S., *Legally Anonymizing Location Data Under the GDPR* , Giugno 2022, pag. 5.

[287] Foglia C., *Il dilemma (ancora aperto) dell'anonimizzazione e il ruolo della pseudonimizzazione*, 2019, pag. 315.

in maniera irreversibile, l'identificabilità dell'interessato. In secondo luogo, l'Unione non prevede norme che stabiliscano tecniche di anonimizzazione da seguire (l'importante è il risultato). Bisogna inoltre prestare importanza ai mezzi che la tecnologia offre per l'identificazione degli individui: vista la continua crescita della potenza di calcolo dei computer, ciò che ieri non era un mezzo «ragionevolmente utilizzabile» ai fini dell'identificazione di una persona fisica, oggi potrebbe esserlo. Infine, occorre tenere presente che ogni tecnica di anonimizzazione presenta un fattore di rischio intrinseco[288].

L'ultima caratteristica è quella più importante: ogni tecnica di anonimizzazione presenta un rischio intrinseco residuo di reidentificazione dei dati, ed è per questo, come si è detto, che il Gruppo di lavoro e la dottrina maggioritaria si soffermino più sulle tecniche di anonimizzazione che non sul risultato (ritenuto a livello pratico quasi irraggiungibile).

Per capire come si è arrivati a questa conclusione bisogna tornare al considerando 26, nella parte in cui recita: «...per stabilire l'identificabilità di una persona è opportuno considerare tutti i mezzi, come l'individuazione, di cui il titolare del trattamento o un terzo può ragionevolmente avvalersi per identificare detta persona fisica direttamente o indirettamente»[289]. L'identificabilità dell'interessato dipende dai mezzi ragionevolmente utilizzabili da chi è in possesso dei dati (si rammenti quanto detto nel paragrafo precedente) e come già detto, affinché un dato personale diventi anonimo, sarà necessario privarlo degli elementi che permettono l'identificabilità della persona fisica[290].Questi due assunti vengono congiuntamente presi in considerazione dal Gruppo di lavoro, che, in merito alla Direttiva madre, affermava:

> «la direttiva suggerisce l'esame dei "mezzi … che possono essere ragionevolmente utilizzati" quale criterio da applicare per valutare se il processo di anonimizzazione sia sufficientemente affidabile, vale a dire se l'identificazione sia diventata "ragionevolmente" impossibile. Il contesto e le circostanze particolari di un caso specifico incidono direttamente sull'identificabilità»[291].

In altre parole, un dato è personale quando, attraverso mezzi ragionevolmente utilizzabili da chi possiede il dato (chiunque questi sia, sia titolare del trattamento, che soggetto terzo ecc.), è possibile identificare l'interessato[292]. Questo dato diviene anonimo quando questo stesso

[288] Parere 05/2014 sulle tecniche di anonimizzazione, pag. 7.

[289] GDPR.

[290] Famoso il caso dell'identificazione del Governatore del Massachussetts partendo da poche informazioni non personali: Sweeney L., *Simple Demographics Often Identify People Uniquely*, Carnegie Mellon University, Data Privacy Working Paper numero 3. Pittsburgh, 2000, pag. 2. Disponibile online al seguente link:
https://dataprivacylab.org/projects/identifiability/paper1.pdf

[291] Parere 05/2014 sulle tecniche di anonimizzazione, pag. 9.

[292] Commento di De Franceschi A., 2021, pag. 159.

soggetto che controlla i dati (chiunque questi sia, sia titolare del trattamento, che soggetto terzo ecc.) elimina gli elementi identificativi in modo tale da non essere più in grado (né lui né gli altri soggetti) di identificare l'interessato attraverso mezzi ragionevolmente utilizzabili (né da lui né dagli altri soggetti nel possesso dei dati). In questi casi si parlerà di identificazione ragionevolmente impossibile e dunque di dati anonimi (dati personali anonimizzati). Per capire se il processo di anonimizzazione è stato effettuato in maniera corretta si richiede che «...i responsabili del trattamento debbano concentrarsi sui mezzi concreti necessari per invertire il processo di anonimizzazione, in particolare per quanto riguarda i costi e le competenze necessarie a mettere in atto tali sistemi e la valutazione della loro probabilità e gravità»[293].

Proseguendo, fin qui si è detto che affinché un dato personale diventi anonimo è necessario che vengano espunti gli elementi che permettono l'identificazione, eppure

> «In generale, eliminare elementi direttamente identificanti non è pertanto di per sé sufficiente a garantire che l'identificazione della persona interessata non sia più possibile. Spesso è necessario adottare misure supplementari per prevenire l'identificazione, ancora una volta a seconda del contesto e degli scopi del trattamento cui sono destinati i dati resi anonimi»[294].

Ciò si ricollega all'assunto secondo cui ogni tecnica di anonimizzazione presenta un rischio residuo di identificabilità.

Le famiglie di tecniche di anonimizzazione sono due, randomizzazione e generalizzazione dei dati[295]. Sebbene entrambe presentino deficit, «ognuna di esse può rivelarsi adeguata, in circostanze e contesti specifici, per conseguire lo scopo desiderato senza compromettere la sfera privata delle persone interessate»[296]. Il rischio dell'identificazione, secondo il Gruppo di lavoro, è solo uno tra altri; nella specie si ha anche il rischio della correlabilità, intesa come la possibilità di associare almeno due dati relativi agli stessi interessati (nella stessa banca dati o in due banche dati diverse). Se per esempio qualcuno riesce ad accedere alla banca dati e a determinare che un determinato gruppo di persone è associato a determinati dati, anche se non sarà in grado di identificare i singoli interessati del gruppo, sarà comunque in grado di determinare delle correlazioni. La tecnica di anonimizzazione proteggerà dunque dall'individuazione ma non dalla correlabilità[297].

---

[293] Parere 05/2014 sulle tecniche di anonimizzazione, pag. 9.

[294] Ibidem, pag. 10.

[295] D'Acquisto G., Naldi M., *Big data e privacy by design: anonimizzazione pseudonimizzazione sicurezza*, 2017, pag. 35.

[296] Parere 05/2014 sulle tecniche di anonimizzazione, pag. 10.

[297] Ibidem, pag. 12.

In quanto alla deduzione invece si intende: «la possibilità di desumere, con un alto grado di probabilità, il valore di un attributo dai valori di un insieme di altri attributi»[298]. Sempre secondo il Gruppo di lavoro «una soluzione che elimini i tre rischi suddetti sarebbe utile per impedire la reidentificazione effettuata mediante i mezzi più probabili e ragionevoli che potrebbero essere utilizzati dal responsabile del trattamento e da altri»[299], anche se nel documento, dopo l'analisi di alcune tecniche di anonimizzazione, si conclude che nessuna di quelle è in grado di eliminare i tre rischi di cui sopra. A quel punto si enunciano quelle che lo stesso Gruppo di lavoro definisce buone pratiche di anonimizzazione. Innanzitutto, ammonisce dall'affidarsi all'approccio «pubblica e dimentica». Sul rischio residuo si afferma invece che sarà necessaria una periodica valutazione di modo da non lasciarsi scappare nuove minacce. Così come andranno valutati i controlli effettuati e in caso adeguarli. E una volta individuati i rischi, monitorarli.

Per quanto concerne set di dati anonimi uniti a set di dati personali non anonimi, si raccomanda di tenere in considerazione il potenziale di identificazione residuo[300]. Ciò che emerge è che l'anonimizzazione non va considerata come un'operazione immobile, e che si raccomanda ai soggetti preposti una valutazione periodica dell'anonimia dei dati. Il tutto va operato attraverso i criteri di ragionevolezza di cui sopra. I fattori che vanno valutati variano tra i costi, le competenze necessarie, i tempi e le risorse richieste affinché si possa ragionevolmente attuare un'anonimizzazione. A loro volta, tali fattori, devono essere rapportati alla crescente disponibilità di tecnologie, a costi ridotti, utili all'identificazione nelle banche dati[301]. Il Gruppo inoltre rileva come vadano esaminati anche i c.d. «elementi contestuali», quali la natura dei dati originali, i meccanismi e le misure di sicurezza presenti, la quantità di dati in questione, eventuali trasferimenti a terzi ecc.[302].

La pseudonimizzazione invece è una misura tecnica[303] volta a tutelare i diritti dell'interessato. Questa viene spesso associata, e talvolta confusa, con l'anonimizzazione[304]. La definizione della pseudonimizzazione non era presente nella Direttiva madre e viene introdotta dal Regolamento con l'articolo 4, paragrafo 1, numero 5 del Regolamento, secondo cui si intende:

> «il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni

[298] Ibidem.

[299] Ibidem.

[300] Parere 05/2014 sulle tecniche di anonimizzazione, pag. 26.

[301] Ibidem, pag. 9.

[302] Parere 05/2014 sulle tecniche di anonimizzazione, pag. 26.

[303] Lo si evince dal disposto degli articoli 25, 32 e 89 del Regolamento.

[304] D'Acquisto G., Naldi M., *Big data e privacy by design: anonimizzazione pseudonimizzazione sicurezza*, 2017, pag. 37.

aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile»[305].

In altre parole, attraverso la pseudonimizzazione si sostituiscono gli identificativi che permettono l'identificazione dell'interessato con uno pseudonimo[306]. Quest'ultimo, senza ulteriori operazioni, non permette l'identificazione dell'interessato. Come detto poc'anzi, la pseudonimizzazione viene alle volte confusa con l'anonimizzazione: la differenza principale risiede nel fatto che il risultato di quest'ultima è il venir meno della classificazione come dato personale e quindi la disapplicazione della disciplina sulla protezione del dato[307]. Invece, secondo il già citato considerando 26 «i dati personali sottoposti a pseudonimizzazione, i quali potrebbero essere attribuiti a una persona fisica mediante l'utilizzo di ulteriori informazioni, dovrebbero essere considerati informazioni su una persona fisica identificabile», e ciò rende applicabile la regolamentazione in materia di protezione dei dati personali[308]. Vi sono dei casi in cui è possibile rinunciare all'identificazione della persona, ma non alla sua identificabilità: in questi casi si procederà attraverso la pseudonimizzazione che appunto permette ancora l'associazione con l'interessato mediante l'utilizzo di informazioni aggiuntive[309]. Il Gruppo di lavoro precisa che si tratta di una misura di sicurezza che riduce la collegabilità all'interessato[310].

La questione sulle informazioni aggiuntive è cardinale. Queste, sempre in possesso del titolare del trattamento, devono essere conservate separatamente rispetto al dato pseudonimizzato, e devono essere tutelate attraverso ulteriori misure tecniche e organizzative di protezione, di modo che attraverso esse non si possa collegare lo pseudonimo ai dati personali di partenza[311]. Queste informazioni ulteriori, utili ad identificare l'interessato,

[305] GDPR.

[306] Parere 05/2014 sulle tecniche di anonimizzazione, pag. 20.

[307] Sui differenti obblighi derivanti dal trattamento di un dato personale, di un dato personale pseudonimizzato e di un dato anonimizzato vedasi Hintze M., *Viewing the GDPR through a de-identification lens: a tool for compliance, clarification and consistency*, 2018, pag. 149.

[308] Ribadito anche nel parere 05/2014 a pag. 11 e nel parere 4/2007 pag. 18.

[309] Commento di De Franceschi A., 2021, pag. 162.

[310] Parere 05/2014 sulle tecniche di anonimizzazione, pag. 20.

[311] Del Federico C., Popoli A. R., *Le definizioni*, 2019, pag. 97; Bolognini L., Pelino E., *Codice della disciplina privacy*, 2019, pag. 40; Voigt P., Von Dem Bussche A., *The EU General Data Protection Regulation (GDPR)*, Springer, 11 Novembre 2017, pag. 15; Hu R., Yu B., *Big Data Analytics for_Cyber-Physical Systems*, Springer, Cham, 2020, pag. 10; Hintze M., *Viewing the GDPR through a de-identification lens: a tool for compliance, clarification and consistency*, 2018, pag. 146; Bolognini L., Bistolfi C., *Pseudonymization and impacts of Big (personal/anonymous) Data processing in the transition from the Directive 95/46/EC to the new EU General Data Protection Regulation*, Computer Law & Security Review, volume 33, questione 2, Aprile 2017, pag. 178.

vengono anche dette chiavi di reidentificazione o di decriptazione; sono fondamentali e sono conservate da chi è nel controllo dei dati, poiché in certi casi sarà necessario utilizzarle per risalire all'identità dell'interessato, ad esempio per garantire l'effettività dei diritti di quest'ultimo (vedi, *inter alia*, il diritto all'accesso).

L'utilizzo della misura tecnica in esame è fortemente incentivato dal Regolamento[312], e il motivo è espresso dal considerando 28, secondo cui **«**l'applicazione della pseudonimizzazione ai dati personali può ridurre i rischi per gli interessati e aiutare i titolari del trattamento e i responsabili del trattamento a rispettare i loro obblighi di protezione dei dati»[313]. Malgrado ciò, l'identificazione rimane pur sempre ancora possibile mediante l'aggiunta di informazioni ulteriori, ecco perché sempre secondo il considerando 28, «l'introduzione esplicita della «pseudonimizzazione» nel presente regolamento non è quindi intesa a precludere altre misure di protezione dei dati»[314]. In dottrina si è detto che la pseudonimizzazione «non scardina il concetto di dato personale, ma riconosce all'informazione pseudonimizzata, e quindi più sicura e protetta da possibili violazioni direttamente impattanti sull'individuo, un minore grado di rischio concreto per i diritti fondamentali, lasciando così maggiore margine di manovra ai titolari del trattamento nell'esecuzione di specifici trattamenti»[315].

Oltre alla pseudonimizzazione esistono altre misure di sicurezza utili ad aumentare il livello di protezione dei dati. Tra le tante si menziona la cifratura[316], alla quale il Regolamento si riferisce in più momenti. In particolare, l'articolo 25, rubricato «protezione dei dati fin dalla progettazione e protezione per impostazione predefinita», menziona la pseudonimizzazione come misura adeguata, di modo da «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

[312] Il considerando 29 afferma che «al fine di creare incentivi per l'applicazione della pseudonimizzazione nel trattamento dei dati personali, dovrebbero essere possibili misure di pseudonimizzazione con possibilità di analisi generale nell'ambito dello stesso titolare del trattamento, qualora il titolare del trattamento abbia adottato le misure tecniche e organizzative necessarie ad assicurare, per il trattamento in questione, l'attuazione del presente regolamento, e che le informazioni aggiuntive per l'attribuzione dei dati personali a un interessato specifico siano conservate separatamente. Il titolare del trattamento che effettua il trattamento dei dati personali dovrebbe indicare le persone autorizzate nell'ambito dello stesso titolare del trattamento».

[313] GDPR. Sul punto anche Voigt P., Von Dem Bussche A., *The EU General Data Protection Regulation (GDPR)*, 2017, pag. 15.

[314] GDPR.

[315] Bolognini L., Pelino E., Bistolfi C., *Il Regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, 2016, pag. 81. Nello stesso senso Voigt P., Von Dem Bussche A., *The EU General Data Protection Regulation (GDPR)*, 2017, pag. 15.

[316] Commento di De Franceschi A., 2021, pag. 162.

presente regolamento e tutelare i diritti degli interessati»[317]; la pseudonimizzazione è anche una misura tecnica utilizzabile per diminuire i rischi alla sicurezza dei dati *ex* articolo 32[318]. Come si vedrà più avanti, l'adozione di misure come la pseudonimizzazione o la cifratura, rileva ai fini della responsabilità da trattamento illecito *ex* articolo 82 del Regolamento.

2.5 L'utilizzo dei dati personali nell'*IoT*.

Nel paragrafo 1.3 dedicato ai profili applicativi dell'*IoT* si è visto come tali tecnologie creino una moltitudine di servizi parecchio utili per gli utenti, alle volte addirittura vitali. Questi dispositivi interconnessi funzionano propriamente quando possono processore una grande mole di dati (si ricordi quanto detto in precedenza sui *Big Data*), che possono essere di diverso tipo: metadati[319], dati personali, dati non personali, dati personali anonimizzati o altro.

In questo paragrafo si illustrerà la particolarità della raccolta dei dati personali in alcuni ambienti tipici dell'*IoT*, traendo spunto dagli esempi illustrati nel paragrafo 1.3.1. Ciò che rileva ai fini del presente lavoro è il trattamento del dato personale. Nel Regolamento ne sono presenti due tipi; dati personali particolari (appartenenti a categorie personali di dati) e dati personali comuni. I primi sono descritti al considerando 51 del GDPR, che li definisce come «dati personali che, per loro natura, sono particolarmente sensibili sotto il profilo dei diritti e delle libertà fondamentali, dal momento che il contesto del loro trattamento potrebbe creare rischi significativi per i diritti e le libertà fondamentali.»[320].

L'articolo 9 esemplifica questi dati stabilendo il divieto di trattare (salvo non si soddisfino i requisiti previsti dalla stessa norma) quelli che «rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona»[321].

Tornando alla raccolta dei dati personali si rammenti come questa, nel mondo dell'*IoT*, possa avvenire da un singolo dispositivo come da un intero ambiente interconnesso. Va anche ricordato quanto detto nel paragrafo 1.2

[317] Sulle differenze tra il testo dell'articolo 25 proposto dalla Commissione e quello approvato da Parlamento e Consiglio in merito alla pseudonimizzazione, vedasi Bincoletto G., *La privacy by design*, Aracne editrice, Giugno 2019, pag. 136.

[318] Bolognini L., Pelino E., *Codice della disciplina privacy*, 2019, pag. 206.

[319] *Ex multis*, Ziccardi G., Perri P. (a cura di), *Dizionario Legal tech*, Milano, 2020, pag.627. Li definisce come «dati su dati, ossia dati che, in qualche modo, si riferiscono ad altre informazioni e che descrivono altri insiemi di dati…».

[320] GDPR.

[321] GDPR.

in merito alle definizioni: il ruolo della macchina è importante tanto quello umano. Alle volte, infatti, i nodi tipici dell'*Internet of Things*, raccolgono dati personali senza che gli interessati se ne accorgano[322], in quanto possono accumulare con discrezione dati relativi al comportamento online, spesso in ambienti privati, con l'obiettivo di anticipare le esigenze degli interessati o offrire loro risposte repentine (complice l'ausilio di tecniche di *machine learning* e intelligenza artificiale) [323]. Inoltre, rilevare la presenza di sistemi *IoT* non è affatto agevole, in quanto questi sono progettati per agire in modo autonomo e passivo[324].

Nel presente paragrafo si illustreranno degli esempi per evidenziare come questi dati entrino nel mondo dell'*Internet of Things*. Gli esempi come già detto saranno relativi agli ambiti *IoT* illustrati nel paragrafo 1.3.1, con alla base la consapevolezza che all'interno dello stesso settore, ad esempio quello delle *smart car*, possono riscontrarsi diversi tipi di ambienti *IoT* a seconda della progettazione dei dispositivi. Questi ambienti, infatti, non sono altro che il frutto della interconnessione tra i diversi *softwares* utilizzati dai singoli dispositivi: una casa automobilistica potrebbe optare per determinati sistemi di comunicazione *wireless* (ad esempio V2R), diversi da quelli applicati da un altro marchio (V2P), pur restando comunque nel settore delle auto intelligenti [325].

Iniziando dagli esempi forniti in precedenza sui sistemi di gestione del traffico (considerato da chi scrive come una sottocategoria della *smart mobility*) nel paragrafo 1.3.1, il sistema Mobywit si serve principalmente dei segnali *bluetooth* e *wi-fi* emessi dai dispositivi portatili (principalmente *smartphones* e *tablets*), senza che vi sia un *input* umano; ciò che il sistema registra è il c.d. *MAC* (*media access control*), ossia «un identificatore univoco attribuito a un'interfaccia di rete e solitamente registrato in un *hardware*, come chip di memoria e/o schede di rete in computer, telefoni, laptop o punti di accesso»[326], in altre parole costituisce l'identificativo della scheda di

---

[322] Conti M., Dehghantanha A., Franke F., Watson S., *Internet of Things security and forensics: Challenges and opportunities*, Future Generation Computer Systems volume 78, Parte 2, Gennaio 2018, pag. 545, disponibile online al seguente link: https://www.sciencedirect.com/science/article/abs/pii/S0167739X17316667

[323] Wachter S., *Data Protection in the Age of Big Data*, Nature Electronics, volume 2, 19 Gennaio 2019, disponibile online al seguente link:

https://ssrn.com/abstract=3355444

[324] Conti M., Dehghantanha A., Franke F., Watson S., *Internet of Things security and forensics: Challenges and opportunities*, 2018, pag. 544.

[325] Dahal K., Giri D., Neogy S., Dutta S., Kumar S. (edito da), *Internet of Things and Its Applications*, Springer, 2020, pag. 56.

[326]Parere 13/2011 sui servizi di geolocalizzazione su dispositivi mobili intelligenti. Disponibile online al seguente link:

https://www.garanteprivacy.it/documents/10160/2181517/WP185

Secondo l'Autorità garante per la protezione dei dati personali (provvedimento n. 303 del 13 luglio 2016) «il MAC Address è costituito da una sequenza numerica (48 cifre binarie) associata in modo univoco dal produttore a ogni scheda di rete ethernet o wireless prodotta al mondo e rappresenta l´indirizzo fisico identificativo di quel particolare dispositivo di rete da cui è possibile desumere l´identità del produttore, la tipologia di

rete del dispositivo che ha emesso il segnale *wi-fi* o *bluetooth*. Come si spiegherà a breve il *MAC* costituisce dato personale ai sensi dell'articolo 4 del Regolamento, ed oltre a questo vengono rilevati e registrati anche la posizione e il momento in cui si è captato il segnale.
Il sistema Mobywit «*detect that a specific MAC is in a place, and later, it can recognize the same MAC at another place, as the device moves. Being the MAC unique, the system is able to detect that a device moves from a place to another*»[327]. L'indirizzo *MAC*, oltre ad essere unico è anche immodificabile.

Poc'anzi si è detto che il sistema Mobywit raccoglie il *MAC* senza che sia necessario un *input* umano: ciò è vero ma merita un chiarimento. Quando su un dispositivo (ad esempio *smartphone* o *tablet*) si attiva la funzione *wi-fi*, lo stesso invia delle richieste (c.d. richieste sonda) ai punti di accesso *wi-fi*, e lo fa per tutto il tempo che rimane attivo. Queste richieste, nel momento in cui incontrano il punto di accesso *wi-fi*, gli comunicano il *MAC* del dispositivo, e riportano al proprietario la risposta del punto di accesso *wi-fi* (ad esempio l'utente riceverà il nome della rete, il suo *MAC*, se questa è privata o pubblica, la qualità del segnale ecc.). Un esempio: Tizio ha attivato il *wi-fi* del suo *smartphone*, dunque, per tutto il tempo in cui questo rimarrà attivo verranno inviate delle richieste sonda nell'etere per cercare punti di accesso *wi-fi*. Quando queste ne troveranno uno gli comunicheranno il *MAC* di Tizio, e quest'ultimo otterrà in cambio le informazioni suddette sul punto di accesso *wi-fi* e la possibilità di connettersi.

L'assenza di *input* umano risiede nel fatto che in pochissimi sono consci di inviare il *MAC* (dato personale) a soggetti terzi fornitori di un servizio di accesso alla rete, e anche qualora lo fossero non sono rari i casi in cui il *wi-fi* viene dimenticato attivo, e quindi continua a comunicare il *MAC* a soggetti terzi senza una volontà attuale e specifica dell'interessato. Una volta che il punto di accesso *wi-fi* riceve il *MAC* del dispositivo che chiede l'accesso alla rete, memorizza e analizza le informazioni che il *MAC* porta con sé: ossia i punti di accesso *wi-fi* a cui Tizio ha acceduto in passato.

Il fatto che il *media access control* costituisca dato personale lo si desume dal disposto del considerando 30 del Regolamento, secondo cui:

---

dispositivo e, in taluni casi, anche risalire all´acquirente o utilizzatore dell´apparato…Per tutto ciò il suo trattamento impone il rispetto della normativa sulla protezione dei dati personali». Disponibile online al seguente link:

https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/5408460

[327] Fernández-Ares A., Mora A. M., Arenas M. G., García-Sanchez P., Romero G., Rivas V., Castillo P. A., Merelo J. J., *Studying real traffic and mobility scenarios for a Smart City using a new monitoring and tracking system*, Future Generation Computer Systems, volume 76, Novembre 2017, pag. 163. Disponibile online al seguente link:

https://www.sciencedirect.com/science/article/pii/S0167739X16306604?via%3Dihub

«Le persone fisiche possono essere associate a identificativi online prodotti dai dispositivi, dalle applicazioni, dagli strumenti e dai protocolli utilizzati, quali gli indirizzi IP, marcatori temporanei (cookies) o identificativi di altro tipo, quali i tag di identificazione a radiofrequenza. Tali identificativi possono lasciare tracce che, in particolare se combinate con identificativi univoci e altre informazioni ricevute dai server, possono essere utilizzate per creare profili delle persone fisiche e identificarle»[328].

Il *MAC* come già detto è un identificatore univoco di un dispositivo dotato di capacità di accesso alla rete. Quando il dispositivo in questione è personale, quindi legato strettamente al suo proprietario (primariamente si pensi ad uno *smartphone*), il *MAC* sarà legato in maniera univoca non solo al dispositivo ma anche al proprietario dello stesso, ecco perché ad oggi viene considerato un dato personale[329].

Nel caso di specie «*the MAC is encrypted using a one-direction process before storing it*»[330]: il Regolamento, ai sensi dell'articolo 32, considera la cifratura una misura di sicurezza al pari della pseudonimizzazione, non

[328] GDPR.

[329] Sulla qualifica di dato personale del MAC si è espresso il Gruppo di lavoro nell'opinione 13/2011 sui servizi di geolocalizzazione su dispositivi mobili intelligenti, secondo cui «un dispositivo mobile intelligente è intimamente connesso a un individuo specifico. La maggior parte delle persone tende a tenere i propri dispositivi mobili molto vicini, dalle tasche o dalla borsa al comodino, vicino al letto. Succede raramente che una persona presti questi oggetti ad un'altra. Per la maggior parte, le persone sono consapevoli del fatto che i loro dispositivi mobili contengono una certa quantità di informazioni molto personali, che vanno da messaggi e-mail a fotografie private, dalla storia di navigazione del browser a, ad esempio, una lista di contatti. Questo consente ai fornitori di servizi basati sulla geolocalizzazione di ottenere una panoramica approfondita di abitudini e modelli di comportamento del proprietario del dispositivo e di costruire profili dettagliati. Da un modello di inattività notturna è possibile dedurre il luogo preposto al sonno, e dal modello di un percorso regolare la mattina è possibile dedurre l'ubicazione del datore di lavoro. Il modello può includere anche dati ricavati dai modelli di spostamento di amici, sulla base del cosiddetto grafico sociale. Un modello comportamentale può anche comprendere speciali categorie di dati, ad esempio se rivela visite in ospedali o luoghi di culto, la partecipazione a manifestazioni politiche o la presenza in altri luoghi specifici, magari che rivelino dati sulla vita sessuale dell'utente. Questi profili si possono utilizzare per prendere decisioni che influiscono in misura significativa sul proprietario». Nella stessa direzione si è espresso il Garante italiano nel provvedimento n. 428 del 19 luglio 2018, ove si afferma che attraverso il MAC «è possibile desumere l´identità del produttore, la tipologia di dispositivo e, in taluni casi, anche risalire all´acquirente o utilizzatore dell´apparato: è infatti sostanzialmente immodificabile e, date le caratteristiche (in particolare, la sua univocità su scala globale), consente di risalire, anche indirettamente, alla postazione corrispondente e di conseguenza all´utente che su di essa sta operando. Per tutto ciò il suo trattamento impone il rispetto della normativa sulla protezione dei dati personali».

[330] Fernández-Ares A., Mora A. M., Arenas M. G., García-Sanchez P., Romero G., Rivas V.Castillo P. A., Merelo J. J., *Studying real traffic and mobility scenarios for a Smart City using a new monitoring and tracking system*, 2017, pag. 164, Disponibile online al seguente link:
https://www.sciencedirect.com/science/article/pii/S0167739X16306604?via%3Dihub

sufficiente dunque ad anonimizzare il dato ed escluderlo dall'ambito applicativo del GDPR. Nell'esempio del sistema Mobywit il dato personale estratto è il *MAC*, ma in altri sistemi di monitoraggio del traffico i dati personali potrebbero essere diversi, quali ad esempio la targa del veicolo.

Per quanto concerne i punti di accesso *wi-fi* pubblici (*hotspot*), il discorso può dirsi sostanzialmente analogo. Chiunque si trovasse a passeggiare lungo la strada e dovesse avere il *wi-fi* attivo (volontariamente o meno), invierebbe il proprio codice *MAC* ai fornitori di servizi di accesso *wi-fi*, con tutte le informazioni che da questo possono essere ricavate, in primis la posizione.

Si è scelto di portare questo esempio di raccolta di dati personali in quanto, secondo chi scrive, si nota chiaramente la capacità delle macchine di operare all'insaputa degli individui, creando così un ambiente "sommerso" di raccolta di dati.

Proseguendo, nell'ambito della sorveglianza intelligente, la quantità di informazioni rilevabili è enorme. Come già detto la sorveglianza nelle città viene effettuata anche attraverso la tecnologia, *in primis* per via di videocamere. Per fornire una panoramica di che tipo di dati vengono acquisiti dalle telecamere si riprenda l'esempio relativo alla polizia gallese (caso *R. (Bridges)* contro *Chief Constable Of South Wales Police & Information Commissioner*)[331] illustrato al paragrafo 1.3.1[332]. Come già detto, in questo caso, sulle vetture della polizia erano state installate delle telecamere con un sistema di riconoscimento facciale automatico; per riprendere le parole utilizzate nella relativa sentenza: «*once a CCTV camera used in a live context captures footage, the software (a) detects human faces and then (b) isolates individual faces"*»*;* in un secondo momento «*taking the faces identified and isolated through "face detection", the software automatically extracts unique facial features from the image of each face, the resulting biometric template being unique to that image*»[333].

Ciò che le telecamere rilevano sono dunque i dati biometrici, definiti dall'articolo 4 del Regolamento come «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»[334].

Nel caso di specie il rilevamento di dati biometrici è inteso ad identificare in modo univoco, attraverso un sistema di intelligenza artificiale applicato nell'*edge*, determinate persone fisiche e ciò fa sì che si integri la fattispecie descritta dall'articolo 9 del Regolamento relativo al trattamento di particolari categorie di dati. Il Garante europeo, nelle linee guida

[331] R. (Bridges) contro Chief Constable Of South Wales Police & Information Commissioner. Disponibile online al seguente link: https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf

[332] Al caso si applicava il Data Protection Act 2018, ossia la legge d'attuazione del GDPR vigente in Galles.

[333] Ibidem.

[334] GDPR.

3/2019[335] sul trattamento dei dati personali attraverso dispositivi video, ha chiarito che affinché si possa parlare di dati biometrici come categoria particolare di dati personali *ex* articolo 9 del Regolamento sono necessarie tre condizioni: la prima attinente alla natura dei dati raccolti, che devono essere relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica; la seconda richiede che questi dati siano ottenuti da un trattamento tecnico specifico; infine è necessario che i dati siano utilizzati al fine di identificare in modo univoco una persona fisica.
Si precisa che il dato biometrico non è l'immagine del volto, ma l'informazione che se ne trae a seguito di uno specifico trattamento volto ad individuare una persona fisica. In altre parole, non si parla di dati biometrici se vengono raccolti immagini del viso ma poi non si tenta di identificare i relativi l'individui: è necessario un trattamento specifico volti ad individuarli.

Nel caso di specie l'individuazione (il *single out*) era possibile in quanto il sistema di riconoscimento facciale automatico era connesso ad un *database* della polizia in cui erano inseriti i volti delle persone da identificare (persone scomparse, sospettati, fuggitivi ecc.). Una volta raccolti i dati biometrici delle persone che entravano nello spettro visivo delle telecamere, il sistema operava in maniera autonoma un confronto tra i volti acquisiti per strada e quelli presenti nel *database*, ed in caso di *match* segnalava all'ufficiale di polizia preposto i risultati della corrispondenza (espressi in percentuale). Solo in caso di corrispondenza rilevante interveniva l'uomo, che a quel punto decideva cosa fare. Più in particolare, i dati biometrici dei volti che (a seguito dell'operazione di *matching*) non presentavano una corrispondenza rilevante, venivano immediatamente eliminati senza che il personale di polizia potesse in alcun modo intervenire (l'elaborazione e l'eliminazione avveniva in meno di un secondo); qualora invece la corrispondenza fosse maggiormente importante il sistema riportava i dati all'ufficiale di polizia. In entrambi i casi si ha un trattamento di dati personali (dati biometrici), ma solo nell'ultimo caso (corrispondenza rilevante per la macchina) vi è un ruolo dell'uomo, che viene dopo due decisioni della macchina (la prima di non corrispondenza con i volti registrati nel database della polizia e la seconda di eliminazione dei dati). Si nota quindi un ruolo non marginale della macchina nel processo decisionale.
Le normali telecamere di sorveglianza non sarebbero certo in grado di compiere operazioni del genere. In queste, infatti, il ruolo dell'uomo è preponderante: questo sceglie quando visionare i filmati (non è la macchina a notificarglielo) e compie in modo autonomo l'operazione di identificazione degli individui filmati decretando la corrispondenza o meno con i soggetti cercati. Infine, decide sull'eventuale eliminazione dei dati raccolti.

Questo esempio è stato scelto in quanto aiuta a comprendere come le tecnologie di cui si serve l'*IoT* (in questo caso l'*edge computing*), comportino

[335] Garante europeo, linee guida 3/2019, disponibili online al seguente link: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_it.pdf

una pervasività maggiore rispetto a quelle normalmente applicate ai generici dispositivi, ed interferiscano in modo più importante nelle decisioni dell'uomo.

Abbandonando l'ambito della sorveglianza intelligente, nel paragrafo 1.3.1 si è scelto di evidenziare alcuni dei campi di applicazione delle tecnologie *IoT* considerando i vari ambienti in maniera isolata (*smart cars, smart health, smart home* ecc.). Con l'esempio che si prospetta di seguito invece si intende proporre un intero ambiente interconnesso in cui è possibile rinvenire diversi ambiti tra quelli prospettati, nella specie *smart home* e *smart health*. Il caso d'uso è quello del progetto "Sphere", portato avanti nella città di Bristol (EN), ad opera dell'università della città.

In circa 100 abitazioni infatti sono stati applicati sensori di diverso tipo, con il seguente obiettivo:

> «*to impact a range of healthcare needs by employing data-fusion and pattern-recognition from a common platform of sensors in the home. Since its inception the project has been working with end users and the public to develop a multi-sensor fusion approach to sensing of health-related behaviours such as sleep, physical activity, eating, domestic chores and social contact. The project has developed custom worn and non-worn sensors, video sensors, low power connectivity solutions and machine learning to reason from these data streams*»[336].

I sensori sono dunque posti nelle case delle persone che hanno aderito all'esperimento, con l'obiettivo di trarre informazioni utili a monitorare lo stato di salute delle stesse. Per quanto concerne il tipo di *smart objects*, sono stati utilizzati tre tipi di sensori: di rilevamento ambientale, indossabili e di monitoraggio video. Relativamente ai primi, quando analizzati unitamente ai dati generati dai dispositivi indossabili, permettono di determinare la posizione degli interessati all'interno della casa (e anche quella di animali domestici o di ospiti). Sono anche in grado di rilevare dati afferenti il suono, o il consumo di energia elettrica (qualora applicati agli elettrodomestici come Tv o forni a microonde)[337].

Per quanto concerne invece i sensori indossabili, sono progettati per trasmettere di continuo i dati attraverso una rete di *gateways* di SPHERE posti nelle loro abitazioni. I dati vengono raccolti attraverso un accelerometro triassiale, che permette di localizzare l'interessato (attraverso la misurazione del segnale generato grazie ai *gateways* di SPHERE) all'interno dell'abitazione. Le tecniche utilizzate per misurare la posizione sono basate su algoritmi di *machine learning* e forniscono informazioni relative alla mobilità, tracciando ad esempio quante volte un

[336] Pagina ufficiale dell'università di Bristol. Disponibile online al seguente link: https://www.bristol.ac.uk/engineering/research/digital-health/research/sphere/.

[337] Pagina ufficiale dell'università di Bristol dedicata ai sensori ambientali. Disponibile online al seguente link: https://www.bristol.ac.uk/engineering/research/digital-health/research/sphere/ambient-sensing/

paziente si alza, si siede, cambia stanza ecc., all'alimentazione, in base agli orari e al tempo in cui si rimane in cucina, al sonno, in virtù degli orari in cui si è fermi in camera da letto ecc.[338]. In merito ai sensori video invece si legge che l'analisi automatica dei dati forniti dalle videocamere permette di realizzare dei profili metrici molto precisi, relativi ad azioni quotidiane come sedersi, alzarsi in piedi o salire le scale. Questi dati, prima di essere analizzati, vengono anonimizzati nella stessa abitazione, e solo in un secondo momento, dopo aver eliminato lo sfondo e dopo aver sostituito la persona con una *silhouette*, sono inviati ai *server* SPHERE. È spiegato come gli algoritmi di visione computerizzata siano capaci di riconoscere posizioni come quelle da seduto e da alzato, e anche di cronometrare l'intervallo utile per passare da una posizione all'altra; il risultato viene analizzato allo scopo di rilevare lo stato generale delle condizioni di salute. Ad esempio, per un paziente che sta recuperando le sue capacità motorie, l'intervallo di transizione da una posizione all'altra, misurato di giorno in giorno, potrà disvelare l'effettivo andamento del recupero[339]. Per comprendere meglio il funzionamento dei sensori di monitoraggio video si consiglia la visione del filmato proposto dalla stessa università[340]. Questi sensori sono inoltre «*accompanied by a number of devices required for (i) data storage, (ii) network connectivity among sensors, and (iii) system management and monitoring*»[341]. Come evidenziato, i dati raccolti da questi sensori sono moltissimi e diversissimi, non resta che capire quali siano classificabili come dati personali e quali no. Nel caso di specie l'identificazione da parte di chi raccoglie i dati (l'università di Bristol) è cosa data, in quanto gli abitanti delle abitazioni hanno prestato esplicitamente il proprio consenso alla raccolta dei dati.

In virtù di ciò tutte le informazioni-contenuto riferibili a queste persone fisiche sono da considerarsi dati personali[342]. La scelta dei sensori disposti nelle abitazioni, come già detto, è orientata all'esame dello stato di salute dei soggetti esaminati. Il metodo è particolare: l'università ha definito una serie di comportamenti 'normali' per soggetti sani, e si è concentrata su tutti quei comportamenti, quei movimenti, quelle abitudini rilevate

[338] Pagina ufficiale dell'università di Bristol dedicata ai sensori indossabili. Disponibile online al seguente link:
https://www.bristol.ac.uk/engineering/research/digital-health/research/sphere/wearable-solutions/

[339] Pagina ufficiale dell'università di Bristol dedicata ai sensori video. Disponibile online al seguente link:
https://www.bristol.ac.uk/engineering/research/digital-health/research/sphere/video/

[340] Video disponibile online al seguente link:
https://www.youtube.com/watch?v=OmaOBr0gmJ4&feature=emb_imp_woyt

[341] Angelakis V, Tragos E., Pöhls H. C., Kapovits A., Bassi A., *Designing, Developing, and Facilitating Smart Cities*, Springer, 2017, pag. 321. Disponibile online al seguente link:
https://link.springer.com/book/10.1007/978-3-319-44924-1

[342] Bolognini L., Pelino E., Bistolfi C., *Il Regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, 2016, pag. 55.

attraverso i sensori, che si discostano dal modello di sanità-normalità da essa predisposto. Per meglio comprendere si riporta quanto espresso dai ricercatori dell'università di Bristol per quanto concerne le informazioni ottenibili dai sensori indossabili:

> «*We now describe how to obtain the inference over certain activities using the acceleration signal from the wearable device. To train the classifier, we collect a set of annotated datasets via performing scripted experiments in different homes. These scripted experiments are designed as follows. We ask the participant to simulate their daily life (e.g. wake from bed, go to the kitchen, stay in the living room, back to the bedroom) whilst wearing a head-mounted camera. The whole process normally takes from 5 to 10 min, after which the recorded videos are annotated with five ambulation and postures: lay down, sit, stair, stand, walk*»[343].

In altre parole, si ottiene una metrica delle attività quotidiane degli abitanti delle case. Da questa si desume il movimento statisticamente normale di quel paziente per quelle determinate pose (sedersi, alzarsi, sdraiarsi, fare le scale, camminare). Una volta ottenuto tale modello, vengono analizzati tutti i movimenti che si distaccano da esso, in quanto anormali[344]. Vista la precisa scelta dell'università di raccogliere questo tipo di dati è ragionevole desumere che da queste sia in grado di trarre delle informazioni relative alla salute, utili e pertinenti rispetto al fine che si è preposta[345]. Inoltre, sempre gli stessi ricercatori scrivono che: «*SPHERE system information are a useful adjunct to descriptive information provided by the PROMs in characterising recovery on an individual basis*»[346]. Le informazioni ottenute attraverso i sensori vengono dunque confrontate con altre derivante dai pazienti stessi (*PROMs* sta per *Patient Reported Outcome Measures*), e come già riportato nel paragrafo 2.3. «ogni successiva informazione-contenuto collegata con un'informazione-identificativo diventa a sua volta dato personale e arricchisce perciò di elementi

[343] Holmes, M., Nieto, M.P., Song, *Modelling Patient Behaviour Using IoT Sensor Data: a Case Study to Evaluate Techniques for Modelling Domestic Behaviour in Recovery from Total Hip Replacement Surgery*, Journal of Healthcare Informatics Research, volume 4, 2020, pag. 245.

https://link.springer.com/article/10.1007/s41666-020-00072-6.

[344] Angelakis V., Tragos E., Pöhls H. C., Kapovits A., Bassi A., *Designing, Developing, and Facilitating Smart Cities*, 2017, pag. 321.

[345] Ibidem. Del resto nell'*abstract* si legge: «*We find that accelerometer and indoor localisation data correctly highlight long-term trends in sleep and movement quality and can be used to predict sleep and wake times and measure sleep and wake routine variance over time, whilst indoor localisation provides context for the domestic routine and mobility of the patient*», pag 238.

[346] Holmes, M., Nieto, M.P., Song, H. et al., *Modelling Patient Behaviour Using IoT Sensor Data: a Case Study to Evaluate Techniques for Modelling Domestic Behaviour in Recovery from Total Hip Replacement Surgery*, 2020, pag. 255.

conoscitivi il dato personale di partenza»[347]. E' quindi possibile concludere che i dati ottenuti attraverso i sensori siano dati personali, in quanto costituiscono informazioni riferite a persone fisiche individuate.

Ai sensi dell'articolo 4 del Regolamento «i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute»[348] sono definiti dati relativi alla salute (o più comunemente dati sanitari). Per comprendere meglio che tipo di informazioni si ottengano dai dati rilevati, si propone uno dei risultati evidenziati dall'università di Bristol:

> «*Movement data extracted from the wearable accelerometer (Fig. 7) shows a stark difference in movement behaviour between patients B (Fig. 7b) and C (Fig. 7c). Whilst the patient in home B shows a healthy pattern of movement and rest, similar to our control in home A (Fig. 7a), the patient in home C (Fig. 7c) shows very low levels of movement throughout the post-operative recovery period. Whilst the patient in home B increases their movement across the period, the patient in home C decreases their overall levels of movement. Accelerometer data may be used as a data source for actigraphy, a family of approaches used to support the study of sleep and circadian rhythms…the relative amplitude (RA) measure is reduced following the operation for both B and C, implying that the participant's circadian rhythm is disrupted*»[349].

Per concludere con il progetto SPHERE, gli stessi studiosi menzionano tecniche di *machine learning* utilizzate per l'addestramento dei modelli[350]. L'esempio di tale progetto è stato proposto in quanto chi scrive ritiene che possa mostrare adeguatamente quanto le applicazioni dell'*IoT* possano rappresentare interi ambienti interconnessi. Questi modelli un giorno saranno estremamente diffusi e secondo chi scrive si arriverà al giorno (non troppo lontano) in cui ci si sposterà tra ambienti interamente connessi ed interconnessi (ci si sveglia in una *smart home*, si prende *una smart car* per andare a prendere un amico nella sua *smart home* e si va a prendere un caffè in un bar in cui non sapevamo ci fosse un *hotspot* e così via). L'ultimo esempio proposto per mettere in evidenza il rapporto che intercorre tra *IoT* e dati personali è creato *ad hoc* da chi scrive.

Innanzitutto, si rammenti quanto detto nel paragrafo 1.3.1. sugli *smartphones*, che sono oggi i principali protagonisti delle architetture *IoT*. La loro interoperabilità li rende difatti collegabili a quasi qualsiasi infrastruttura

---

[347] Bolognini L., Pelino E., Bistolfi C., *Il Regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, 2016, pag. 55.

[348] GDPR.

[349] Holmes, M., Nieto, M.P., Song, H. et al., *Modelling Patient Behaviour Using IoT Sensor Data: a Case Study to Evaluate Techniques for Modelling Domestic Behaviour in Recovery from Total Hip Replacement Surgery*, 2020, pag. 249.

[350] Ibidem: «*With respect to the machine learning and artificial intelligence techniques, the next step is to further reduce the requirement on the amount of training data*», pag. 257.

digitale. A ciò si aggiunga che le odierne *smart cars* producono e inviano una quantità enorme di dati ai *cloud* della propria casa produttrice; questi dati vengono tendenzialmente suddivisi tra quelli relativi alla vettura (ad esempio stato della batteria, livello di carburante, chilometri totali effettuati ecc.) e quelli personali, dunque riferibili al conducente o ad altre persone fisiche identificabili.

L'esempio che si propone è a prima vista molto semplice: quattro amici sono diretti a Piacenza in auto. Andando più nel dettaglio si intende mostrare come una situazione all'apparenza così semplice possa essere estremamente sfaccettata. L'auto dell'esempio è una *smart car* prodotta da Mercedes-Benz, dotata di sistema MBUX[351], con quattro passeggeri a bordo di cui uno diversamente abile, diretta a Piacenza. Attraverso la pagina ufficiale di Mercedes-Benz si apprende che grazie all'applicazione Mercedes Me (di cui si è detto nel paragrafo 1.3.1), dotata di Remote Package[352] (scaricabile dallo *smartphone*), è possibile tracciare la propria posizione e quella dell'auto.

Il gestore dell'applicazione raccoglie dunque i dati relativi all'ubicazione dello *smartphone* del proprietario dell'auto e dell'auto stessa. In più, richiedendo a chi scarica l'app di inserire il numero di telaio del veicolo (che costituisce un identificativo univoco dell'auto e quindi del proprietario della stessa[353]) o il QR code (considerato un punto di accesso a dati personali[354]), crea una relazione biunivoca tra l'individuo che ha scaricato l'applicazione e la vettura a cui questa è collegata.
Ai sensi dell'articolo 4 del Regolamento i dati relativi all'ubicazione della persona fisica possono essere classificati come dati personali. La particolarità di questo sistema di tracciamento risiede nel fatto che la geolocalizzazione della persona fisica sia frutto dell'interconnessione dei dati generati dallo *smartphone* dove è stata scaricata l'app Mercedes Me, e quelli della vettura. I dati così raccolti sono classificabili come dati personali

[351] Pagina ufficiale di Mercedes-Benz dedicata al sistema MBUX. Disponibile online al seguente link: https://www.mercedes-benz.it/passengercars/mercedes-benz-cars/local-landing/mbux/mbux-content.module.html

[352] Pagina ufficiale di Mercedes-Benz dedicata al Remote Package. Disponibile online al seguente link:
https://www.mercedes-benz.it/passengercars/being-an-owner/mercedes-me-connect.pi.html/being-an-owner/mercedes-me-connect/mercedes-me-recommendations/remote-package

[353] Cass. civ., Sez. I, 7 luglio 2021, n. 19270: «…correttamente è stato riconosciuto il carattere di dato personale al numero di telaio dell'autoveicolo, in quanto idoneo a far pervenire all'identificazione della persona del proprietario dello stesso». Disponibile online al seguente link:
https://sentenze.laleggepertutti.it/sentenza/cassazione-civile-n-19270-del-07-07-2021

[354] Il Garante non si è espresso chiaramente sulla natura del QR code, limitandosi a sottolineare la possibilità di accedere attraverso di esso ad una moltitudine di dati personali. A detta di chi scrive lo si potrebbe considerare un identificatore indiretto. L'intervento del Garante in questione è disponibile online al seguente link: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9673513

in seguito al presente ragionamento (essendo l'interessato identificato attraverso la registrazione all'app). Mercedes Me richiede la registrazione preventiva, in cui va inserito un identificativo (nome e cognome, reali o meno) e la mail; il connubio tra l'identificativo dell'utente e i dati relativi all'ubicazione prodotti sia dell'auto che dallo *smartphone* dell'utente, permette l'individuazione della persona fisica in questione.
Un esempio di scuola può aiutare: i dati relativi all'ubicazione dell'utente e della vettura dicono che il soggetto registratosi nell'app Mercedes Me con l'identificativo 'AX 1', tra le ore 00:00 e 08:30 non si muove mai da Via delle Cascate (solitamente tra i civici 2 e 30). Tra le 09:00 e le 18:00 dei giorni feriali lo si trova invece sempre fermo in un parcheggio di proprietà di alcuni uffici di Via Aldo Rossi 9; le domeniche mattina invece intorno alle 09:30 i dati ci dicono che 'AX 1' si muove e si dirige nei pressi di una chiesa cattolica. Attraverso questi dati è possibile identificare AX 1 poiché in Via delle Cascate tra i civici 2 e 30 vivono circa 100 persone, ma solo 8 di queste sono proprietarie di auto Mercedes-Benz; inoltre, solo due tra queste otto persone lavorano in Via Aldo Rossi 9 e soltanto una è di fede cattolica. Come già detto nel paragrafo 2.3, conoscere il nome reale di una persona fisica non è necessario: è sufficiente l'individuazione di questa in un gruppo più o meno esteso di persone, cosa fattibile nel caso di scuola prospettato.

Proseguendo nell'esempio, il conducente in questione è alla ricerca di un parcheggio adatto allo stato di salute del passeggero diversamente abile. Attraverso lo stesso *smartphone* in cui è stata scaricata l'app Mercedes Me, si potrà operare il download dell'applicazione Piacenza[355] (la quale richiede la registrazione tramite identificativo, mail e poi l'attivazione del servizio di geolocalizzazione dello *smartphone*) che, sfruttando i dati relativi all'ubicazione, indicherà all'utente il tragitto più veloce o meno trafficato per raggiungere il parcheggio per diversamente abili prescelto. L'applicazione riceverà i dati relativi all'ubicazione e l'identificativo per la registrazione, ma non solo: la richiesta di un parcheggio adatto a soggetti diversamente abili fornirà informazioni relative allo stato di salute. Questi dati però solo difficilmente possono essere classificati come dati sanitari, in quanto i gestori dell'app Piacenza dovrebbero poi individuare, *singling out*, a quale dei quattro passeggeri si riferisca l'esigenza del particolare parcheggio. Potrebbero facilmente dedurre che quei dati non si riferiscano al proprietario del veicolo in quanto dal suo storico degli spostamenti si rileva che questi non parcheggia mai in posti riservati ai diversamente abili, ma potrebbe essere irragionevole ritenere per loro possibile dedurre chi tra gli altri possibili passeggeri sia quello per cui è stato richiesto il parcheggio. Proseguendo nell'esempio: durante la navigazione verso Piacenza il conducente ha messo a disposizione il *wi-fi* della sua Mercedes-Benz. Molti modelli delle odierne *smart cars* sono infatti oggi dotati di una connessione autonoma alla rete Internet (nell'esempio in questione le auto dotate di

[355] Pagina ufficiale dell'app Piacenza. Disponibile online al seguente link: https://www.comune.piacenza.it/servizi/segnalazioni-e-comunicazioni/app-piacenza

sistema MBUX della suddetta casa produttrice hanno tale facoltà). L'attivazione della rete Internet dell'auto è possibile solo stipulando un contratto con il service provider di accesso alla rete, sempre attraverso l'app di Mercedes Me[356]. L'auto che trasporta i quattro amici a Piacenza è diventata così una piccola rete Internet alla quale i passeggeri possono connettersi.

Affinché si possa concludere il contratto di accesso alla rete (Mercedes-Benz si collega a Vodafone) sarà necessario sottoscrivere anche il trattamento di alcuni dati personali, quali mail e identificativo. Nel frattempo la medesima auto, come già detto, sta producendo una quantità enorme di dati (personali e non) e li sta inviando al *cloud* della sua casa produttrice. Questi dati, come evidenziato nel paragrafo 1.4.1, costituiscono oggi un enorme fonte di conoscenza e ricchezza; sono talmente appetibili che nell'ultimo decennio sono nate società che si occupano di acquistare tali dati, analizzarli e rivenderli. Una di queste è Otonomo[357], che avendo stipulato accordi con le principali case produttrici automobilistiche acquista pacchetti di dati[358], personali e non, li elabora e li rivende. Tra le case automobilistiche vi è anche Mercedes-Benz.

Ricapitolando, si ha un'auto che comunica con il suo *cloud* di riferimento inoltrandogli una grande mole di dati (personali e non). La stessa ha anche una connessione diretta con il fornitore di accesso alla rete[359] e grazie a ciò l'auto è diventata una piccola rete locale alla quale i passeggeri possono collegarsi. Essa è anche collegata allo *smartphone* del proprietario tramite l'applicazione Mercedes Me (attraverso l'identificativo del numero di telaio o QR code), alla quale invia moltissime informazioni, tra cui la posizione. Dall'altro lato, attraverso lo *smartphone*, per via dell'app Mercedes Mi, è possibile compiere una moltitudine di azioni da remoto (monitorare l'ubicazione della vettura, misurare la pressione degli pneumatici, attivare l'aria condizionata ecc.). La medesima app, inoltre, tratta i dati personali del conducente (id, mail e posizione) ricavandoli dalla procedura di registrazione e dallo *smartphone*. Quest'ultimo si connette

---

[356] Video dimostrativo relativo alla connessione ad Internet della vettura. Le informazioni visibili nel video non sono reperibili se non si possiede una Mercedes-Benz abbinabile all'app Mercedes Me, si è dunque fatto riferimento a tale filmato, disponibile online al seguente link:

https://www.youtube.com/watch?v=MHlnNLDpIJ4&t=54s

[357] Pagina ufficiale della società. Disponibile online al seguente link: https://otonomo.io/

[358] Per una panoramica sui dati raccolti (personali e non), elaborati e venduti da Otonomo per quanto concerne le vetture Mercedes-Benz si operi il download dal seguente link:

https://info.otonomo.io/thank-you-daimler-ds?submissionGuid=e57275a2-13b4-46ad-bbfb-b015a55abaf2

[359] Non è stato possibile conoscere quali dati vengono inviati in quanto il contratto tra il proprietario dell'auto e il fornitore del servizio di accesso alla rete è accessibile solo a chi abbia inserito il proprio numero di telaio o QR code nell'app Mercedes Me (impossibile per chi non possiede una vettura del genere).

all'applicazione Piacenza, a sua volta collegata con una moltitudine di sensori sparsi per la città emiliana. Infine, il *cloud* di cui si è detto inizialmente cede informazioni (anche personali) a soggetti terzi. Ciò che si è inteso dimostrare con questo esempio è come ad oggi (ma soprattutto in futuro sempre più frequentemente) una situazione semplice come un viaggio in auto possa essere il contenitore di un'intricata rete di connessioni con una moltitudine di protagonisti della quale si è più o meno consci. Lo *smartphone* è ad oggi lo *smart object* più importante in quanto può connettersi a quasi tutti i *softwares* in circolazione, e grazie ai *cloud* ai quali è collegato non soffre di capacità computazionale. Questo caso potrebbe essere inserito nell'ambito della *smart mobility* (per il parcheggio intelligente) o delle *smart cars* (per via delle molteplici connessioni che questa riesce ad instaurare).

Nel presente capitolo si è tentato di evidenziare il rapporto che intercorre tra l'*Internet of Things*, come descritto nel primo capitolo, e la protezione dei dati personali. Nel primo paragrafo si è operato un generico riferimento al rapporto intercorrente tra tecnologia e diritto. Nel paragrafo 2.1 invece si è messo in luce come le evoluzioni tecnologiche avutesi in particolare dagli anni sessanta in poi, abbiano fatto nascere l'ambito di studi oggi definito come protezione dei dati personali. Essendo i dati personali il fulcro della materia, nel paragrafo 2.3 si è tentato di definirli brevemente. Successivamente si è posta la questione dell'anonimizzazione e delle sue difficoltà, e la diversa misura della pseudonimizzazione. Infine, si è cercato di fornire degli esempi che evidenziassero le particolari relazioni tra l'*IoT* e i dati personali. I primi due capitoli costituiscono le premesse, fondamentali, per la prosecuzione della tesi; questi elementi verranno infatti messi in rapporto con il principio di *Accountability* (capitolo 3) e con l'*Internet of Things* (capitolo 5), cercando così di mostrare la complessità della realtà tecnologica e giuridica in cui circolano i dati personali.

Capitolo 3 – Il principio di *Accountability*

3.1 L'evoluzione del principio di *accountability* nella protezione dei dati personali

Il principio di *accountability* è uno dei più importanti principi del Regolamento[360]. Esso è esplicitamente previsto all'articolo 5, ma non nel primo paragrafo insieme agli altri principi (liceità, correttezza, trasparenza, limitazione delle finalità, minimizzazione, esattezza, limitazione della conservazione, integrità e riservatezza), bensì in un paragrafo apposito, il secondo, che recita: «il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»)». Secondo alcuni[361], ciò denota una diversa natura del principio in esame rispetto agli altri previsti dalla norma: in particolare, mentre i principi cristallizzati nel primo paragrafo sarebbero attinenti alla qualità del trattamento, il principio di *accountability* concernerebbe la ripartizione delle responsabilità relative al trattamento.

Inoltre, un'interpretazione di ordine sistematico ci impone di rilevare come il principio suddetto sia posto a chiusura degli altri principi: esso difatti impone il rispetto e la dimostrabilità di tutti gli altri. In tal senso è stato definito un meta principio[362]. Nel caso dell'*accountability* si parla spesso di novità[363], e ciò in quanto il principio in esame era sicuramente molto diffuso nei sistemi di *common law*, mentre non si può dire altrimenti per i sistemi di *civil law*. Nel parere numero 3 del 2010 del Gruppo di lavoro (ove si chiedeva alla Commissione di valutare l'opportunità di inserire legislativamente tale principio), si evidenzia come «il termine inglese «*accountability*» proviene dal mondo anglosassone, dove è di uso comune e dove il suo significato è

[360] Definito anche «principio dei principi» in Riccio G. M., Scorza G., Belisario E. (a cura di), *GDPR e normativa privacy*, 2018, pag. 241; o «principio cardine», in Amore G., *Fairness, Transparency e Accountability nella protezione dei dati personali*, Studium Iuris, volume 4, 2020, pag. 416.

[361] Commento di Malgieri C., in D'Orazio R., Finocchiaro G., Pollicino O., Resta G., *Codice della privacy e data protection*, 2021, pag. 189.

[362] Urquhart L., Chen J., *On the Principle of Accountability: Challenges for Smart Homes & Cybersecurity*, 2020, pag. 6. Disponibile online al seguente link: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3629119

[363] Bolognini L., Pelino E., *Codice della disciplina privacy*, 2019, pag. 201; Riccio G. M., Scorza G., Belisario E. (a cura di), *GDPR e normativa privacy*, 2018, pag. 237; Pizzetti F., *Privacy e il diritto europeo alla protezione dei dati personali. Il Regolamento europeo 2016/679*, 2016, pag.4.

ampiamente compreso e condiviso. Ciononostante, risulta complesso definire che cosa significhi «*accountability*» nella pratica»[364].

Come evidenziato in dottrina[365], il principio in analisi era ben conosciuto soprattutto nei contesti aziendali dei settori assicurativo e bancario, e non è apparso opportuno tentare di tradurlo, in quanto la lingua italiana non conosce termini che presi singolarmente possano descrivere il concetto di *accountability*. Si ritiene pertanto corretto continuare ad utilizzare il termine anglosassone, sebbene nella traduzione italiana del Regolamento esso sia stato tradotto con «principio di responsabilizzazione». Nonostante il Regolamento costituisca il primo atto vincolante a portata generale dell'UE (in materia di protezione dei dati personali) a prevedere esplicitamente tale principio, è possibile notare come fosse stato preso in forte considerazione già in passato.

Già nel 1980 infatti, l'Organizzazione per la cooperazione e lo sviluppo economico (Ocse), emanò le linee guida sulla protezione della privacy e sui flussi transfrontalieri di dati personali[366], ove fu cristallizzato per la prima volta il principio di *accountability* nella disciplina della protezione dei dati personali[367]. All'articolo 14, sotto la rubrica «*accountability principle*» si

[364] Parere 3/2010 del Gruppo di lavoro *ex* articolo 29 sul principio di responsabilità, pag.8. Nella stessa pagina si enunciano i diversi modi in cui in Europa era stato proposto di rendere il concetto di *accountability*. Disponibile online al seguente link:

https://www.garanteprivacy.it/documents/10160/10704/Articolo+29+-+WP173+-+Parere+3+2010+sul+principio+di+responsabilit%C3%A0.pdf/006f43b3-7180-4485-903e-bf8b4f367763?version=1.2

[365] Ricciuto V., *La patrimonializzazione dei dati personali*, in Cuffaro V., D'Orazio R., Ricciuto V., *I dati personali nel diritto europeo*, 2019, pag. 20: «a riassumere il sistema risultante da siffatte disposizioni, è diffuso il riferimento al principio di accountability ed alla compliance dei trattamenti. L'uso di termini mutuati dall'esperienza delle organizzazioni aziendali e societarie rende così avvertiti del mutamento di prospettiva che connota il più recente intervento normativo e consente di registrare la peculiare valenza che è venuta ora a segnare la regolamentazione di questo ormai non marginale ambito dell'attività giuridicamente rilevante. La normativa di ultima generazione, della quale il Regolamento 2016/679 costituisce il più recente ma non ultimo esempio, tende dunque a focalizzare l'attenzione sulla struttura dell'attività di trattamento dei dati, seguendo quasi inconsapevolmente il medesimo percorso che in altri settori di rilievo economico, quali quello bancario e assicurativo, ha portato ad irrobustire l'approntamento di regole di condotta cui devono attenersi gli operatori, il rispetto delle quali vale in qualche misura a conformare l'attività di trattamento dei dati. Nella medesima direzione, la disciplina europea sul trattamento dei dati personali si atteggia allora a disciplina del mercato dei dati, sollecitando a comportamenti virtuosi gli operatori del trattamento, incoraggiati a condotte coerenti con i principi di protezione in vista del conseguimento di una maggiore affidabilità agli occhi dei fornitori di dati, cioè, in definitiva, delle stesse persone i cui dati sono oggetto di trattamento».

[366] Disponibile online al seguente link:

https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

[367] Riccio G. M., Scorza G., Belisario E. (a cura di), *GDPR e normativa privacy*, 2018, pag. 239.

stabiliva infatti che «*a data controller should be accountable for complying with measures which give effect to the principles stated above*».

Nella sua prima accezione, dunque, il principio di *accountability* era inteso nel senso di «*responsibility for specific tasks and duties*»[368].

Tali linee guida sono state aggiornate nel 2013[369], ed il principio in esame è stato confermato nell'ambito della protezione dei dati personali a livello internazionale. In questo documento aggiornato però si richiede ai titolari del trattamento un «salto di qualità»[370]: li si indirizza difatti verso un'impostazione attiva, in una prospettiva non già più riparatoria ma preventiva; da qui, un principio di *accountability* inteso come dovere di conformità e dimostrabilità[371]. Il danno va prevenuto attraverso comportamenti tarati sul caso di specie, che devono poter essere dimostrati in caso di richiesta da parte delle autorità competenti o di altri enti responsabili della promozione all'aderenza ai codici di condotta.

Nell'anno seguente rispetto alla prima versione delle linee guida veniva approvata la Convenzione 108 del 1981. In questa, l'articolo 7, rubricato «sicurezza dei dati», prevedeva che «idonee misure di sicurezza vengono adottate per la protezione dei dati a carattere personale registrati nelle collezioni automatizzate contro la distruzione accidentale o non autorizzata, o la perdita accidentale, nonché contro l'accesso, la modificazione o la diffusione non autorizzati». Si notano delle diversità rispetto alle linee guida dell'anno precedente. Al di là della natura dell'atto, se l'Ocse aveva impostato la *quaestio* in termini di *accountability* intesa come responsabilità, i paesi firmatari della convenzione avevano preferito riportare l'obbligo di adottare misure utili alla salvaguardia dei dati personali nell'alveo della sicurezza dei dati. Come sottolineato in dottrina, ciò si deve in parte ai pericoli dell'elaborazione automatizzata che si manifestavano in quegli anni, i quali avevano spinto i paesi firmatari a concentrarsi sui profili di sicurezza, quali ad esempio l'accesso non autorizzato[372].

La Direttiva madre nel 1995 si pone in continuità con entrambe le norme appena esaminate. Le disposizioni di riferimento della Direttiva sono

---

[368] Docksey C., *Article 24. Responsability of the controller*, in Kuner C., Bygrave L. A., Docksey C., Drechsler L., *The EU General Data Protection Regulation (GDPR): A Commentary,* 2020, pag. 557.

[369] Versione del 2013 disponibile online al seguente link: https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf

[370] Riccio G. M., Scorza G., Belisario E. (a cura di), *GDPR e normativa privacy*, 2018, pag. 239.

[371] Docksey C., *Article 24. Responsability of the controller*, 2020, pag. 558: «*the updated OECD Privacy Guidelines from 2013 maintain the original Accountability Principle but add the new meaning of accountability, in the sense of proactive and demonstrable compliance…* ». Difatti l'articolo 15 del documento aggiornato prevede che il titolare del trattamento sia «*prepared to demonstrate its privacy management programme as appropriate, in particular at the request of a competent privacy enforcement authority or another entity responsible for promoting adherence to a code of conduct or similar arrangement giving binding effect to these Guidelines*…».

[372] Italia V., *Codice della privacy*, Giuffrè editore, Milano, 2004, pag. 486.

l'articolo 6 paragrafo 2[373] e l'articolo 17[374]. Il primo, come indica la sua rubrica, prevedeva dei principi inerenti alla qualità dei dati, ponendo in capo al responsabile del trattamento (titolare nel lessico del Regolamento) l'obbligo di farli rispettare, ricalcando così i termini di *accountability* intesa come *responsability* delle linee guida dell'Ocse[375]. L'articolo 17 invece riportava la questione nei termini della *data security*[376], imponendo l'adozione di «misure tecniche ed organizzative appropriate al fine di garantire la protezione dei dati personali dalla distruzione accidentale o illecita, dalla perdita accidentale o dall'alterazione, dalla diffusione o dall'accesso non autorizzati» e che «tali misure devono garantire, tenuto conto delle attuali conoscenze in materia e dei costi dell'applicazione, un livello di sicurezza appropriato rispetto ai rischi presentati dal trattamento e alla natura dei dati da proteggere». L'articolo 17 offre una prospettiva dinamica[377] delle misure di sicurezza, in quanto l'adeguatezza è da valutarsi

[373] L'articolo 6 stabiliva: «gli Stati membri dispongono che i dati personali devono essere: a) trattati lealmente e lecitamente; b) rilevati per finalità determinate, esplicite e legittime, e successivamente trattati in modo non incompatibile con tali finalità. Il trattamento successivo dei dati per scopi storici, statistici o scientifici non è ritenuto incompatibile, purché gli Stati membri forniscano garanzie appropriate; c) adeguati, pertinenti e non eccedenti rispetto alle finalità per le quali vengono rilevati e/o per le quali vengono successivamente trattati; d) esatti e, se necessario, aggiornati; devono essere prese tutte le misure ragionevoli per cancellare o rettificare i dati inesatti o incompleti rispetto alle finalità per le quali sono rilevati o sono successivamente trattati, cancellati o rettificati; e) conservati in modo da consentire l'identificazione delle persone interessate per un arco di tempo non superiore a quello necessario al conseguimento delle finalità per le quali sono rilevati o sono successivamente trattati. Gli Stati membri prevedono garanzie adeguate per i dati personali conservati oltre il suddetto arco di tempo per motivi storici, statistici o scientifici. Il responsabile del trattamento è tenuto a garantire il rispetto delle disposizioni del paragrafo».

[374] L'articolo 17 stabiliva: «gli Stati membri dispongono che il responsabile del trattamento deve attuare misure tecniche ed organizzative appropriate al fine di garantire la protezione dei dati personali dalla distruzione accidentale o illecita, dalla perdita accidentale o dall'alterazione, dalla diffusione o dall'accesso non autorizzati, segnatamente quando il trattamento comporta trasmissioni di dati all'interno di una rete, o da qualsiasi altra forma illecita di trattamento di dati personali.

Tali misure devono garantire, tenuto conto delle attuali conoscenze in materia e dei costi dell'applicazione, un livello di sicurezza appropriato rispetto ai rischi presentati dal trattamento e alla natura dei dati da proteggere».

[375] *«Under this typology the term accountability was originally used in data protection law in the sense of responsibility, a controller being responsible for ensuring compliance with the data protection rules, particularly those on data quality. This meaning can be seen in the original accountability principle in paragraph 14 of the OECD Guidelines 1980, Article 6(2) DPD and now Article 5(2) GDPR*», Docksey C., *Article 24. Responsability of the controller*, 2020, pag. 561.

«*First, accountability requires controllers and processors to take responsibility for the personal data they handle. In this sense it was present in Article 6(2) DPD and has been carried over into Article 5(2) GDPR*», ibidem.

[376] Italia V., *Codice della privacy*, 2004, pag. 488.

[377] Cuffaro V., D'Orazio R., Ricciuto V., *Il codice del trattamento dei dati personali*, G. Giappichelli Editore, Torino, 2006, pag. 222.

in base alle «attuali conoscenze in materia», soggette ad una spesso rapida obsolescenza.

Con la Direttiva madre si inizia dunque a vedere un approccio preventivo[378] rispetto ai rischi alla sicurezza che potevano eventualmente realizzarsi. La Direttiva madre presenta dunque un principio di *accountability* inteso come «principio di responsabilità»[379] all'articolo 6, accompagnato da un separato obbligo specifico di adozione di misure di sicurezza volte a prevenire possibili danni, previsto dall'articolo 17, e dal ricorso, in certi casi, al controllo preliminare dell'autorità garante[380]. La Direttiva madre viene attuata nell'ordinamento italiano attraverso la legge numero 675 del 1996. L'articolo 15 della legge 675/1995, rubricato «sicurezza dei dati», disponeva:

> «I dati personali oggetto di trattamento devono essere custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta. Le misure minime di sicurezza da adottare in via preventiva sono individuate con regolamento emanato con decreto del Presidente della Repubblica, ai sensi dell'articolo 17, comma 1, lettera a), della legge 23 agosto 1988, n. 400, entro centottanta giorni dalla data di entrata in vigore della presente legge, su proposta del Ministro di grazia e giustizia, sentiti l'Autorità per l'informatica nella pubblica amministrazione e il Garante»

[378] «*The protection categories-view concerns the idea of preventing an incident from happening, detecting if it has happened and at finally, react to the incident, reducing negative impacts and regain a normal situation. Article 17 uses the phrase "protecting against" unlawful destruction or accidental loss of information. The term "protecting against" emphasizes the proactive aspect of protection, which fits well with the protection category "prevention" in our protection-categories-view. Using the protection category-view, "prevention" appears to be the main security element accentuated*», Malbakken O. K., *Towards Measuring Legal Compliance. A case study on EU Directive 95/46, Article 17: Security in Processing*, 2004, pag. 20. Disponibile online al seguente link: https://ntnuopen.ntnu.no/ntnu-xmlui/bitstream/handle/11250/143920/M%C3%83%C2%A5lbakken_-_Towards_measuring_legal_compliance.pdf?sequence=1

[379] «*The 1980 OECD Privacy Guidelines included an Accountability Principle similar to the principle of responsibility in Article 6(2) DPD*», Docksey C., *Article 24. Responsability of the controller*, 2020, pag. 558.

«*The precursor to the principle of accountability is the principle of responsibility, which can be found in Article 6(2) DPD: 'It shall be for the controller to ensure that paragraph 1 is complied with'. In addition, Article 17(1) DPD required data controllers to implement measures of both a technical and organisational nature to ensure security of processing*». Ibidem.

[380] Pizzetti F., *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, 2016, pag 283.

Le ragioni della scelta di proseguire nel solco della *data security* sono espresse nelle parole nella relazione annuale del 1997 del Garante, secondo cui:

> «Le disposizioni che in varia forma regolano la raccolta, l'elaborazione e la divulgazione delle informazioni personali risulterebbero inefficaci qualora non fossero assistite da un'idonea politica della sicurezza che porti a custodire i dati e a gestire i sistemi riducendo al minimo il rischio della perdita anche accidentale delle informazioni o di un accesso non corretto o non consentito»[381].

La norma appresta un «doppio binario» di tutela: si hanno quindi delle misure «idonee» previste dal primo comma e delle misure «minime» previste dal secondo, entrambe accomunate dal dover essere preventive. La ragione della scelta del doppio binario si ritrova nella consapevolezza che la disciplina dettata dal primo comma appariva inidonea a garantire allo stesso tempo certezza del diritto e mantenimento del passo con i progressi della tecnica[382].
Per ovviare a tale problema, il secondo comma prevede delle misure minime di sicurezza obbligatorie. Queste erano specificatamente individuate per la prima volta dal regolamento numero 318 del 1999.
Come sottolineato, affinché una misura fosse «idonea», era necessario che fosse apprestata in base alle più recenti «conoscenze acquisite in base al progresso tecnico»[383], in base alla «natura dei dati»[384] e alle «specifiche caratteristiche del trattamento». L'aver legato l'idoneità delle misure *ex* primo comma al requisito del progresso tecnico conduceva ad una particolare ampiezza della forbice di misure concretamente applicabili[385]. Le misure «minime» invece, erano quelle specificatamente indicate nel regolamento numero 318 del 1999. A questa differenza si devono i due

---

[381] La relazione annuale è disponibile online al seguente link:
https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1343323#2.2

[382] Cuffaro V., D'Orazio R., Ricciuto V., *Il codice del trattamento dei dati personali*, 2006, pag. 223.

[383] «il riferimento a specifiche misure non sarebbe risultato possibile dal momento che esse mutano continuamente al variare delle nuove tecnologie». Cassano G., Fadda S., *Codice in materia di protezione dei dati personali*, Wolters Kluwer Italia, Ipsoa, 2004, pag. 211. Nello stesso senso vedasi Monducci J., Sartor G., *Il codice in materia di protezione dei dati personali*, Cedam, Padova, 2004, pag. 142.

Per i problemi interpretativi della norma vedasi invece Pardolesi R., *Diritto alla riservatezza e circolazione dei dati personali*, Giuffrè, Milano, 2003, pag. 761.

[384] «è evidente, infatti, che per i dati sensibili, sanitari o giudiziari, occorrerà una protezione superiore rispetto ai semplici dati personali, con conseguente aggravio della relativa responsabilità in caso di mancata adozione». Cassano G., Fadda S., *Codice in materia di protezione dei dati personali*, 2004, pag. 210.

[385] Monducci J., Sartor G., *Il codice in materia di protezione dei dati personali*, 2004, pag. 142.

diversi profili di responsabilità legati ora alla mancata predisposizione di misure «idonee» (responsabilità civile), ora alla manca apposizione di misure «minime» (anche responsabilità penale). Da evidenziare in ultimo, come l'esplicito riferimento ai «i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta» possa far emergere un embrionale approccio al rischio apprestato dal legislatore italiano[386].

Per quanto riguarda invece il vecchio Codice Privacy, le principali norme di riferimento erano l'articolo 31 e 33, che riprendevano quanto già previsto dalla legislazione previgente[387], avendo il pregio di essere più chiare e definite[388]. L'articolo 31, rubricato «obblighi di sicurezza», stabiliva:

> «dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta».

L'articolo 33, rubricato «misure minime»:

> «Nel quadro dei più generali obblighi di sicurezza di cui all'articolo 31, o previsti da speciali disposizioni, i titolari del trattamento sono comunque tenuti ad adottare le misure minime individuate nel presente capo o ai sensi dell'articolo 58, comma 3, volte ad assicurare un livello minimo di protezione dei dati personali».

L'articolo 31 si ricollegava ai principi generali sulla sicurezza espressi nell'articolo 7 della convenzione 108/1981, nell'articolo 17 della Direttiva

---

[386] «La nozione di rischio era, tuttavia, scarsamente enfatizzata dal legislatore italiano nel suo (tardivo) affacciarsi sulla scena europea della regolamentazione in materia di trattamento dei dati personali. Nell'articolato normativo, tale nozione era infatti principalmente circoscritta ed assorbita dai riferimenti alla sicurezza dei dati (alla quale il menzionato art. 15 era dedicato), cui maggior attenzione veniva posta e che costituiva oggetto specifico dei compiti del titolare. Il rischio diveniva però l'elemento portante della disciplina per quanto concerneva i profili di responsabilità civile, in virtù dell'espresso richiamo all'art. 2050 c.c. effettuato dall'art. 18 della I. 675/1996», Mantelero A., *La gestione del rischio*, 2019, pag. 473.

[387] «Conformemente a quanto già previsto vigente la precedente normativa, anche il Codice prevede un duplice livello di sicurezza: quello costituito da «tutte le misure idonee ad evitare il danno», idoneo ad evitare la responsabilità civile *ex* art. 15 del Codice e quello costituito dal livello minimale, rappresentato per l'appunto da altre misure di sicurezza». Finocchiaro G., *Privacy e protezione dei dati personali*, Zanichelli editore, Torino, 2012, pag. 254.

[388] Cuffaro V., D'Orazio R., Ricciuto V., *Il codice del trattamento dei dati personali*, 2006, pag. 225.

madre, e nell'articolo 4 della posizione comune CE 57/96 sulla riservatezza nelle telecomunicazioni[389]. I principali rischi da questo individuati erano dunque la distruzione o la perdita, anche accidentale, dei dati; l'accesso non autorizzato, ed il trattamento non consentito o non conforme alle finalità del trattamento[390]. La norma è quasi identica al disposto dell'articolo 15 comma 1 della legge 675 del 1996, e da essa emergevano due importanti obblighi: di custodia e di controllo, da rispettare mediante l'adozione di «di idonee e preventive misure di sicurezza». Non era chiaro quale fosse il soggetto gravato dagli obblighi *ex* articolo 31, né la sanzione che conseguiva alla mancata attuazione degli stessi; tuttavia, attraverso un'interpretazione sistematica era possibile rilevare che il soggetto fosse il titolare, e ove nominato il responsabile del trattamento[391]. I doveri di custodia e controllo venivano inoltre definiti «doveri di sicurezza dinamici», in quanto il titolare ed il responsabile non potevano considerarsi esenti da responsabilità per il solo fatto di averli rispettati in un dato momento storico: si richiedeva loro di custodirli e controllarli durante l'intero ciclo del trattamento, considerando tutte le caratteristiche del trattamento *de quo*[392]. L'attuazione di misure idonee era strumentale al soddisfacimento degli obblighi di custodia e controllo, e la diligenza che il titolare doveva tenere era mutevole e da ragguagliare *per relationem*[393] rispetto ai parametri indicati dallo stesso articolo 31, e quindi alle «conoscenze acquisite in base al progresso tecnico»[394], alla «natura dei dati» e alle «specifiche caratteristiche del trattamento».

Per quanto concerne le misure concretamente applicate, la loro idoneità andava valutata anche attraverso un criterio preminentemente teleologico, che dimostrasse di aver ridotto al minimo i rischi di distruzione o perdita, di accesso non autorizzato o non conforme alle finalità acconsentite. Considerato il regime di responsabilità previsto dallo stesso

---

[389] Italia V., *Codice della privacy*, 2004, pag. 486.

[390] Imperiali R., Imperiali R., *Codice della privacy*, Il Sole 24 Ore, Milano, 2004, pag. 211.

[391] Cuffaro V., D'Orazio R., Ricciuto V., *Il codice del trattamento dei dati personali*, 2006, pag. 229. La questione veniva così risolta anche in riferimento all'articolo 15 della Legge 675 del 1996: Pardolesi R., *Diritto alla riservatezza e circolazione dei dati personali*, 2003, pag. 756.

[392] Finocchiaro G., *Privacy e protezione dei dati personali*, 2012, pag. 253; Acciai R., *Il diritto alla protezione dei dati personali*, Maggioli Editore, Santarcangelo di Romagna, 2004, pag. 239.

[393] Del Ninno A., *La tutela dei dati personali*, Cedam, Padova, 2006, pag. 129; Sica S., Stanzione P., *La nuova disciplina della privacy*, Zanichelli Editore, Torino, 2005, pag. 127.

[394] Si ritiene attuale quanto affermato in dottrina in merito al tema degli ultimi sviluppi tecnologici: è stato sottolineato che era difficile stabilire, in sede di responsabilità, quali fossero le frontiere tecnologiche acquisite in un determinato ambito tecnologico. Non si tratterà dell'ultima innovazione tecnologica, ma di quelle conoscenze adeguatamente sviluppate, testate e diffuse che il titolare avrebbe potuto e dovuto utilizzare. Sul punto Cuffaro V., D'Orazio R., Ricciuto V., *Il codice del trattamento dei dati personali*, 2006, pag. 231.

codice, incentrato sull'articolo 2050[395] del codice civile, era possibile «postulare una sostanziale identità tra *misure idonee ad evitare il danno* (di cui all'art. 2050 c.c.) e *misure idonee a ridurre al minimo i rischi* (di cui all'art. 31)»[396]. Conseguentemente, la misura era da considerarsi adeguata nel caso in cui, in un giudizio *ex ante*, fosse idonea a prevenire i rischi ordinari che potevano presentarsi nell'ambito di quello specifico trattamento[397]. Anche il codice, così come la Direttiva madre, prevedeva una responsabilità civile in caso di violazione di misure idonee e penale in caso di misure minime.

Per quanto concerne le misure minime, queste erano previste dagli articoli 34 e seguenti, e dal disciplinare tecnico contenuto nell'allegato B, che sostituiva l'abrogato d.P.R. 318/1999, il quale disponeva obblighi giuridici ed informatici[398]. Alla violazione dell'allegato B, l'articolo 169 comma 1 del codice, collegava una sanzione penale *(*«chiunque, essendovi tenuto, omette di adottare le misure minime previste dall'articolo 33 è punito con l'arresto sino a due anni o con l'ammenda da diecimila euro a cinquantamila euro»). Il codice, all'articolo 4 comma 3 sulle definizioni, definiva le misure minime come «il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31».

3.2 Il principio di *accountability* e il *quid novi* rispetto alla Direttiva 95/46/CE

Nel citato parere numero 3 del 2010 del Gruppo di lavoro, si proponeva l'inserimento di una nuova disposizione avente lo scopo di promuovere misure concrete e pratiche, in grado di applicare i principi generali del trattamento. Si enfatizzava la figura del responsabile del trattamento (titolare nel lessico del Regolamento), che avrebbe dovuto garantire l'efficacia di tali misure ed essere in grado di dimostrarne l'applicazione e l'efficacia. Si descriveva la disposizione scomponendola in

[395] L'articolo 2050 del codice civile, rubricato «responsabilità per l'esercizio di attività pericolose», prevede che «chiunque cagiona danno ad altri nello svolgimento di un'attività pericolosa, per sua natura o per la natura dei mezzi adoperati, è tenuto al risarcimento, se non prova di avere adottato tutte le misure idonee a evitare il danno».

[396] Cuffaro V., D'Orazio R., Ricciuto V., *Il codice del trattamento dei dati personali*, 2006, pag. 231; similmente anche Sica S., Stanzione P., *La nuova disciplina della privacy*, 2005, pag. 128; Del Ninno A., *La tutela dei dati personali*, 2006, pag. 128; Imperiali R., Imperiali R., *Codice della privacy*, 2004, pag. 210.

[397] Cuffaro V., D'Orazio R., Ricciuto V., *Il codice del trattamento dei dati personali*, 2006, pag. 231.

[398] Italia V., *Codice della privacy*, 2004, pag. 482.

due elementi principali: l'adozione di misure appropriate ed efficaci al fine di garantire i principi del trattamento e la loro dimostrabilità[399].

Il principio di *accountability* è oggi menzionato esplicitamente all'articolo 5 paragrafo 2 e nel considerando 85 del Regolamento[400], tradotto con l'espressione «principio di responsabilizzazione». L'articolo 5 paragrafo 2 ne offre una definizione, stabilendo che «il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»)». In altre parole, il titolare deve rispettare i principi del trattamento previsti dall'articolo 5 paragrafo 1 e dev'essere in grado di dimostrarne la conformità.

L'origine dell'articolo 5 paragrafo 2 è ravvisabile nell'articolo 6 paragrafo 2 della Direttiva madre, cui è stata aggiunto l'obbligo di comprovare l'osservanza dei principi esposti al paragrafo 1[401].

Nel paragrafo dedicato alle fonti del diritto alla protezione dei dati personali (capitolo 2, paragrafo 2), si è fatto riferimento al cambio di paradigma che è avvenuto con il passaggio dalla Direttiva madre al GDPR. In questo capitolo se ne parlerà più diffusamente, in quanto il cambiamento d'impostazione si deve in gran parte al principio di *accountability*[402]: grazie ad esso, infatti, si è passati da un modello incentrato sull'autodeterminazione dell'interessato sulla base del consenso informato, ad uno in cui vengono responsabilizzate alcune figure tipiche (titolare e responsabile del trattamento) attraverso la doverosa valutazione, prevenzione e gestione del rischio unita ad una serie di doveri specifici[403]. Da

---

[399] Parere 3/2010 del Gruppo di lavoro *ex* articolo 29 sul principio di responsabilità, pag. 9.

[400] Considerando numero 85: «…Pertanto, non appena viene a conoscenza di un'avvenuta violazione dei dati personali, il titolare del trattamento dovrebbe notificare la violazione dei dati personali all'autorità di controllo competente, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che il titolare del trattamento non sia in grado di dimostrare che, conformemente al principio di responsabilizzazione, è improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche…».

[401] Riccio G. M., Scorza G., Belisario E. (a cura di), *GDPR e normativa privacy*, 2018, pag. 61.

[402] Amore G., *Fairness, Transparency e Accountability nella protezione dei dati personali*, 2020, pag. 415.

[403] «In questa prospettiva, proprio l'analisi dei rischi ed il conseguente processo di mitigazione di questi ultimi rappresentano la chiave di volta di un modello a venire, in cui la centralità dell'individuo e della sua tutela muovono da una dimensione endogena verso una esogena. Partendo, infatti, dall'assunto che gli individui non sono e non possono, per i motivi anzidetti, essere completamente consapevoli delle potenziali conseguenze del trattamento dei dati in sistemi complessi, si deve approdare alla conclusione che tali conseguenze devono essere necessariamente e previamente valutate ad opera di terzi, in maniera per certi versi analoga a quanto accade per la sicurezza dei prodotti». Mantelero A., *Responsabilità e rischio nel Reg. UE 2016/679*, Le nuove leggi civili commentate, volume 1, Febbraio 2017, pag. 149. Nello stesso senso Tosi E., *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale*, 2019, pag. 35; Bilotta F., *La responsabilità civile nel trattamento dei dati personali*, 2019, pag. 446; Greco L., *L'organigramma privacy: i soggetti del trattamento*, in Finocchiaro G., *La protezione dei dati*

segnalarsi come parte della dottrina abbia segnalato un cambiamento più apparente che sostanziale[404], in quanto, come visto poc'anzi nell'analisi della previgente disciplina, la valutazione del rischio era prevista anche prima del GDPR e non era possibile limitarsi alla mera applicazione delle misure minime di sicurezza[405]. Si rammenta infatti come l'articolo 31 del vecchio Codice Privacy, riprendendo l'impianto del doppio binario delle misure di sicurezza già previsto nella legge numero 675 del 1995, richiedesse al titolare del trattamento la preventiva adozione di misure che, in base ad un giudizio *ex ante*, fossero idonee a prevenire i rischi ordinari che potevano verificarsi in quello specifico trattamento. Dunque, la preventiva valutazione del rischio era già presente prima del GPDR[406]. Il Regolamento ha tuttavia il pregio di specificare le disposizioni relative alla gestione del rischio, mettendole in risalto rispetto a quanto fatto dalla Direttiva madre,

personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101, 2019, pag. 324; Riccio G. M., Scorza G., Belisario E. (a cura di), *GDPR e normativa privacy*, 2018, pag. 337.

[404] Mantelero A., *La gestione del rischio*, 2019, pag. 476.

In modo più specifico: «l'approccio alla regolamentazione del trattamento dei dati personali incentrato sull'analisi e gestione del rischio, sebbene non innovativo, costituisce l'aspetto centrale del nuovo Regolamento 2016/679. Tale impostazione si colloca nel solco della storica attenzione per gli aspetti procedurali e tecnologici dell'impiego delle informazioni, che hanno sin dalle origini connotato le normative in materia di trattamento dati», Mantelero A., *Responsabilità e rischio nel Reg. UE 2016/679*, 2017, pag.163.

Nello stesso senso, il Gruppo di lavoro nell'opinione del 30 Maggio 2014 dedicata all'approccio al rischio, pag. 2: «*the so-called "risk-based approach" is not a new concept, since it is already well known under the current Directive 95/46/EC especially in the security (Article 17) and the DPA prior checking obligations (Article 20*)». Il parere è disponibile online al seguente link:

https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf

Vedasi anche il parere numero 3 del 2010 del Gruppo di lavoro (pag. 10), in cui: «il Gruppo di lavoro articolo 29 desidera sottolineare che, per la maggior parte, gli obblighi contemplati nella nuova disposizione sono in realtà già previsti, anche se meno esplicitamente, dalla normativa vigente. Infatti, in forza dell'attuale quadro giuridico, i responsabili del trattamento sono tenuti a rispettare i principi e gli obblighi stabiliti dalla direttiva. A tal fine, è intrinsecamente necessario creare, ed eventualmente verificare, le procedure relative alla protezione dei dati. In quest'ottica, una disposizione sulla responsabilità non rappresenta una grande novità, e per la maggior parte non impone obblighi che non fossero già impliciti nella normativa vigente. In sintesi, la nuova disposizione non mira ad assoggettare i responsabili del trattamento a nuovi principi, ma piuttosto a garantire di fatto l'effettiva osservanza di quelli esistenti». Disponibile online al seguente link: https://www.garanteprivacy.it/documents/10160/10704/Articolo+29+-+WP173+-+Parere+3+2010+sul+principio+di+responsabilit%C3%A0.pdf/006f43b3-7180-4485-903e-bf8b4f367763?version=1.2

[405] «Da qui un quadro contrassegnato da continuità e, nel contempo, da mutamenti, ma in linea con la centralità della dimensione del rischio, che ha connotato tutta la storia della disciplina del trattamento dati», Mantelero A.., *La gestione del rischio*, 2019, pag. 477.

[406] Vi è chi parla di principio di *accountability ante litteram* in merito alla disciplina del vecchio codice privacy, Tosi E., *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale*, 2019, pag. 31.

delineando anche il tipo di ruolo che in relazione ad esse assumono il titolare ed il responsabile del trattamento, così come le autorità di controllo[407].

Il Regolamento presenta dunque un assetto volto a responsabilizzare chi tratta i dati personali: si impone a questi di scegliere di volta in volta le misure più opportune per modulare l'applicazione dei principi previsti dal Regolamento in base al caso concreto ed ai rischi che questo presenta[408], così da meglio garantire la protezione dei dati e le libertà fondamentali[409]. Le misure da predisporre sono nella sua piena e libera disponibilità[410] (il Regolamento incoraggia l'utilizzo di alcune misure, quali la pseudonimizzazione, senza però mai obbligare alla loro applicazione). Tale libertà di scelta ha l'obiettivo di responsabilizzare il titolare del trattamento, in quanto questi dovrà proattivamente valutare caso per caso quali misure adottare per meglio garantire la conformità al Regolamento, senza più appoggiarsi alle misure minime previste in precedenza, scomparse con l'avvento del Regolamento[411].

Quanto riportato mette in evidenza come si sia passati da un sistema imperniato su specifiche disposizioni ad uno decisamente più elastico, che impone al titolare del trattamento di scegliere le misure da apprestare,

[407] Mantelero A., *Responsabilità e rischio nel Reg. UE 2016/679*, 2017, pag. 163.

[408] «*A risk-based approach in data protection law means to directly link the level of risks to the rights and freedoms of natural persons to the nature and extent of the measures taken to protect them».* Selzer A., *The Appropriateness of Technical and Organisational Measures under Article 32 GDPR*, European Data Protection Law Review, 2021, pag. 120.

[409] Finocchiaro G., *Il Principio di Accountability*, Giurisprudenza Italiana, Dicembre 2019, pag. 2778.

[410] «Discrezionalità libera ma non illimitata, anzi necessariamente parametrata alle condizioni indicate nello stesso art. 24 GDPR, quali la natura, l'àmbito di applicazione, il contesto e le finalità del trattamento, nonché il rischio di lesione dei diritti e delle libertà delle persone fisiche», Amore G., *Fairness, Transparency e Accountability nella protezione dei dati personali*, 2020, pag. 424.

[411] «Infine, coerentemente con il continuo evolvere della tecnologia e dei rischi connessi, il Regolamento adotta un approccio dinamico al rischio, incentrato sul caso concreto e sull'evoluzione dei fattori di rischio da affrontarsi mediante una revisione periodica dell'analisi di questi ultimi, superando - per quanto riguarda l'esperienza italiana - l'arretratezza di un modello normativo statico qual era quello che emergeva in larga parte dall'Allegato B al d.lgs. 196/2003, la cui natura obsoleta era di chiara evidenza», Mantelero A., *La gestione del rischio*, 2019, 476.

prestando particolare attenzione ai profili di rischio[412] che potrebbero verificarsi in quel determinato trattamento[413].

I riferimenti normativi cui è possibile ricondurre il principio di *accountability* sono diversi, e unitamente considerati ne restituiscono la portata complessiva. Le relative norme principali sono il già citato articolo 5 paragrafo 2 e gli articoli 24, 25 e 32[414]. L'articolo 5 paragrafo 2 stabilisce che «il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»)»[415]. L'articolo 24 invece sancisce che:

> «Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario.
>
> Se ciò è proporzionato rispetto alle attività di trattamento, le misure di cui al paragrafo 1 includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento. L'adesione ai codici di condotta di cui all'articolo 40 o a un meccanismo di certificazione di cui all'articolo 42 può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento»[416].

---

[412] Alcuni rischi connessi al trattamento sono indicati al considerando 75: « I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati.», e al considerando 83: «rischi presentati dal trattamento dei dati personali, come la distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati a dati personali trasmessi, conservati o comunque elaborati, che potrebbero cagionare in particolare un danno fisico, materiale o immateriale».

[413] Tosi E., *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale*, 2019, pag. 37; Finocchiaro G., *Il Principio di Accountability*, 2019, pag. 2778.

[414] Tosi E., *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale*, 2019, pag. 36.

[415] GDPR.

[416] GDPR.

L'articolo 32 infine dispone che:

> «Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:
>
> a) la pseudonimizzazione e la cifratura dei dati personali…»[417].

Queste norme restituiscono gli elementi di responsabilizzazione più rilevanti, ma non sono le uniche. Attraverso la scelta di tale principio (e non di una disposizione puntuale) si è inteso ammantare l'intero sistema, riformandolo radicalmente[418].

Il principio di *accountability* espresso nel GDPR segna il completamento del passaggio (già iniziato dalla Direttiva madre[419]) da una prospettiva riparatoria (rivelatasi inadeguata[420]) ad una preventiva, con disposizioni che apprestano una protezione da un momento anteriore rispetto al trattamento[421].

A tal proposito, significative appaiono le parole di Giovanni Buttarelli, già Garante europeo dei dati personali, che nel 2016 affermava: «nel settore

---

[417] GDPR.

[418] «Tuttavia esso costituisce una forza sotterranea che informa di sé pressoché tutti gli istituti del Regolamento. È il verso nella cui direzione occorre applicare e interpretare le norme nella materia de qua», Bolognini L., Pelino E., *Codice della disciplina privacy*, 2019, pag. 88; «…nei fora internazionali di data protection si parla di "overarching concept of accountability", dove overarching sta proprio ad indicare la portata globale dell'obbligo di responsabilità…», Riccio G. M., Scorza G., Belisario E. (a cura di), *GDPR e normativa privacy*, 2018, pag. 237; «in base a tali principi, letti in combinato disposto con quello di *accountability* che di fatto permea l'intero assetto del Regolamento…», Panetta M., *I controlli aziendali e le indagini* difensive, in Panetta R., *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, 2019, pag. 378.

[419] Malbakken O. K., *Towards Measuring Legal Compliance. A case study on EU Directive 95/46, Article 17: Security in Processing*, 2004, pag. 20.

[420] Borrillo B., *La tutela della privacy e le nuove tecnologie: il principio di accountability e le sanzioni inflitte dalle Autorità di controllo dell'Unione europea dopo l'entrata in vigore del GDPR*, Dirittifondamentali.it, fascicolo 2, 2020, pag. 351. Disponibile online al seguente link: https://dirittifondamentali.it/2020/05/18/5984/

[421] Mantelero A., *Responsabilità e rischio nel Reg. UE 2016/679*, 2017, pag. 146; Panetta R., *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, 2019, pag. 9: «la principale chiave di lettura per interpretare la riforma è l'accento posto sull'*accountability* di chi tratta i dati. Nuovi istituti come la portabilità dei dati, l'illustrazione della logica decisionale adottata, i registri del trattamento e la valutazione di impatto *privacy* (c.d. DPIA) spostano il focus dalla rigidità dello scrutinio *ex ante* dell'Autorità Garante alla responsabilizzazione dei titolari, che internalizzano le proprie valutazioni utilizzando il rischio per i diritti e le libertà delle persone fisiche come parametro-guida».

pubblico e privato sarà richiesto non semplicemente di rispettare le norme, e quindi di fare una check-list degli adempimenti minimi, ma di tradurre in pratica questi principi con diversi "compiti a casa" in chiave di creatività e proattività»[422]. I titolari del trattamento hanno oggi non solo la suddetta possibilità di scegliere autonomamente le misure più appropriate, ma anche l'opportunità di considerare come il Garante abbia valutato le misure minime di sicurezza applicate in passato, utilizzando quei provvedimenti come punto di riferimento per l'adozione delle misure più opportune[423]. Tra le ragioni legate all'introduzione di un principio siffatto vi è il nuovo contesto informatico in cui i dati circolano. Oggi si è dinanzi ad uno scambio di informazioni non più unidirezionale (dall'interessato al titolare) e non regolabile attraverso la sola disciplina del consenso. Le informazioni circolano attraverso i *social networks*, i motori di ricerca, e sono parte di un modello di condivisione e cogestione dei dati destinato ad una circolazione globale[424], non più regolabile in modo soddisfacente dalla Direttiva madre[425]. A tale aumento di autonomia di scelta, fa da contraltare una maggiorata responsabilizzazione del titolare[426]: intesa questa come un dovere di autonoma e costante ricerca dei mezzi più appropriati per assicurare la protezione dei dati personali e delle libertà fondamentali (l'ultima parte del primo paragrafo dell'articolo 24 stabilisce che «dette misure sono riesaminate e aggiornate qualora necessario»); unitamente all'obbligo di renderne conto alle autorità competenti. Ciò pone il titolare al centro della disciplina[427]: questo riceve dal Regolamento onerose attribuzioni di autonomia di scelta[428], pena la sua responsabilità *ex* articolo 82 del Regolamento. Ogni qualvolta il Regolamento conferirà questo tipo di libertà di scelte, allora si sarà dinanzi ad una manifestazione del principio di *accountability*. A parere di chi scrive, le norme succitate (articolo 5 paragrafo 2, articolo 24 , 25 e 32) forniscono i punti cardinali dell'istituto: esso è un principio generale (espresso esplicitamente all'articolo 5 paragrafo 2),

[422] Intervista a Giovanni Buttarelli, 18 Gennaio 2016, disponibile online al seguente link: https://www.corrierecomunicazioni.it/digital-economy/buttarelli-data-protection-tanti-compiti-a-casa-per-gli-stati-e-l-ue/

[423] Finocchiaro G., *Il principio di accountability*, 2019, pag. 2782.

[424] Finocchiaro G., *Introduzione al Regolamento europeo sulla protezione dei dati,* Nuove leggi civili commentate, volume 1, 2017, pag. 1.

[425] Riccio G. M., Scorza G., Belisario E. (a cura di), *GDPR e normativa privacy*, 2018, pag. 237.

[426] Tosi E., *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale*, 2019, pag. 37.

[427] Greco L., *L'organigramma privacy: i soggetti del trattamento*, 2019, pag. 324.

[428] «Il GDPR riconosce e attribuisce al titolare del trattamento il potere di scegliere modalità e strumenti di attuazione delle prescrizioni europee a fronte dell'obbligo di dimostrarne la correttezza e l'adeguatezza rispetto al caso concreto. Pro e contro dunque: da un lato discrezionalità e diritto di scelta, dall'altro incertezza della "bontà" dell'operato e delle valutazioni effettuate fino all'eventuale esame da parte dell'autorità giudiziaria o amministrativa», Amore G., *Fairness, Transparency e Accountability nella protezione dei dati personali*, 2020, pag. 422.

inerente alla responsabilità del titolare del trattamento (articolo 24), da rispettare sin dalla progettazione del trattamento (articolo 25), che impone l'applicazione di adeguate misure tecniche ed organizzative (24, 25 e 32), con particolare attenzione ai profili di sicurezza disciplinati dall'articolo 32; in funzione di una corretta previsione, prevenzione e gestione del rischio derivante dal trattamento, sì da evitare la violazione del diritto alla protezione dei dati personali e delle libertà fondamentali degli interessati; infine, il tutto dev'essere dimostrabile in ogni momento (*ex* articoli 5 paragrafo 2 e 24). Gli obblighi principali imposti dal principio di *accountability* sono due[429].

Il primo si sostanzia nell'adozione di misure tecniche e organizzative adeguate per garantire il rispetto dei principi e delle altre prescrizioni previste dal Regolamento. Il secondo invece consiste nell'obbligo di dimostrare in ogni momento all'autorità (garante o giudiziaria che effettui le valutazioni *ex post* del caso) la conformità al Regolamento imposta dalla prima prescrizione[430]. Chi scrive ritiene che il principio di *accountability* possa anche essere considerato alla stregua di un metodo, che va applicato in tutte le fasi del trattamento («sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso» secondo il dettame dell'articolo 25) nell'ottica di garantire la miglior protezione dei dati personali e delle libertà fondamentali possibile.

3.3 Le misure tecniche ed organizzative adeguate

Come già visto, uno dei doveri principali imposti dall'articolo 24 del Regolamento è quello di apprestare adeguate misure tecniche ed organizzative volte a garantire che il trattamento avvenga conformemente al Regolamento. Le misure tecniche ed organizzative, oltre all'articolo 24, sono previste in diversi punti del Regolamento, ad esempio nell'articolo 25 («protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita»), 28 («responsabile del trattamento»), 32 («sicurezza del trattamento») e 83 («condizioni generali per infliggere sanzioni amministrative pecuniarie»).

[429] «Il principio della accountability si sostanzia in due obblighi: a) adottare misure per implementare i principi sul trattamento dei dati e b) dimostrare, su richiesta, il rispetto di tali principi. In ciò possiamo individuare due livelli di applicazione: il primo, generale, si applica a tutti i titolari e concerne il mero rispetto del Regolamento e l'onere di provare tale rispetto; il secondo, volontario, consiste in misure scelte dal singolo titolare per l'efficace salvaguardia dei diritti dei soggetti interessati dal trattamento», commento di Malgieri C., 2021, pag. 189.

[430] «*Accountability* che si declina nel fare e nel provare di aver fatto», Tosi E., *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale*, 2019, pag. 37.

Il GDPR non definisce cosa si intenda per esse; soccorrono in questo caso le linee guida numero 4 del 2019 dell'Edpb[431], in cui si afferma che per misura può intendersi qualsiasi metodo o strumento che il titolare può sfruttare per il trattamento[432]; per fare alcuni esempi, una misura organizzativa tipica è la designazione del capitale umano da impiegare per il trattamento, come la nomina di un particolare responsabile del trattamento perito del settore specifico in cui avviene il trattamento. Un'altra misura organizzativa comune consiste nel tenere corsi di formazione periodici per tutti i soggetti coinvolti nel trattamento, di modo che tutte le fasi di questo si svolgano in conformità al Regolamento; per ultimo si potrebbe pensare alle valutazioni d'impatto ai sensi dell'articolo 35 del Regolamento. Per quanto concerne invece le misure tecniche, si pensi a quelle previste contro la distruzione o perdita dei dati, quali i *back-up* automatici; oppure a quelle applicate per garantire la confidenzialità delle informazioni, ad esempio la crittografia. Si evince dunque una atipicità di dette misure, in ossequio al principio di *accountability*, secondo cui è compito del titolare del trattamento individuare le più adeguate[433]. La ragione può rinvenirsi nelle parole del Gruppo di lavoro nel parere numero 3 del 2010, dove si affermava:

---

[431] Linee guida numero 4 del 13 Novembre 2019 del European Data Protection Board sull'articolo 25 e il principio di *Data Protection by Design and by Default*, disponibili online al seguente link:

https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf

[432] Linee guida 4/2019 del European Data Protection Board sull'articolo 25 e il principio di *Data Protection by Design and by Default*, pag. 6.

[433] Amore G., *Fairness, Transparency e Accountability nella protezione dei dati personali*, 2020, pag. 424; anche Riccio G. M., Scorza G., Belisario E. (a cura di), *GDPR e normativa privacy*, 2018, pag. 240: «il Regolamento dunque non prevede un elenco esaustivo di "misure adeguate" e questo fa sì che debba ritenersi necessaria una valutazione caso per caso seguendo gli orientamenti e le indicazioni in merito dell'Autorità Garante per la protezione dei dati personali (Garante), tenendo conto anche dello stato dell'arte».

Il Gruppo di lavoro, nel parere numero 3 del 2010 (pag. 12) aveva proposto un elenco non esaustivo di misure applicabili dal titolare del trattamento: «istituzione di procedure interne prima della creazione di nuove operazioni di trattamento dei dati personali (revisione interna, valutazione, ecc.); formulazione per iscritto di politiche di protezione dei dati vincolanti da prendere in considerazione e applicare alle nuove operazioni di trattamento dei dati (ad esempio, qualità dei dati, comunicazione, principi di sicurezza, accesso, ecc.), che dovrebbero essere a disposizione degli interessati; mappatura delle procedure per garantire la corretta identificazione di tutte le operazioni di trattamento dei dati e gestione di un inventario di dette operazioni; nomina di un incaricato della protezione dei dati e di altri soggetti responsabili della protezione dei dati; adeguata formazione e istruzione del personale in materia di protezione dei dati. Il personale in questione dovrebbe includere gli incaricati (o responsabili) del trattamento dei dati personali (come i direttori delle risorse umane), ma anche dirigenti e sviluppatori in campo informatico, e direttori di unità commerciali. Dovrebbero essere stanziate risorse sufficienti per la gestione della privacy, ecc.; creazione di procedure trasparenti per gli interessati finalizzate alla gestione delle richieste di accesso, rettifica e cancellazione; istituzione di un meccanismo interno di gestione dei reclami; definizione di procedure interne per la gestione e la comunicazione efficace di violazioni della sicurezza; effettuazione di valutazioni d'impatto sulla privacy, in circostanze specifiche; attuazione e controllo delle procedure di verifica per

«da quanto precede risulta che nel determinare i tipi di azioni da attuare, non esistono alternative valide alle soluzioni "su misura". Infatti, le misure specifiche da applicare devono essere determinate in funzione dei fatti e delle circostanze di ciascun caso specifico, con particolare attenzione al rischio inerente al trattamento e al tipo di dati. Un approccio uguale per tutti avrebbe il solo effetto di costringere i responsabili del trattamento all'interno di strutture inadatte e si rivelerebbe quindi fallimentare»[434].

Proseguendo, il Regolamento non si esprime sul significato del requisito dell'adeguatezza; soccorre dunque il parere del Garante europeo della protezione dei dati del 7 Marzo 2012 (sulla proposta di regolamento che sarebbe poi divenuta l'odierno GDPR), ove si affermava che il termine «adeguate» implica che le misure siano apprestate sulla base del contesto e delle specifiche circostanze del caso[435]. Il fatto che la misura debba variare in base alle esigenze del singolo caso, evidenzia la scalabilità del principio di *accountability*, in quanto la responsabilizzazione del titolare muta al mutare del caso concreto, il quale nelle sue irripetibili circostanze (tipi di dati trattati, livello di rischio ecc.) determinerà l'adeguatezza di una misura o di un'altra[436].

Sulla idoneità delle misure si esprime anche l'Edpb nelle già citate linee guida numero 4 del 2019, quando afferma che per essere idonee, le misure devono essere adattate in modo da raggiungere lo scopo prefissato[437]. In merito ai criteri attraverso cui va parametrata l'adeguatezza della misura tecnica o organizzativa il Regolamento offre dei parametri ai succitati articoli 24, 25 e 32, unitamente al considerando numero 74; questi presentano alcuni elementi in comune: ambito di applicazione, contesto e finalità del trattamento, natura del trattamento e rischi aventi probabilità e gravità

---

assicurare che tutte le misure esistano non solo sulla carta, ma siano applicate e funzionino nella pratica (audit interni o esterni ecc.)».

[434] Parere 3/2010 del Gruppo di lavoro *ex* articolo 29 sul principio di responsabilità, pag. 13. A tal proposito, nello stesso documento, il Gruppo di lavoro prende in considerazione le perplessità relative all'incertezza del diritto derivante dall'ampiezza di un principio siffatto (pag. 14).

[435] «*The term 'appropriate' implies that the measures should take account of the context and the specific circumstances of the case». This is an important element that ensures the 'scalability' of the general obligation in practice, i.e. that effective measures can be required under all circumstances in a way appropriate for the relevant case*», opinione del European data protection supervisor sul pacchetto di riforme sulla protezione dei dati personali, pag. 28. Disponibile online al seguente link:

https://edps.europa.eu/data-protection/our-work/publications/opinions/data-protection-reform-package_en

[436] «*This is an important element that ensures the 'scalability' of the general obligation in practice, i.e. that effective measures can be required under all circumstances in a way appropriate for the relevant case*», ibidem.

[437] Linee guida 4/2019 del European Data Protection Board sull'articolo 25 e il principio di *Data Protection by Design and by Default*, pagina 6.

diverse per i diritti e le libertà delle persone fisiche. Gli articoli 25 e 32, rispetto all'articolo 24 e al considerando numero 74, richiedono anche la valutazione dello stato dell'arte e dei costi di attuazione, mentre l'articolo 32 richiede inoltre la valutazione dell'oggetto del trattamento. In merito ai criteri utili a modulare le misure necessarie, il Gruppo di lavoro, prendendo in considerazione i rischi derivanti dal trattamento e la natura dei dati trattati, scriveva che i grandi titolari del trattamento dovrebbero sempre attuare misure molto rigorose; talvolta però, le medesime accortezze potrebbero essere richieste anche alle piccole e medie imprese (*rectius*: piccoli e medi titolari del trattamento), qualora protraggano trattamenti che presentino un elevato livello di rischio: si faceva l'esempio dei servizi sanitari online[438].

Il titolare del trattamento dovrà prendere in considerazione tutti questi parametri per valutare la misura da apprestare, e lo stesso faranno le autorità in caso di valutazione *ex post* delle misure. La valutazione circa l'idoneità delle misure avverrà dunque sia *ex ante* che *ex post*[439]. Il titolare del trattamento dovrà valutare l'adozione delle misure già dalla fase di progettazione (*ex ante*) ed in un secondo momento queste misure verranno esaminare dalle autorità (*ex post*)[440]. Una valutazione positiva di idoneità *ex post* coinciderà con una misura adeguata applicata *ex ante*[441]. Non sempre sarà invece il contrario, ossia che una misura che inizialmente appariva adeguata mediante un giudizio *ex ante*, risulti adeguata anche nel giudizio *ex post*.

Queste misure, ai sensi dell'articolo 24 paragrafo 1, vanno inoltre riesaminate ed aggiornate qualora necessario: l'adeguatezza delle stesse potrebbe difatti venir meno in un momento successivo rispetto alla primaria applicazione. Nella proposta originaria della Commissione[442], all'articolo 22

---

[438] Parere 3/2010 del Gruppo di lavoro *ex* articolo 29 sul principio di responsabilità, pag.14.

[439] «Avendo, a questo punto, compreso quanto la validità delle misure debba essere considerata sia ex ante, ossia prima della loro adozione e prima che il trattamento abbia effettivamente inizio, sia ex post, vale a dire una volta adottate al termine del trattamento medesimo…», Bolognini L., Pelino E. *Codice della disciplina privacy*, 2019, pag. 201.

[440] «Si è pertanto anche parlato di "privatizzazione" delle regole sulla protezione dei dati, poiché il controllo pubblico è intermediato dal principio della responsabilizzazione dei soggetti privati», commento di Malgieri G., 2021, pag. 189.

[441] «*The above section seems to mean that accountability is dual in the GDPR because ex-post accountability cannot be properly work if appropriate measures have not been ex-ante prepared during the design phase of the processing activity. It shows alike that both the demonstration of compliance and the failure to demonstrate compliance have legal consequences for data controllers and processors. The failure exposes to sanctions23 while the demonstration of compliance allows to transfer the data outside the EU.24*», Lachaud E., *Accountability and Certification in the GDPR*, 22 Ottobre 2021, pag. 3. Disponibile online al seguente link:

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3948093.

[442] Disponibile online al seguente link: https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=celex%3A52012PC0011

paragrafo 3[443] sulla responsabilità del titolare del trattamento, era prevista una revisione operata da revisori esterni ed indipendenti. Il Parlamento europeo invece, aveva proposto un obbligo di revisione biennale delle politiche di conformità al Regolamento. Queste proposte, sebbene non approvate, indicherebbero la via per il titolare del trattamento, che dovrebbe promuovere revisioni periodiche, di modo da garantire l'adeguatezza delle misure preposte in ogni momento del trattamento[444].

3.4 La gestione del rischio e il principio di *accountability*

Si è già evidenziato come il GDPR sia incentrato sulla valutazione preventiva dei rischi del trattamento: più specificamente si tratta di valutare «rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche» (articoli 24, 25, e con parole diverse l'articolo 32). La gestione del rischio è fondamentale all'interno del Regolamento[445]: si è infatti sottolineato come alla base della scelta di regolamentazioni sovranazionali o quantomeno regionali, vi sia proprio la dimensione transnazionale dei rischi derivanti dal trattamento di dati (personali e non)[446]. Essa era già conosciuta nell'ambito della protezione dei dati personali, ma il Regolamento ha il pregio di formalizzarla in esplicite disposizioni, molto rilevanti, in cui si attribuiscono determinati obblighi, anche procedurali, a determinati attori.

Il mezzo attraverso cui prevenire tali rischi sono le predette misure tecniche ed organizzative, con l'obiettivo di rispettare i principi e le altre prescrizioni previste dal Regolamento, in quanto, nell'intenzione del legislatore europeo, rispettando queste norme vengono garantiti «i diritti e le libertà delle persone fisiche»[447]. La valutazione del rischio è un'attività

[443] Il terzo paragrafo recitava: «*the controller shall implement mechanisms to ensure the verification of the effectiveness of the measures referred to in paragraphs 1 and 2. If proportionate, this verification shall be carried out by independent internal or external auditors*».

[444] «*The element of audit by the controller remains in Article 28(3)(h), as part of the obligation on the processor to demonstrate compliance, in Article 39(b), as part of the tasks of the DPO, and in Article 47, as part of the mechanisms under a BCR to ensure verification of compliance*», Docksey C., *Article 24. Responsability of the controller*, 2020, pag. 562.

[445] «Il Regolamento generale sulla protezione dei dati suggerisce al titolare del trattamento un approccio proattivo rispetto alla sicurezza dei dati. Rispetto alla direttiva 95/46/CE, il GDPR è improntato al cd. *risk-based approach,* basato sul principio di *accountability*», Giovannangeli S. F., *La violazione di dati o data breach*, in Panetta R., *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, 2019, pag. 395.

[446] Mantelero A., *Responsabilità e rischio nel Reg. UE 2016/679*, 2017, pag. 147.

[447] Amore G., *Fairness, Transparency e Accountability nella protezione dei dati personali*, 2020, pag. 416.

richiesta dal principio di *accountability* in ogni fase del trattamento[448], e consequenzialmente, in base ai risultati, il titolare del trattamento dovrà modulare i propri obblighi[449]. L'articolo 25 GDPR ed il considerando numero 78 infatti, precisano che l'analisi dei rischi va effettuata sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso. Vi sono poi dei casi in cui il Regolamento specifica ulteriormente questo tipo di valutazione. Ad esempio, al momento della scelta circa l'opportunità di procedere con una valutazione d'impatto (articolo 35); nella valutazione in merito alla necessità di dotarsi di un registro dei trattamenti per le imprese o organizzazioni con meno di 250 dipendenti (articolo 30 paragrafo 5); per l'eventuale notifica di una violazione dei dati personali all'autorità di controllo e all'interessato (articolo 33 e 34) ecc. Importante sottolineare come quest'attività di gestione del rischio sia esplicitamente demandata anche al responsabile del trattamento (articolo 39 paragrafo 2). Più basso sarà il rischio, meno verrà richiesto al titolare (o responsabile), e viceversa[450].

Si procederà adesso attraverso l'analisi di alcune norme dalle quali emerge maggiormente il nuovo approccio *risks-based*. Innanzitutto, in dottrina è stato evidenziato come il Regolamento abbia adottato un sistema di gestione del rischio aperto, e non basato su *standard* di certificazione specifici. Per descriverlo, lo si può immaginare come diviso in tre moduli scalari: il primo sarebbe rappresentato dalle valutazioni preventive generiche, dettate dagli articoli 24, 25 e 32. Il secondo dalla valutazione di impatto ai sensi dell'articolo 35 ed infine dall'eventuale verifica operata dalle autorità di controllo[451].

Nel primo modulo spicca l'approccio incentrato sui principi di *data protection by design e by default*, che impongono una progettazione del trattamento che tenga in considerazione, tra i diversi fattori, i «rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento». La norma specifica che il trattamento va progettato già al momento in cui vengono scelte le relative modalità, attraverso la giustapposizione di misure tecniche ed organizzative adeguate. Inoltre, il principio di *data protection by default* prescrive che «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». Una corretta

---

[448] Tosi E., *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale*, 2019, pag. 94.

[449] Macenaite M., *The "Riskification" of European Data Protection Law through a two-fold Shift*, Cambridge University Press, 10 Ottobre 2017, pag. 20.

[450] «*…a data controller whose processing is relatively low risk may not have to do as much to comply with its legal obligations as a data controller whose processing is high-risk*», opinione del 30 Maggio 2014 del Gruppo di Lavoro, pag. 2.

«There should be recognition that not every accountability obligation is necessary in every case – for example where processing is small-scale, simple and low-risk», ibidem, pag. 3.

[451] Mantelero A., *La gestione del rischio*, 2019, pag. 493.

applicazione di tali principi potrebbe rendere superflua una valutazione finale del rischio, in quanto il prodotto o il servizio che si stava progettando sarà già stato adeguatamente modellato in relazione ai rischi derivabili dal trattamento[452]. Commentatori hanno sottolineato come queste valutazioni attribuiscano, in ossequio al principio di accountability, grande autonomia al titolare del trattamento nella scelta dei mezzi attraverso cui scegliere le precauzioni da adottare[453]. Qualora invece dal trattamento dovesse risultare, in virtù dell'uso di nuove tecnologie, della natura, dell'oggetto, del contesto e delle finalità del trattamento, «un rischio elevato per i diritti e le libertà delle persone fisiche», allora l'articolo 35 del Regolamento imporrà al titolare del trattamento di procedere attraverso una valutazione d'impatto. Questa rappresenta il secondo modulo di prevenzione del rischio; essa è solo eventuale, in quanto qualora non dovesse prevedersi un rischio elevato non sarà richiesta[454]. L'articolo 35 rappresenta una delle formalizzazioni operate dal Regolamento in merito alla gestione del rischio, che lo rende un *quid pluris* rispetto alla Direttiva madre[455], e che, sempre secondo chi scrive, mitiga l'autonomia conferita al titolare del trattamento dagli articoli 24, 25 e 32. Si può evidenziare, difatti, come il terzo paragrafo, preveda una serie di ipotesi[456] in cui la valutazione d'impatto è obbligatoria in quanto il rischio elevato si considera in *re ipsa*. Si parla di presunzione relativa, in quanto l'esistenza di un rischio elevato potrà essere smentita appunto attraverso la suddetta valutazione[457]. Il titolare, in queste ipotesi, non è dunque più libero di valutare l'opportunità di procedere attraverso la valutazione d'impatto. In altri casi non previsti invece, l'eventuale esistenza di un rischio elevato sarà interamente rimessa all'apprezzamento del titolare del trattamento, sempre in virtù del principio di *accountability*. Proseguendo, dal combinato disposto dei commi 7 e 11, si può affermare che la valutazione d'impatto conduca il titolare del trattamento attraverso cinque fasi: nella prima questi opera un'analisi del processo, prodotto, o attività, descrivendo sistematicamente i trattamenti previsti, le finalità e ove presente, il suo legittimo interesse; nella seconda fase valuta la necessità e proporzionalità dei trattamenti in relazione alle finalità, e i rischi per i diritti e le libertà degli interessati; nella terza descrive invece le misure che intende adottare per affrontare i rischi individuati; nella quarta verifica l'adeguatezza delle misure; infine, l'ultima fase è rappresentata dal monitoraggio periodico

[452] Ibidem, pag. 494; Mantelero A., *Responsabilità e rischio nel Reg. UE 2016/679*, 2017, pag. 157.

[453] Ratti M., in D'Orazio R., Finocchiaro G., Pollicino O., Resta G., *Codice della privacy e data protection*, 2021, pag. 418.

[454] Sulla questione circa l'automaticità o meno di rischi elevati derivanti dal contesto tecnologico odierno si dirà nel quinto capitolo.

[455] Mantelero A., *La gestione del rischio*, 2019, pag. 494.

[456] Il quarto paragrafo specifica che tali casi possono essere ampliati da quelli previsti dall'Autorità di controllo.

[457] Mantelero A., *Responsabilità e rischio nel Reg. UE 2016/679*, 2017, pag. 157.

di detta adeguatezza, che va mantenuta durante tutte le fasi del trattamento[458].

Si nota dunque una procedimentalizzazione della valutazione del rischio, connotata da una certa discrezionalità in merito alle specifiche valutazioni da farsi. Procedendo, il primo paragrafo dell'articolo 36 del Regolamento, così come interpretato dal Gruppo di lavoro[459,] impone al titolare del trattamento di consultare l'Autorità di controllo nel caso in cui vi siano degli alti rischi residuanti anche dopo l'apposizione delle misure che questi ha indicato nella valutazione d'impatto (paragrafo 7 dell'articolo 35). Tale istituto è stato preso maggiormente in considerazione dal Regolamento rispetto alla previgente disciplina[460]; attraverso esso si è inteso adottare un sistema semi-autorizzatorio, in cui ad una prima autovalutazione operata dal titolare del trattamento con la valutazione d'impatto, segue (solo eventualmente) una verifica da parte delle Autorità di controllo[461]. Concludendo, secondo chi scrive, anche nella valutazione del rischio, che costituisce il core del Regolamento, può notarsi un'importante discrezionalità attribuita al titolare ed al responsabile del trattamento[462], espressione del principio di *accountability*, contemperata però dagli istituti della valutazione d'impatto, caratterizzata da un certo grado di procedimentalizzazione che in taluni casi è obbligatoria, e della consultazione preventiva (eventuale), che aggiunge una valutazione del rischio esterna da parte delle Autorità di controllo.

3.5 L'obbligo di conformità al Regolamento

Come già detto, gli obblighi derivanti dal principio di *accountability* sono due: l'obbligo di conformità al Regolamento (principi e disposizioni puntuali) e l'obbligo di essere in grado di dimostrarlo. Di seguito si procederà alla disamina del rapporto tra i due obblighi sopracitati.

Iniziando dall'obbligo di conformità al Regolamento, questo si sostanzia in un generico rispetto di tutti i principi e gli obblighi imposti al titolare (o responsabile ove nominato) dal Regolamento. Di seguito si

[458] Mantelero A., *La gestione del rischio*, 2019, pag. 500.

[459] Nelle Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679, si è stabilito quando è necessaria la consultazione all'Autorità di controllo (pag. 22 del documento in italiano). Le linee guida sono disponibili online al seguente link:

https://ec.europa.eu/newsroom/article29/items/611236

[460] Mantelero A., *La gestione del rischio*, 2019, pag. 514.

[461] Ibidem, pag. 515.

[462] Si noti che molto spesso è il responsabile del trattamento ad occuparsi della gestione del rischio, in quanto per codeste operazioni è prassi nominare persone giuridiche esterne: vedasi Mantelero A., *La gestione del rischio*, 2019, pag. 515.

analizzano, senza pretesa di esaustività, alcuni tra gli obblighi in cui è più evidente la filosofia dell'*accountability*. Come primo esempio si prenda l'articolo 7 del Regolamento (rubricato «condizioni per il consenso»): «qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali».

Lo spirito dell'*accountability* si rinviene se si esamina la succitata norma alla luce della previgente disciplina. Ai sensi della Direttiva madre difatti il consenso andava documentato per iscritto (e nel caso di trattamento di dati sensibili anche manifestato per iscritto) e non vi era dunque spazio per una possibile valutazione del titolare del trattamento circa le migliori modalità attraverso cui documentare il consenso. Ad oggi invece, la norma non prevede più un'indicazione specifica in merito alle regole da attuare (es. per iscritto come prima), ma sarà onere del titolare individuare il miglior mezzo per adempiere a tale obbligo[463]. A tal proposito, sebbene il requisito della documentazione per iscritto sia venuta meno, esso rimane attuale, poiché assiste il titolare del trattamento in uno dei suoi aspetti principali, quello della dimostrazione[464]. Procedendo, si esamini il primo paragrafo dell'articolo 12 (rubricato «informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato»), secondo cui:

> «Il titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni di cui agli articoli 13 e 14 e le comunicazioni di cui agli articoli da 15 a 22 e all'articolo 34 relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori. Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici. Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato»[465].

Il disposto sopracitato, in ben tre occasioni lascia ampio margine di scelta al titolare del trattamento: *in primis* quando stabilisce che deve adottare «misure appropriate»; la seconda e la terza volta si lascia al titolare la scelta dei mezzi attraverso i quali identificare l'interessato e fornirgli le informazioni[466]. Sarà poi onere del titolare fornire la prova di aver operato

[463] Finocchiaro G., *Il principio di accountability*, 2019, pag. 2780.

[464] D'Ottavio A., *Ruoli e funzioni privacy principali ai sensi del regolamento*, in Panetta R., *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, 2019, pag. 151.

[465] GDPR.

[466] Amore G., *Fairness, Transparency e Accountability nella protezione dei dati personali*, 2020, pag. 422; Borrillo B., *La tutela della privacy e le nuove tecnologie: il principio di accountability e le sanzioni inflitte dalle Autorità di controllo dell'Unione europea dopo l'entrata in vigore del GDPR*, 2020, pag. 350; Finocchiaro G., *Il principio di* accountability, 2019, pag. 2780.

tali scelte in modo tale da garantire i diritti dell'interessato. La disposizione in questione si trova nel capo III, sezione 1, rubricata «trasparenza e modalità»; essa, unitamente all'articolo 5, paragrafo 1, lettera a («trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza») e al paragrafo 2 che prevede l'obbligo di dimostrazione, fornisce alcune coordinate relative al principio di trasparenza, che rappresenta un cardine importante del più generale principio di accountability[467].

Proseguendo, il secondo paragrafo dell'articolo 17 (inerente al diritto di cancellazione), prevede:

> «Il titolare del trattamento, se ha reso pubblici dati personali ed è obbligato, ai sensi del paragrafo 1, a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione adotta le misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali».

Risulta evidente l'ampia discrezionalità concessa al titolare nella valutazione tecnica del contesto tecnologico in cui si svolge il trattamento. A questa si aggiunge una valutazione di tipo economico, relativa alla opportunità di apprestare solo le misure ragionevolmente proporzionate ai costi sostenibili[468]. La responsabilizzazione del titolare emerge anche dal disposto dell'articolo 28, il quale stabilisce che:

> «Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre 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».

---

[467] «Il principio di accountability è un principio di effettività di garanzia verso l'interessato che implica la massima trasparenza», Riccio G. M., Scorza G., Belisario E. (a cura di), *GDPR e normativa privacy*, 2018, pag. 241.

In modo diverso, il citato Parere 3/2010 del Gruppo di lavoro *ex* articolo 29 sul principio di responsabilità, pag. 14: «la trasparenza è parte integrante di molte misure concernenti responsabilità. La trasparenza nei confronti degli interessati e del pubblico in generale contribuisce alla responsabilità dei responsabili del trattamento. Per esempio, un maggiore livello di responsabilità si consegue pubblicando su Internet le politiche in materia di privacy, fornendo trasparenza riguardo alle procedure interne di gestione dei reclami, e attraverso la pubblicazione di relazioni annuali». Ancora, «la trasparenza è intrinsecamente legata sia a queste regole che, in particolare, ai principi di correttezza ed *accountability*», Giovannangeli S. F., *L'informativa agli interessati e il consenso al trattamento*, 2019, pag. 139.

[468] Amore G. *Fairness, Transparency e Accountability nella protezione dei dati personali*, 422.

Il riferimento alle «garanzie sufficienti» rimette interamente in capo al titolare la scelta del possibile responsabile. Non sono richieste competenze minime, il che rende ampiamente discrezionale la scelta del responsabile (da rammentare che un eventuale danno causato dal responsabile del trattamento potrebbe causare una corresponsabilità del titolare, in virtù della c.d. *culpa in eligendo* e *in vigilando* di cui è gravato, ma di cui si dirà meglio nel prossimo capitolo).

La norma sulla *data security* è impressa nell'articolo 32 (rubricato «sicurezza del trattamento»), che stabilisce:

> «Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso: la pseudonimizzazione e la cifratura dei dati personali; …».

Il medesimo *design* legislativo lo si ritrova qui: si impone al titolare del trattamento di effettuare delle valutazioni di natura diversissima tra loro, che recano anche un certo grado di tecnicismo[469]. L'importanza della norma si ritrova nella rottura con la previgente disciplina, che come già detto imponeva delle misure minime di sicurezza all'Allegato B al vecchio codice privacy. Il cambio di paradigma è evidente: quei vincoli minimi sono stati sostituiti da una grande libertà di scelta, solo in parte orientata da misure che vengono proposte, incoraggiate, ma non imposte (come la pseudonimizzazione e la crittografia).

Secondo chi scrive, una delle norme più emblematiche è poi l'articolo 35, secondo cui:

> «Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi».

La norma presenta una struttura simile a quella degli articoli 24, 25 e 32; difatti impone di esaminare determinati fattori, quali ad esempio «…l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità

[469] Amore G., *Fairness, Transparency e Accountability nella protezione dei dati personali*, 2020, pag. 422.

del trattamento…». La valutazione d'impatto è una delle norme in cui emerge maggiormente il principio di *accountability*[470], in quanto ad una grande discrezionalità si contrappone una responsabilità più rigorosa. In sede di attribuzione e misurazione della responsabilità da trattamento illecito infatti, si valutano, *ex* articolo 83, le misure «adottate dal titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati». Una mancata valutazione d'impatto nei casi in cui è richiesta, sarà idonea ad aggravare la posizione del titolare del trattamento.

Nella disposizione in esame emerge la volontà del Legislatore europeo di imporre agli attori del trattamento una valutazione *ex ante* dei possibili rischi verificabili, sempre a conferma della volontà di instaurare una tutela quanto più preventiva possibile, accompagnata comunque da una di tipo riparatore (si è detto dei maggiori poteri attribuiti dal GDPR alle autorità di controllo nel paragrafo 2 del capitolo 2).

3.6 L'obbligo di dimostrabilità

Il secondo obbligo derivante dal principio di *accountability* è quello di essere in grado di dimostrare di aver adottato misure adeguate a garantire la conformità ai principi e alle diverse disposizioni del Regolamento. Ciò è previsto dagli articoli 5 paragrafo 2, e 24 del Regolamento. A ciò si aggiunge quanto sancito dal considerando 74, secondo cui va dimostrata l'efficacia delle misure adottate.

Come si è detto, queste devono succedere ad un'attenta valutazione delle circostanze del caso concreto, con una particolare attenzione ai profili di rischio. Si precisa che non dovrà essere dimostrata solo l'esistenza di una misura volta a conformare il trattamento al Regolamento, ma anche il processo decisionale complessivo di cui essa è risultato[471]. Le autorità non sono gli unici soggetti cui il titolare deve dimostrare la conformità al Regolamento; essa andrà comprovata anche dinanzi all'interessato[472].

[470] Tosi E., *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale*, 2019, pag. 40; «tra gli strumenti che garantiscono l'*accountability* del titolare del trattamento risiedono la nomina, il ruolo e la funzione del DPO, gli obblighi di *privacy-by-design* e *privacy-by-default,* l'identificazione delle misure di sicurezza adeguate, la perimetrazione intelligente dei presupposti giuridici del trattamento e delle politiche di *retention* da iscrivere nel registro dei trattamenti, ma il più importante di tutti è la "Valutazione di Impatto per la Protezione dei Dati" (detta anche la *Data Protection Impact Assessment* — DPIA)», Panetta R., *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, 2019, pag. 26.

[471] Finocchiaro G., *Il principio di accountability*, 2019, pag. 2782; Tosi E., *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale*, 2019, pag. 129.

[472] Bieker F., *The Right to Data Protection*, 2022, pag. 32; Docksey C., *Article 24. Responsability of the controller*, 2020, pag. 562.

Procedendo, il Regolamento, in linea con lo spirito dell'*accountability*, non definisce cosa sia necessario per dimostrare la suddetta conformità, in quanto questa varierà in virtù delle circostanze del singolo caso, non prevedibili a monte dal legislatore[473] (si è visto a proposito, l'esempio dell'articolo 7 relativo alle modalità attraverso cui provare di aver ottenuto il consenso dell'interessato). A proposito di ciò il Gruppo di lavoro *ex* articolo 29, nel parere numero 3 del 2010, affermava che vi sono dei casi in cui la dimostrazione della corretta applicazione delle misure non richiede particolari sforzi, come nel caso della creazione di un registro relativo alle risorse umane; in altri casi invece, come quando si usano innovativi dispositivi biometrici, potrebbe essere richiesto un impegno di dimostrazione maggiore, consistente ad esempio nel fornire la prova della nomina di personale specializzato, o di una valutazione d'impatto *ex* articolo 35 del Regolamento[474].

L'articolo 24 paragrafo 3 e il considerando numero 77 prevedono dei mezzi di dimostrazione della conformità al Regolamento (codici di condotta[475] *ex* articolo 40, meccanismi di certificazione[476] *ex* articolo 42 e linee guida fornite dal Comitato europeo per la protezione dei dati), proponendoli come opzioni (privilegiate), e non come mezzi minimi, o necessari, o sufficienti[477]. Il titolare sarà difatti libero di farne a meno e di procedere mediante ulteriori mezzi di dimostrazione. Particolare mezzo utile alla conformità al Regolamento è poi il registro dei trattamenti previsto dall'articolo 30[478], il quale secondo la lettera della norma è obbligatorio per le imprese e le organizzazioni con più di 250 dipendenti. Il registro è uno strumento volto a garantire il principio di trasparenza previsto all'articolo 5, in quanto rende dimostrabile in ogni momento tutto quanto indicato dall'articolo 30 GDPR (dalle finalità del trattamento ai mezzi utilizzati, dalle categorie dei dati interessati alle misure di sicurezza apprestate ecc.)[479]. La trasparenza è chiaramente un elemento

[473] Docksey C., *Article 24. Responsability of the controller*, 2020, pag. 562.

[474] Parere 3/2010 del Gruppo di lavoro *ex* articolo 29 sul principio di responsabilità, pag. 14.

[475] In particolare, in merito ai codici di condotta, l'ultima parte del considerando numero 98 recita: «…In particolare, tali codici di condotta potrebbero calibrare gli obblighi dei titolari del trattamento e dei responsabili del trattamento, tenuto conto del potenziale rischio del trattamento per i diritti e le libertà delle persone fisiche».

[476] «Sulla scia del risk based approach, le certificazioni previste dall'art. 42 costituiscono uno strumento a disposizione del titolare del trattamento per valutare l'adeguatezza degli standards adottati», Amore G., *Fairness, Transparency e Accountability nella protezione dei dati personali*, 2020, pag. 426.

[477] A proposito di questi strumenti, è stato sottolineato che: «*the GDPR opens the demonstration of compliance to private actors by promoting private third-party bodies to design and manage codes of conduct and certification mechanisms under the oversight of the supervisory authorities*», Lachaud E., *Accountability and Certification in the GDPR*, 2021, pag. 6.

[478] Mantelero A., *La gestione del rischio*, 2019, pag. 504 e ss.

[479] «Si badi bene che l'obbligo normativo di tenuta dei registri, nonostante sia riservato solo a determinate realtà aziendali (cfr. art. 30, par. 5), in concreto si estende a

cardine della dimostrabilità e quindi del principio di *accountability*. Il succitato obbligo di dimostrazione, nelle sue più libere modalità, ha condotto ad un cambiamento del ruolo dell'autorità garante. Difatti, questa adesso non potrà più limitarsi a verificare la formale applicazione di una misura, ad esempio la pseudonimizzazione; dovrà invece valutare tutte le circostanze nel cui contesto quella misura è stata adottata, in modo da verificarne l'adeguatezza[480].

Sempre in merito al ruolo delle autorità di controllo rispetto al principio di *accountability*, alla maggiore libertà di scelta accordata dal suddetto principio sono state contrapposte aggravate sanzioni amministrative comminabili dal Garante (e dell'Edpb), che oggi, in forza dell'articolo 83 del Regolamento possono raggiungere i 20 milioni di euro o il 4% del fatturato mondiale annuo dell'impresa[481].

Il principio di *accountability* così descritto può essere interpretato come un principio che comprende reattività, trasparenza e responsabilità[482].

La trattazione del principio di accountability non è comunque finita. Nel prossimo capitolo si evidenzieranno importanti aspetti relativi al rapporto tra *accountability* e il regime di responsabilità delineato dall'articolo 82 del Regolamento. Si è però ritenuto opportuno esporre dapprima il principio di *accountability* e il regime di responsabilità, e solo in un secondo momento evidenziarne il legame.

tutti coloro che effettuano attività di trattamento, avendo il predetto principio di dimostrabilità, su cui si fonda l'intera normativa, una portata ampia e generale», Riccio G. M., Scorza G., Belisario E. (a cura di), *GDPR e normativa privacy*, 2018, pag. 241.

[480] Finocchiaro G., *Il principio di accountability*, 2019, pag. 2783.

[481] Panetta R., *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, 2019, pag. 6.

[482] Docksey C., *Article 24. Responsability of the controller*, 2020, pag. 561.

Capitolo 4 – La responsabilità civile da illecito trattamento dei dati personali

Nel presente capitolo si illustrerà il regime di responsabilità civile delineato dal Regolamento in caso di trattamento illecito di dati personali. Dopo una breve introduzione con esposizione degli elementi principali della disciplina apprestata dalla Direttiva madre e dalla normativa nazionale d'attuazione, si procederà alla disamina delle norme previste dal Regolamento. La discussione sulla responsabilità si articolerà attraverso la trattazione degli elementi principali dell'istituto: profili soggettivi, oggettivi, individuazione della natura e dei limiti della responsabilità, con conseguenti danno risarcibile ed onere probatorio.

La norma principale in tema di responsabilità civile da trattamento illecito di dati personali prevista dal GDPR è l'articolo 82[483]. Preliminarmente occorre sottolineare come la questione relativa alla responsabilità è una di quelle che impegna maggiormente l'interprete. Difatti, pur essendo direttamente applicabile[484], il Regolamento non è bastevole ai fini di un'applicazione pratica del regime di responsabilità in tutti i suoi aspetti, in quanto mancano diverse indicazioni. La dottrina si è profusa per delineare le caratteristiche principali dei vari regimi di responsabilità: in Italia si distingue tra responsabilità da inadempimento, precontrattuale e da illecito; tra responsabilità oggettiva, aggravata e soggettiva, con importanti conseguenze pratiche[485]. Indicazioni queste, che mancano nel Regolamento, in quanto attraverso di esso si è preferito fissare solo gli elementi essenziali

[483] Bolognini L., Pelino E., *Codice della disciplina privacy*, 2019, pag. 441.

[484] Zanfir-Fortuna G., *Article 82. Right to compensation and liabilty*, in Kuner C., Bygrave L. A., Docksey C., Drechsler L., *The EU General Data Protection Regulation (GDPR): A Commentary,* 2020, pag. 1163.

[485] Alpa G., Manuale di diritto privato, Wolters Kluwer Italia, Milano, 2020; Barcellona M., *Trattato della responsabilità civile*, Wolters Kluwer Italia, Milano, 2011; Bianca C. M., *Diritto civile. La responsabilità*, Giuffrè Francis Lefebvre, Milano, 2021; Bigliazzi Geri L., Breccia U., Busnelli F.D., Natoli U., *Diritto civile*, Utet, Torino, 1991; Castronovo C., Mazzamuto S., *Manuale di diritto* privato, Giuffrè Editore, Milano, 2007; Franzoni M., *L'illecito*, Giuffrè editore, Milano, 2004; Gazzoni F., *Manuale di diritto privato*, Edizioni Scientifiche Italiane s.p.a., Napoli, 2021; Mazzamuto S., *Manuale di diritto privato*, G. Giappichelli Editore, Torino, 2019; Mazzamuto S., *Il contratto di diritto europeo*, G. Giappichelli Editore, Torino, 2020; Mengoni L., *Obbligazioni di mezzi e obbligazioni di risultato*, Rivista di diritto commerciale, fascicolo 5-6, 1954; Torrente A., Schlesinger P., *Manuale di diritto privato*, Giuffrè Francis Lefebvre, Milano, 2019; Trimarchi P., *Rischio e responsabilità oggettiva*, Giuffrè, Milano, 1961; Trimarchi P., *La responsabilità civile: atti illeciti, rischio, danno*, Giuffrè, Milano, 2021; Venezian G., *Danno e risarcimento fuori dei contratti*, Opere giuridiche, volume 1, Roma, 1919.

della disciplina, tenendo in considerazione le possibili divergenze presenti negli Stati membri. Le distinzioni suddette non sono mere ripartizioni teoriche. Dall'una o l'altra applicazione discendono infatti importanti conseguenze pratiche. Ecco, dunque, il ruolo dell'interprete: ricostruire il regime di responsabilità partendo da quanto stabilito dal Regolamento, per poi integrare con la normativa nazionale compatibile.

Prima di procedere all'analisi degli articoli del GDPR, si ritiene opportuno esaminare brevemente quanto stabilito dalla previgente Direttiva madre e la relativa disciplina di attuazione nazionale italiana.

4.1 Disciplina previgente

4.1.1 Direttiva madre

La Direttiva madre concentrava nel solo articolo 23 il regime di responsabilità in caso di illecito trattamento dei dati personali. La norma prevedeva quanto segue:

> «gli Stati membri dispongono che chiunque subisca un danno cagionato da un trattamento illecito o da qualsiasi altro atto incompatibile con le disposizioni nazionali di attuazione della presente direttiva abbia il diritto di ottenere il risarcimento del pregiudizio subito dal responsabile del trattamento.
>
> Il responsabile del trattamento può essere esonerato in tutto o in parte da tale responsabilità se prova che l'evento dannoso non gli è imputabile».

Innanzitutto, è possibile notare come l'unico soggetto gravato da responsabilità fosse il responsabile del trattamento (il titolare secondo la lettera del GDPR), e ciò seppur fosse previsto dall'articolo 16 che anche l'incaricato (l'attuale responsabile secondo il GDPR) potesse, secondo le istruzioni del responsabile, trattare i dati personali.

Secondo dottrina europea, l'articolo 23, nella parte in cui stabiliva che il risarcimento fosse dovuto dal titolare ogni qualvolta vi fosse un danno derivante da un trattamento illecito o da qualsiasi altro atto incompatibile con le disposizioni nazionali di attuazione della presente direttiva, prefigurava una responsabilità non fondata sul generale principio della colpa (*strict liability*), in quanto non si richiedeva un'indagine in merito al dolo o alla colpa del danneggiante[486]. Conseguentemente, si affermava che il titolare non potesse liberarsi dall'obbligo se non allegando cause di forza

[486] *«…the escape clause of article 82(3) still refers exclusively to "events beyond control", i.e. an abnormal occurrence which cannot be averted by any reasonable measures and which does not constitute the realisation of the risk for which the person is strictly liable*», Van Alsenoy B., *Liability under EU Data Protection Law*, Jipitec, 2016, pag. 273.

maggiore o il caso fortuito, anche perché il considerando numero 55 esemplificava la prova liberatoria della forza maggiore e del fatto dell'interessato[487].

Per quanto concerne invece l'onere probatorio del soggetto danneggiato, individuato con l'espressione «chiunque», questi doveva dimostrare: l'esistenza di un trattamento illecito, ossia non conforme alla Direttiva; l'esistenza di un danno subito, e il nesso causale tra la violazione della norma operata dal titolare del trattamento e il danno subito[488].

Il rapporto che si instaurava mediante il trattamento veniva dai più classificato come extracontrattuale[489].

4.1.2 Codice privacy

Per quanto concerne la normativa italiana in attuazione della Direttiva madre, venne approvata dapprima la legge numero 675 del 1996, ed in un secondo momento il d.lgs. numero 196 del 2003 (vecchio codice privacy). Infine, in virtù dell'entrata in vigore del GDPR nel 2018, è stato approvato il d.lgs. numero 101 del 2018 (decreto di armonizzazione), con il quale si è adeguato il codice privacy al Regolamento (in seguito lo si indicherà come nuovo codice privacy).

Nel presente paragrafo si descrive brevemente quanto previsto dal vecchio codice privacy in merito alla responsabilità civile da illecito trattamento di dati personali, in ottemperanza alla Direttiva madre [490].

La norma di riferimento era l'articolo 15[491], il quale, in linea con il disposto dell'articolo 18 della legge 675 del 1996[492], prevedeva che:

---

[487] Considerando numero 55 della Direttiva madre: «considerando che, in caso di violazione dei diritti delle persone interessate da parte del responsabile del trattamento, le legislazioni nazionali devono prevedere vie di ricorso giurisdizionale; che i danni cagionati alle persone per effetto di un trattamento illecito devono essere riparati dal responsabile del trattamento, il quale può essere esonerato dalla propria responsabilità se prova che l'evento dannoso non gli è imputabile, segnatamente quando dimostra l'esistenza di un errore della persona interessata o un caso di forza maggiore…».

[488] Van Alsenoy B., *Liability under EU Data Protection Law*, 2016, pag. 274.

[489] «*Considering its characteristics, the controller's civil liability according to art. 23 of Data Protection Directive is a non-contractual liability for violation of law/a tort liability with an optional, relatively open rule concerning liability exoneration reversing the burden of proof in favor of the victim*», Kosmides T., *The legal nature of the controller's civil liability according to art. 23 of Directive 95/46 EC (Data Protection Directive)*, Atene, 2013, pag. 7.

[490] Per un inquadramento storico e sistematico degli avvenimenti che hanno condotto alle prime previsioni legislative in tema di risarcimento del danno da illecito trattamento vedasi Italia V., *Codice della privacy*, 2004, pag. 198 e ss.

[491] Oggi abrogato per via dell'articolo 27, lettera a, punto 2 del decreto di armonizzazione.

[492] L'articolo 18 stabiliva: «chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile». Per un'analisi del regime di responsabilità apprestato dalla legge 675 del 1996

«Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile.

Il danno non patrimoniale è risarcibile anche in caso di violazione dell'articolo 11».

Per quanto concerne i profili soggettivi, l'espressione «chiunque cagiona danno…» portava ad affermare che potesse essere chiamato a risarcire il nocumento chiunque avesse concorso o cagionato interamente il danno derivante dal trattamento, financo dunque il produttore del *software* o dell'*hardware*[493]. Rispetto alla Direttiva madre, si evidenziava un ampliamento della categoria dei soggetti nei cui confronti poteva richiedersi il risarcimento del danno[494]. Dall'altro lato del rapporto, il legittimato attivo all'azione di risarcimento poteva essere chiunque avesse sofferto il danno, a prescindere dal suo rapporto con il danneggiante[495].

Il vecchio codice, nel ricondurre le attività di trattamento dei dati personali nell'alveo dell'articolo 2050 c.c., operava un collegamento con le attività pericolose del codice civile[496]; prevedeva inoltre la risarcibilità del danno non patrimoniale, ricollegandosi tacitamente all'articolo 2059 del codice civile.

La scelta dell'articolo 2050 c.c.[497] si spiegava con la volontà di concedere al danneggiato una maggiore tutela, in quanto, in questo modo, questo godeva di un percorso processuale più agevole, non dovendosi più preoccupare di provare il dolo o la colpa del danneggiante[498], ma solo l'evento dannoso e il nesso di causalità con la condotta del titolare del trattamento. A causa del rimando all'articolo 2050 c.c., la dottrina e la giurisprudenza prevalenti ammesso come prova liberatoria solo il caso

---

vedasi Cuffaro V., D'Orazio R., Ricciuto V., *Il codice del trattamento dei dati personali*, 2006, pag. 119.

[493] Sica S., Stanzione P., *La nuova disciplina della privacy*, 2005, pag. 68.

[494] Cuffaro V., D'Orazio R., Ricciuto V., *Il codice del trattamento dei dati personali*, 2006, pag. 156.

[495] Ibidem, pag. 157.

[496] Per il dibattito in merito alla riconduzione delle attività di trattamento dei dati personali alle attività pericolose si rimanda a Bianca C. M., *La protezione dei dati personali*, Cedam, Padova, 2007, pag. 380; Cuffaro V., D'Orazio R., Ricciuto V., *Il codice del trattamento dei dati personali*, 2006, pag. 159; Tosi E., *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale*, 2019, pag. 112.

[497] La disposizione prevede: «chiunque cagiona danno ad altri nello svolgimento di un'attività pericolosa, per sua natura o per la natura dei mezzi adoperati, è tenuto al risarcimento, se non prova di avere adottato tutte le misure idonee a evitare il danno».

[498] Bilotta F., *La responsabilità civile nel trattamento dei dati personali*, 2019, pag. 449; Tosi E., *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale*, 2019, pag. 31.

fortuito, la forza maggiore, e il fatto del terzo o del danneggiato[499]; altri, in termini diversi, richiedevano la dimostrazione di aver adottato tutte le misure idonee[500]. Non mancavano soluzioni miste[501], ma emergeva un orientamento generalmente condiviso nella direzione di una responsabilità tendenzialmente oggettiva, inquadrata in un rapporto extracontrattuale[502].

In questa brevissima retrospettiva rimane da sottolineare il disposto del secondo paragrafo dell'articolo 15 del vecchio codice privacy; questo prevedeva il risarcimento del danno non patrimoniale in caso di trattamento in violazione dei principi generali previsti dall'articolo 11[503], e la non utilizzabilità degli stessi dati.

4.2 Profili soggettivi

4.2.1 Titolare del trattamento

Si riporta adesso l'attenzione sul Regolamento, avviando l'analisi della responsabilità da illecito trattamento dei dati personali dai relativi profili soggettivi, attivi e passivi. Il primo paragrafo dell'articolo 82 del GDPR si occupa della questione, indicando i legittimati passivi dell'azione risarcitoria, ossia il titolare ed il responsabile del trattamento (protagonisti attivi del trattamento), e quelli attivi, individuati con l'espressione generica «chiunque subisca un danno…».

Prendendo dapprima in considerazione i protagonisti attivi del trattamento, a differenza di quanto precedentemente previsto dal vecchio

[499] *Ex multis* vedasi Alpa G., Conte G., (a cura di), *La responsabilità d'impresa*, Giuffrè Editore, Milano, 2015, pag. 670; Finocchiaro G., Delfini F., (a cura di), *Diritto dell'informatica*, Wolters Kluwer Italia, Milano, 2014, pag. 831; Cuffaro V., D'Orazio R., Ricciuto V., *Il codice del trattamento dei dati personali*, 2006, pag. 157.

[500] Finocchiaro G., *Privacy e protezione dei dati personali*, 2012, pag. 277.

[501] Sica S., Stanzione P., *La nuova disciplina della privacy*, 2005, pag. 70.

[502] Tosi E., *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale*, 2019, pag. 32. Gli autori sin qui citati, pur proclamando l'oggettività della natura della responsabilità da trattamento illecito, intendono indicare la mera impossibilità per il titolare del trattamento di liberarsi dimostrando l'assenza di colpa. La responsabilità oggettiva pura non ammette prova liberatoria: se ne parlerà più diffusamente al paragrafo 4.4.1.

[503] L'articolo 11 stabiliva che «i dati personali oggetto di trattamento sono: a) trattati in modo lecito e secondo correttezza; b) raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi; c) esatti e, se necessario, aggiornati; d) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati; e) conservati in una forma che consenta l'identificazione del l'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati. I dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati».

codice privacy e similmente a quanto sancito dalla Direttiva madre[504], i soggetti responsabili sono oggi, ai sensi dell'articolo 82 GDPR, il titolare ed il responsabile del trattamento. Il titolare del trattamento è, ai sensi dell'articolo 4 GDPR:

> «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».

Le ragioni di una così ampia definizione[505] sono da rinvenire nel fatto che il legislatore europeo non abbia voluto limitare in alcun modo il novero di soggetti qualificabili come titolari. Come statuito dalla più recente giurisprudenza di legittimità, la qualifica soggettiva di titolare del trattamento si deve in virtù della concreta attività svolta, dunque in base alla determinazione delle finalità e dei mezzi del trattamento, e non sulla base di eventuali accordi privatistici[506]. Con finalità ci si riferisce alle ragioni che conducono il titolare a trattare quei dati personali; per mezzi, invece, i «*tools and instruments*» che vengono utilizzati per quel trattamento[507].

Ai sensi dell'articolo 28 paragrafo 1, il titolare può nominare un responsabile del trattamento tra i soggetti che presentino «garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate» al fine di assicurare la conformità del trattamento al Regolamento. Il responsabile del trattamento è, ai sensi dell'articolo 4 del GDPR, la «persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento».

Secondo alcuni commentatori, il rapporto che lega titolare e responsabile ha natura contrattuale, in quanto, ai sensi dell'articolo 28 paragrafo 3, questi sono legati in forza di un contratto «o altro atto giuridico a norma del diritto dell'Unione o degli Stati membri»[508]; nell'atto andrà

---

[504] «L'art. 23, direttiva 46/95/CE identificava, invece, nel solo titolare (responsabile, secondo la terminologia comunitaria) il soggetto responsabile; l'art. 15 Codice della Privacy, invece, prevedeva un principio di atipicità soggettiva (denotata dall'utilizzo del pronome "chiunque"), senza specificare lo status soggettivo o il ruolo concretamente rivestito dal danneggiante», Riccio G. M., Scorza G., Belisario E. (a cura di), *GDPR e normativa privacy*, Ipsoa, Milano, 2022, pag. 724.

[505] Per le problematicità derivanti dall'ampiezza della definizione vedasi Wong B., *Problems with controller-based responsability in EU data protection law*, International Data Privacy Law, volume 11, numero 4, 2021, pag. 382.

[506] Cassazione, Sezione I, ordinanza del 26 Aprile 2021, numero 11020.

[507] Inacio I., Silveira e Silva V., *The liability of data controllers/of data processors*, 2020, pag. 6.

[508] Un esempio è costituito dal contratto di *outsourcing*: per un inquadramento dei ruoli in questo tipo contrattuale alla luce della Direttiva madre vedasi Mantelero A., *Processi*

sempre indicata 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»[509]. Il secondo paragrafo dell'articolo 82 del GDPR è dedicato alla distinzione delle due responsabilità: il titolare del trattamento è responsabile nel caso in cui un suo trattamento in violazione del Regolamento abbia causato un danno. Il responsabile del trattamento, diversamente, risponde del danno causato dal trattamento in soli due casi: o «se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento», o nel caso in cui «ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento». Ciò significa che, in questi due casi, i soggetti danneggiati da tale inadempimento potranno rivolgersi direttamente nei confronti del responsabile del trattamento[510].

Ai sensi dell'articolo 28 paragrafo 1 del GDPR, la nomina di uno o più responsabili è rimessa alla discrezionalità del titolare del trattamento. Questa è una delle misure organizzative adeguate che il titolare può (ed in certi casi deve) apprestare per garantire la conformità del trattamento al Regolamento ai sensi dell'articolo 24 GDPR[511]. In virtù di ciò, versa in capo al titolare del trattamento una responsabilità per *culpa in eligendo* e *in vigilando*, che si attiverà qualora il responsabile, attenendosi alle legittime direttive del titolare, dovesse cagionare un danno a terzi a causa della sua negligenza, incompetenza o imperizia[512]. Per evitare di incappare nella responsabilità *in eligendo*, il titolare dovrà autorizzare al trattamento soltanto soggetti in grado di garantire che il trattamento si svolga in conformità al Regolamento, e dovrà impartire loro direttive documentate (attraverso contratto o altro atto giuridico di designazione, *ex* articolo 28 paragrafo 3) che consentano a questi di portare avanti il trattamento in piena rispondenza al GDPR[513]. Per evitare invece la responsabilità *in vigilando* dovrà monitorare il lavoro svolto dal responsabile del trattamento

di outsourcing informatico e cloud computing: la gestione dei dati personali ed aziendali, Il diritto dell'informazione e dell'informatica, fascicolo 4-5, 2010, pag. 680; alla vigenza del GDPR, Greco L., *L'organigramma privacy: i soggetti del trattamento*, 2019, pag. 344.

[509] Articolo 28 paragrafo 3 GDPR.

[510] In questi casi si parla di responsabilità diretta del responsabile. Vedasi Ratti M., *La responsabilità da illecito trattamento dei dati personali*, in Finocchiaro G., *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, 2019, pag. 776.

[511] Ai sensi del considerando numero 81, il titolare del trattamento dovrà nominare responsabili del trattamento «che presentino garanzie sufficienti, in particolare in termini di conoscenza specialistica, affidabilità e risorse».

[512] Tosi E., *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale*, 2019, pag. 60; vedasi anche Greco L., *L'organigramma privacy: i soggetti del trattamento*, 2019, pag. 334.

[513] Tosi E., *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale*, 2019, pag. 61.

e correggerlo in caso di errori; oppure dovrà dimostrare che il responsabile abbia occultato la propria attività così da impedire un'effettiva vigilanza[514].

Qualora si verificassero queste ipotesi di responsabilità (responsabile non idoneo cagiona un danno), il danneggiato potrà rivolgersi direttamente nei confronti del titolare o contro il responsabile del trattamento, e questi, dopo aver risarcito per intero il danno, potrà rivalersi sull'altro soggetto responsabile. Tale conclusione si spiega leggendo il combinato disposto dei commi 4 e 5 dell'articolo 82 GDPR.

Il quarto paragrafo dell'articolo 82 prende in considerazione l'ipotesi in cui ad essere responsabili siano sia il titolare che il responsabile, oppure più titolari o responsabili. In questi casi ogni soggetto danneggiante è responsabile in solido per l'intero ammontare del danno. Ai sensi del quinto paragrafo poi, il soggetto che abbia pagato l'intero risarcimento, potrà agire attraverso l'azione di regresso nei confronti degli altri debitori[515] per «la parte del risarcimento corrispondente alla loro parte di responsabilità per il danno…»[516].

Dunque, questi due commi prefigurano una responsabilità solidale con relativa azione di regresso nel caso in cui vi sia corresponsabilità tra titolari e responsabili (o tra due o più titolari del trattamento, o tra due o più responsabili del trattamento)[517]. Da precisare che nel caso previsto dal paragrafo 4 dell'articolo 82, più che di responsabilità solidale in senso stretto, si dovrebbe parlare di responsabilità *pro quota*, in quanto al quinto paragrafo è prevista l'azione di rivalsa. Tale impostazione sarebbe confermata dal dettato del considerando numero 146, secondo cui il risarcimento «può essere ripartito in base alla responsabilità che ricade su ogni titolare del trattamento o responsabile del trattamento per il danno cagionato dal trattamento…»[518]. A contrario, si evince che, qualora non vi sia corresponsabilità, non vi sarà responsabilità solidale. Conseguentemente, nel caso in cui un responsabile del trattamento opportunamente scelto dal

---

[514] Ibidem, pag. 61.

[515] Ratti M., *La responsabilità da illecito trattamento dei dati personali*, 2019, pag. 782.

[516] Articolo 82 paragrafo 5 GDPR.

[517] Il 7 Marzo 2012, lo European Data Protection Supervisor rilasciava un parere sul progetto di riforma relativo alla protezione dei dati personali varato dalla Commissione. In questo (pag. 44) si leggeva: «*however, in view of the responsibility of the controller, a data subject should not have to choose between the controller and the processor. It should be possible always to address the controller, regardless of where and how the damage arose. The Regulation should provide for a subsequent settlement of the damages between the controller and the processor, once the distribution of liability among them has been clarified. The same applies to the case of multiple controllers and processors*». L'articolo 82, ai commi 4 e 5, stabilisce però una regola diversa, incompatibile con quanto affermato nel citato parere, che dunque, nella parte riportata, non può essere ritenuto applicabile. Il parere è disponibile online al seguente link:

https://edps.europa.eu/sites/default/files/publication/12-03-07_edps_reform_package_en.pdf

[518] Vedasi Bolognini L., Pelino E., *Codice della disciplina privacy*, 2019, pag. 443.

titolare dovesse cagionare un danno nell'adempimento dei suoi doveri specifici (che è una delle sue specifiche ipotesi di responsabilità ex articolo 82 paragrafo 2), sorgerà una sua responsabilità diretta: il danneggiato potrà rivolgersi direttamente nei confronti del responsabile del trattamento, che dovrà risarcire il danno. Rimarrà invece esente il titolare del trattamento[519].

Riassumendo, quando il titolare del trattamento nomina un responsabile, il titolare risponde o nel caso in cui il responsabile del trattamento cagioni un danno seguendo le sue istruzioni illegittime, o qualora esso si verifichi in quanto il responsabile non è sufficientemente preparato per adempiere alle legittime istruzioni del titolare (*culpa in eligendo*), o quando il responsabile, pur essendo professionalmente adeguato, cagiona un danno seguendo le legittime istruzioni del titolare del trattamento.

4.2.2 Contitolari

Procedendo con i profili soggettivi passivi, va esaminata la responsabilità *ex* articolo 82 dei contitolari, figura espressamente disciplinata dall'articolo 26 del Regolamento[520]. Quest'ultimo stabilisce che si è dinanzi a contitolari del trattamento quando due o più soggetti «determinano congiuntamente le finalità e i mezzi del trattamento»[521]. Mediante accordo interno, questi devono delineare le rispettive responsabilità in merito al rispetto dei precetti del Regolamento. A tal riguardo, la norma enfatizza la ripartizione delle responsabilità riguardo all'esercizio dei diritti dell'interessato e agli obblighi informativi *ex* articoli 13 e 14; la ripartizione delle responsabilità non è comunque indiscriminata, in quanto, sempre il primo paragrafo dell'articolo 26, pone un limite,

[519] Quanto detto sembra anche in linea con quanto stabilito dalla Suprema corte nella ordinanza del 23 Luglio 2021, numero 21234.

[520] L'articolo 26 recita: «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. 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. 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».

[521] Difficoltà emergono quando ad essere contitolari sono due o più persone giuridiche. In questi casi si tenta di capire se un soggetto sia contitolare in base alla regola dell'influenza. Per le consequenziali complessità vedasi Wong B., *Problems with controller-based responsability in EU data protection law*, 2021, pag. 377.

affermando che la suddivisione avviene: «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».

Data la solidarietà dell'obbligazione (articolo 82 paragrafo 4), la misura dell'attività concretamente svolta dai soggetti attivi, rileverà solamente in sede di riparto interno della responsabilità[522]. Vi sono casi, tuttavia, in un contesto con due o più titolari, in cui uno affida all'altro dei dati di modo che questi possa operare in autonomia: in un siffatto contesto, solamente quest'ultimo titolare sarà chiamato a rispondere di un eventuale danno, in quanto sarà l'unico ad aver determinato i mezzi e le finalità del trattamento[523]. Il secondo paragrafo invece prevede che l'accordo debba riflettere «adeguatamente» i ruoli e i rapporti tra i contitolari e gli interessati; inoltre, il contenuto essenziale dell'accordo[524] è messo a disposizione degli interessati. Nonostante la rilevanza assegnata dalla norma all'accordo tra i contitolari, il terzo paragrafo stabilisce che «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».

4.2.3 Responsabile del trattamento

Tra i soggetti eventualmente responsabili, l'articolo 82 del Regolamento individua anche i responsabili del trattamento. Ai sensi dell'articolo 4 GDPR, il responsabile del trattamento è «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento». Questo, come già detto, risponde solo in due casi: o «se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento», o nel caso in cui «ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento». La responsabilità diretta del responsabile è da ricondurre a queste due ipotesi. Ve ne è un'altra poi, che può essere ricompresa nella prima fattispecie menzionata, che si realizza quando il responsabile del trattamento viola il Regolamento determinando finalità e mezzi del trattamento: il paragrafo 10 dell'articolo 28 prevede che in questi casi al responsabile viene applicata la disciplina prevista per il titolare del trattamento[525]. Da ciò discende che,

[522] Caterina R., Thobani S, *Il diritto al risarcimento dei danni*, Giurisprudenza italiana, Dicembre 2019, pag. 2806.

[523] Ibidem.

[524] In dottrina si è definito accordo contrattuale, vedasi Tosi E., *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale*, 2019, pag. 62.

[525] In merito a quest'ultima ipotesi è possibile prendere in esame quanto stabilito dalla Suprema corte, la quale ha precisato che al responsabile verrà applicato il regime di regole dettate per il titolare del trattamento, comprese quelle sulla responsabilità «in ragione dell'autonomia decisionale e gestionale manifestata nell'aver disatteso le

malgrado la constatata rilevanza attribuita all'accordo che lega titolare e responsabile (ed eventualmente sub-responsabile) e alla relativa ripartizione dei ruoli, la qualifica di ogni attore si deve in base alle concrete attività realizzate[526].

Raffrontando brevemente i regimi di responsabilità cui sono tenuti il titolare ed il responsabile del trattamento, è possibile affermare che la responsabilità del primo è più ampia di quella del secondo[527]: qualora il responsabile del trattamento cagioni il danno seguendo le istruzioni legittime del titolare, non potrà essere chiamato a rispondere, in quanto tale ipotesi non è prevista tra quelle esplicitamente indicate dall'articolo 82 paragrafo 2.

Procedendo, il responsabile non può a sua volta nominare un altro responsabile (c.d. sub-responsabile), a meno che non vi sia un'autorizzazione scritta del titolare. Nel caso vi sia l'autorizzazione, al sub-responsabile si estende l'accordo (e quindi i relativi obblighi) che lega il titolare al primo responsabile. Qualora il sub-responsabile cagioni un danno in violazione del Regolamento o di altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati personali, il responsabile del trattamento ne conserva la responsabilità nei confronti del titolare del trattamento[528].

In merito all'accordo che lega titolare e responsabile, si sottolinea che da esso debba emergere il ruolo di subordinazione del responsabile rispetto al titolare[529] (l'interessato deve sempre poter sapere chi sta determinando i mezzi e le finalità del trattamento, e chi invece sta solo eseguendo istruzioni). Inoltre, l'articolo 28 paragrafo 3 GDPR prevede degli obblighi specifici in capo al responsabile del trattamento, imponendo che siano inseriti nel contratto o nell'altro accordo che lega titolare e responsabile del trattamento. La norma, in breve, prevede che il responsabile tratti i dati personali solo su istruzione documentata del titolare del trattamento; che garantisca che gli autorizzati al trattamento abbiano un adeguato accordo o obbligo legale di riservatezza; che adotti tutte le misure di sicurezza previste dall'articolo 32 del Regolamento; ricorra alle condizioni previste nei commi 2 e 4 dell'articolo 28 per ricorrere ad un altro responsabile; che assista il titolare del trattamento con misure tecniche ed organizzative adeguate,

---

disposizioni a lui impartite», Corte di Cassazione, ordinanza numero. 21234 del 23 Luglio 2021.Il provvedimento citato verte sulla individuazione degli attori del trattamento nella vigenza del codice privacy *ante* decreto di armonizzazione; si ritiene tuttavia ancora considerabile, in quanto il titolare del trattamento si distingue dal responsabile del trattamento in virtù della scelta delle finalità e dei mezzi del trattamento, comune ad entrambe le discipline.

[526] Caterina R., Thobani S, *Il diritto al risarcimento dei danni*, 2019, pag. 2806.

[527] Ibidem.

[528] Tosi E., *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale*, 2019, pag. 65; Bolognini L., Pelino E., *Codice della disciplina privacy*, 2019, pag. 443; Greco L., *L'organigramma privacy: i soggetti del trattamento*, 2019, pag. 337.

[529] Settimio R., *Obblighi e responsabilità dei soggetti del trattamento: titolare e responsabile a confronto*, GiustiziaCivile.com, 18 Marzo 2022, pag. 7, nota a: Cassazione civile, 23 luglio 2021, numero 21234, sezione I.

tenendo conto della natura del trattamento, nella misura in cui ciò sia possibile al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato; che assista il titolare nel rispetto degli obblighi ex articoli 32, 33, 34, 35 e 36 del Regolamento, tenendo conto della natura del trattamento e delle informazioni a sua disposizione; che cancelli o restituisca, su volontà del titolare, tutti i dati personali una volta terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati; informi il più possibile il titolare del trattamento in modo che possa dimostrare di aver ottemperato agli obblighi previsti ai sensi dell'articolo 28; che informi immediatamente il titolare del trattamento nel caso in cui ritenga che un'istruzione violi il presente regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati; che istituisca il registro dei trattamenti *ex* articolo 30.

Per questi specifici obblighi, il responsabile risponde in via diretta (non si configura la solidarietà con il titolare del trattamento)[530].

In conclusione, è possibile affermare che la responsabilità del titolare del trattamento sia generica, non limitata a singole ipotesi, mentre quella del responsabile sia circoscritta a determinate fattispecie specificatamente individuate[531].

4.2.4 Rappresentante del titolare o del responsabile

Per quanto concerne invece la figura del rappresentante del titolare o del responsabile, esso è definito dall'articolo 4 del Regolamento come «la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento». La norma che disciplina la sua attività è l'articolo 27 del GDPR. In questa è previsto che nel caso di titolari del trattamento stabiliti in paesi al di fuori dell'Unione, il titolare o il responsabile del trattamento devono nominare per iscritto un rappresentante dell'Unione europea. Ai sensi del paragrafo 4 dell'articolo 27, questi ha il compito di assistere o sostituire il titolare o il responsabile nel dialogo con le autorità di controllo e con gli interessati in merito ai trattamenti protratti. Specularmente, l'articolo 58 GDPR statuisce che l'autorità di controllo possa ottenere dal rappresentante tutte le informazioni utili allo svolgimento delle sue funzioni. L'articolo 30 paragrafo 1 GDPR, inoltre, prevede che il rappresentante sia tenuto alla

[530] Greco L., *L'organigramma privacy: i soggetti del trattamento*, 2019, pag. 334.

[531] Commento di Sica S., in D'Orazio R., Finocchiaro G., Pollicino O., Resta G., *Codice della privacy e data protection*, 2021, pag. 892.

predisposizione del registro dei trattamenti, insieme al titolare del trattamento[532]. In virtù di questa funzione ausiliaria[533], il rappresentante dell'Unione non viene annoverato tra i soggetti attivi del trattamento. Il considerando numero 80 precisa che questi agisce per conto del titolare o del responsabile del trattamento e che «la designazione di tale rappresentante non incide sulla responsabilità generale del titolare del trattamento o del responsabile del trattamento ai sensi del presente regolamento».

L'Edpb ha precisato che in virtù della lettura combinata del succitato considerando e dell'articolo 27 paragrafo 5, si può desumere che «il RGPD non stabilisce una responsabilità vicaria del rappresentante rispetto al titolare o al responsabile del trattamento che egli rappresenta nell'Unione»[534]. Dunque, il rappresentante del titolare o del responsabile del trattamento non risponde ai sensi dell'articolo 82 del GDPR[535].

4.2.5 Responsabile per la protezione dei dati personali (DPO)

Una delle novità fondamentali del Regolamento è poi la figura del *data protection officer*, o responsabile per la protezione dei dati personali (in

[532] Linee-guida 3/2018 sull'ambito di applicazione territoriale del RGPD (articolo 3), pag. 30: «il CEPD ritiene che, sebbene la tenuta di tale registro sia un obbligo imposto sia al titolare o al responsabile del trattamento sia al rappresentante, il titolare o il responsabile del trattamento non stabilito nell'Unione è responsabile del contenuto principale e dell'aggiornamento del registro e deve, al contempo, fornire al proprio rappresentante tutte le informazioni, precise e aggiornate, in modo che anche quest'ultimo possa tenere e rendere disponibile il registro in qualsiasi momento».

[533] «Il rappresentante non costituisce un mero soggetto ausiliario del titolare o del rappresentante, ma incorpora altresì un'importante funzione di garanzia per gli interessati. Esso è infatti un vero e proprio strumento di tutela a cui gli interessati possono far riferimento ove non sia possibile o sia eccessivamente oneroso rivolgersi al titolare o al responsabile del trattamento. Non a caso una delle poche esplicitate funzioni del rappresentante è proprio quella di fungere da interlocutore non solo delle autorità di controllo, ma anche e soprattutto degli interessati (art. 27,4° comma), così ribadendo la sua funzione di garanzia e di raccordo», Greco L., *L'organigramma privacy: i soggetti del trattamento*, 2019, pag. 340.

[534] Linee-guida 3/2018 sull'ambito di applicazione territoriale del RGPD (articolo 3), pag. 30.

[535] *Contra*, Bilotta F., *La responsabilità civile nel trattamento dei dati personali*, 2019, pag. 459.

Si è anche sostenuto che il rappresentante dell'Unione possa essere chiamato a rispondere in base alle regole sul mandato: «tuttavia, inquadrando l'istituto entro la fattispecie contrattuale del mandato, si ritiene che possano applicarsi gli artt. 1218 e 1710 c.c. Il rappresentante quindi risponderà in caso di specifiche responsabilità contrattuali inerenti al contratto con il titolare o responsabile rappresentato, nonché in caso di violazione del generale obbligo di diligenza nell'assolvimento dei suoi compiti», Greco L., *L'organigramma privacy: i soggetti del trattamento*, 2019, pag. 341.

seguito anche DPO)[536]. I riferimenti normativi sono gli articoli 37 GDPR e seguenti. Il primo paragrafo dell'articolo 37 del Regolamento prevede i casi in cui il titolare e il responsabile del trattamento devono nominare il DPO, che si sostanziano nei casi in cui ad effettuare il trattamento dei dati personali è un'autorità pubblica (eccezion fattasi per l'autorità giudiziaria) o un organismo pubblico[537]; quando si necessita un monitoraggio degli interessati su larga scala; quando occorre trattare su larga scala i dati particolari *ex* articoli 9 e 10. Tale dovere di nomina è presidiato dalla sanzione amministrativa prevista dall'articolo 83 paragrafo 4, lettera a, del Regolamento[538].

Oltre alle ipotesti obbligatorie appena viste, il Regolamento prevede dei casi in cui alcuni soggetti possono nominare facoltativamente il DPO: ad esempio, si prevede che un gruppo imprenditoriale, o un'autorità pubblica, o un organismo pubblico, possano nominare un unico DPO, purché sia facilmente raggiungibile dalle varie imprese del gruppo o dai vari organismi dell'ente pubblico (commi 2 e 3); si è sottolineato come, attraverso un ragionamento a contrario, il DPO possa essere nominato spontaneamente nel caso in cui un soggetto privato, nell'ambito della sua attività di

[536] La centralità della figura del DPO emerge subito nelle Linee guida sui responsabili della protezione dei dati del Gruppo di lavoro del Gruppo di lavoro (WP 243), adottate il 13 Dicembre 2016 ed emendate il 5 aprile 2017: «i responsabili della protezione dei dati (RPD) saranno al centro di questo nuovo quadro giuridico in molti ambiti, e saranno chiamati a facilitare l'osservanza delle disposizioni del RGPD», pag. 5. Le linee guida sono disponibili online al seguente link:

https://ec.europa.eu/newsroom/article29/items/612048/en

[537] Il GDPR non offre le definizioni di autorità ed organismo pubblico. A proposito, le FAQ sul responsabile della protezione dei dati personali fornite dal Garante italiano riportano alcuni esempi: «ad esempio, le amministrazioni dello Stato, anche con ordinamento autonomo, gli enti pubblici non economici nazionali, regionali e locali, le Regioni e gli enti locali, le università, le Camere di commercio, industria, artigianato e agricoltura, le aziende del Servizio sanitario nazionale, le autorità indipendenti ecc.). Occorre, comunque, considerare che, nel caso in cui soggetti privati esercitino funzioni pubbliche (in qualità, ad esempio, di concessionari di servizi pubblici), può risultare comunque fortemente raccomandato, ancorché non obbligatorio, procedere alla designazione di un RPD. In ogni caso, qualora si proceda alla designazione di un RPD su base volontaria, si applicano gli identici requisiti - in termini di criteri per la designazione, posizione e compiti - che valgono per i RPD designati in via obbligatoria». Le FAQ sono disponibili online al seguente link:

https://www.garanteprivacy.it/faq-sul-responsabile-della-protezione-dei-dati-rpd-in-ambito-pubblico

Sempre sullo stesso punto, le citate linee guida (WP 243), pag. 8, precisano che «il Gruppo di lavoro raccomanda, in termini di buone prassi, che gli organismi privati incaricati di funzioni pubbliche o che esercitano pubblici poteri nominino un RPD».

[538] La norma stabilisce che «in conformità del paragrafo 2, la violazione delle disposizioni seguenti è soggetta a sanzioni amministrative pecuniarie fino a 10 000 000 EUR, o per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore:

a) gli obblighi del titolare del trattamento e del responsabile del trattamento a norma degli articoli 8, 11, da 25 a 39, 42 e 43».

trattamento, non effettui trattamenti su larga scala[539]; un altro caso di nomina facoltativa è prevista dal quarto paragrafo, ed è concessa al titolare del trattamento, al responsabile del trattamento o alle associazioni e agli altri organismi rappresentanti le categorie di titolari del trattamento o di responsabili del trattamento (la nomina diviene obbligatoria se prevista dal diritto dell'Unione o degli Stati membri). Il responsabile per la protezione dei dati viene nominato in funzione delle qualità professionali in materia di protezione dei dati personali per la capacità di ottemperare ai doveri imposti dall'articolo 39, rubricato «compiti del responsabile della protezione dei dati» (articolo 37 paragrafo 5). L'ultimo paragrafo dell'articolo 37 infine statuisce che la scelta del DPO può avvenire anche al di fuori del personale dell'impresa, dando vita ad una vera e propria esternalizzazione delle funzioni tipiche del *data protection officer*[540].

Ai sensi dell'articolo 38 paragrafo 1 del Regolamento, quest'ultimo è tempestivamente reso edotto e coinvolto dal titolare e dal responsabile in merito a quanto concerne i trattamenti, e gli stessi devono garantirgli le risorse per assolvere ai compiti *ex* articolo 39 (articolo 38 commi 1 e 2).

La figura del DPO è dotata di grande autonomia e indipendenza per l'esercizio delle sue funzioni: ad esempio, nell'ambito dell'organizzazione gerarchica societaria, dovrà interfacciarsi direttamente con il consiglio d'amministrazione[541]; inoltre non potrà ricevere istruzioni in merito allo svolgimento delle sue funzioni; allo stesso tempo, tuttavia, non potrà versare in conflitto di interessi con altre aree delle realtà societarie (commi 3 e 6). Una misura posta a salvaguardia della sua indipendenza, è il divieto di rimozione o penalizzazione ad opera del titolare o del responsabile del trattamento.

Per quanto invece concerne gli obblighi specifici del DPO, l'articolo 39 prevede:

> «Il responsabile della protezione dei dati è incaricato almeno dei seguenti compiti: a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati; b) sorvegliare

[539] Gaetano G., *La mancata nomina del responsabile per la protezione dei dati personali per i soggetti privati*, Data Protection Law, Gennaio – Giugno 2021, pag. 44.

[540] Tosi E., *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale*, 2019, pag. 67

[541] Tosi E., *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale*, 2019, pag. 68; Gaetano G., *La mancata nomina del responsabile per la protezione dei dati personali per i soggetti privati*, 2021, pag. 49. *Contra*, Ricci S., Vaciago G., *Gli adempimenti del dpo*, Giuffrè Francis Lefebvre, Milano, 2019, pag. 17, secondo cui: «in via generale si può affermare che sussista un rischio di conflitto di interessi in relazione a ruoli managerali di vertice (amministratore delegato, Responsabile operativo, Responsabile finanziario, Responsabile sanitario, direttore marketing, direttore risorse umane, Responsabile IT)».

l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo; c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35; d) cooperare con l'autorità di controllo; e e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione. Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo».

Oltre ai compiti previsti dall'articolo 39 GDPR, il DPO può svolgerne degli altri. A tal proposito, il titolare ed il responsabile del trattamento devono assicurarsi che tali ulteriori compiti non diano adito ad un conflitto di interessi[542]. Tornando all'esame dei soggetti responsabili ai sensi dell'articolo 82 GDPR, il Gruppo di lavoro specifica in più punti che «il titolare del trattamento o il responsabile del trattamento mantengono la piena responsabilità dell'osservanza della normativa in materia di protezione dei dati e devono essere in grado di dimostrare tale osservanza»[543]. Si conclude affermando dunque che, anche in caso di nomina di un DPO, gli unici responsabili ai sensi dell'articolo 82 GDPR sono solo il titolare ed il responsabile del trattamento.

4.2.6 Soggetti terzi

Il decreto di armonizzazione del codice privacy, tra i molti, ha abrogato l'articolo 30, rubricato «incaricati del trattamento», che al primo paragrafo recitava: «le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite». Malgrado l'abrogazione, si può

[542] «L'articolo 39, paragrafo 1, contiene un elenco non esaustivo dei compiti affidati al RPD. Pertanto, niente vieta al titolare del trattamento o al responsabile del trattamento di affidare al RPD il compito di tenere il registro delle attività di trattamento sotto la responsabilità del titolare o del responsabile stesso», WP 243, pag. 25; Ricci S., Vaciago G., *Gli adempimenti del dpo*, 2019, pag. 18.

[543] WP 243, pag. 20. Inoltre, nell'allegato alle linee guida (pag. 33) si legge che «il RPD non è responsabile personalmente in caso di inosservanza degli obblighi in materia di protezione dei dati. Spetta al titolare del trattamento o al responsabile del trattamento garantire ed essere in grado di dimostrare che il trattamento è effettuato conformemente al regolamento. La responsabilità di garantire l'osservanza della normativa in materia di protezione dei dati ricade sul titolare del trattamento o sul responsabile del trattamento».

affermare che la suddetta categoria sia stata ripresa dall'articolo 2-*quaterdecies* del nuovo codice privacy[544], secondo cui:

> «Il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità. Il titolare o il responsabile del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta».

Questa norma è da leggere unitamente all'articolo 28 paragrafo 3, lettera b, del Regolamento, che prende in considerazione «le persone autorizzate al trattamento» (o autorizzati) e all'articolo 29, relativo a soggetti che agiscono sotto l'autorità del titolare o del responsabile. Tali soggetti autorizzati (o designati secondo la lettera del nuovo codice privacy) ricoprono la stessa qualifica propria degli incaricati previsti dall'articolo 30 del vecchio codice privacy. Ci si è chiesti chi risponda del danno cagionato da un designato: chi scrive ritiene non sia possibile considerare tali soggetti come legittimati passivi dell'azione di risarcimento per tre ordini di ragioni. La prima consegue ad un'interpretazione di tipo letterale: l'articolo 2-*quaterdecies* del nuovo codice privacy stabilisce che i designati stanno «sotto la responsabilità» del titolare o del responsabile del trattamento, ponendosi in linea con quanto stabilito dall'articolo 82 GDPR, secondo cui a rispondere sono solo il titolare e il responsabile del trattamento.

La seconda ragione si deve ad un argomento sistematico: quando voluto, il legislatore europeo ha sempre specificato il regime di responsabilità dei soggetti disciplinati (si sono analizzate poc'anzi le norme relative alla responsabilità dei titolari, contitolari, responsabili, e sub-responsabili), mentre nulla ha stabilito sui soggetti autorizzati. Inoltre, tenendo a mente il ruolo primario attribuito al titolare del trattamento[545], il

[544] La ragione la si ritrova nei lavori preparatori relativo al decreto di armonizzazione, in particolare nel dossier del Servizio Studi della Camera dei deputati (pag. 52), ove, in merito all'attuale articolo 2-*quaterdecies* del nuovo codice privacy, si afferma che «la disposizione attua in particolare quanto previsto dall'articolo 29 del Regolamento e sostanzialmente sostituisce l'attuale articolo 30 del Codice della privacy». Dossier disponibile online al seguente link:

https://documenti.camera.it/Leg18/Dossier/Pdf/gi0007.Pdf

Nello stesso senso la relazione illustrativa al nuovo codice privacy (pag.30), disponibile online al seguente link:

http://documenti.camera.it/apps/nuovosito/attigoverno/Schedalavori/getTesto.ashx?file=0022_F001.pdf&leg=XVIII#pagemode=none

[545] «…è opportuno fin d'ora evidenziare come tale figura venga oggi eretta a vero e proprio caposaldo della protezione dei dati personali. Seppur anche nelle discipline precedenti il titolare era gravato dell'obbligo di garantire la riservatezza e l'integrità dei dati, il Regolamento prevede che ora il titolare sia il primo fra tutti a doversi adoperare per

fatto che i soggetti autorizzati sono scelti ed indicati nell'accordo intercorrente tra titolare e responsabile del trattamento, e che la responsabilità del titolare è generica mentre quella del responsabile è limitata alle scelte operate a monte dal legislatore europeo nelle norme esaminate, il soggetto chiamato a rispondere degli eventuali danni causati dai soggetti autorizzati sarà solo il titolare del trattamento, senza che si prefiguri la responsabilità solidale con i soggetti designati (o autorizzati)[546]. Una tale impostazione trova conforto in quanto stabilito dall'articolo 1228 del codice civile[547], che prevede la responsabilità del soggetto che si serve di ausiliari[548].

Concludendo, si ritiene che i legittimati passivi all'azione di risarcimento *ex* articolo 82 siano soltanto i titolari ed i responsabili del trattamento[549].

4.2.7 Danneggiati

Per quanto concerne invece i soggetti danneggiati che possono richiedere il risarcimento ai sensi dell'articolo 82 del Regolamento, dalla lettera della norma («chiunque subisca un danno…») si evince come il legislatore europeo, in un'ottica di tutela, abbia preferito lasciare indefinite le categorie di soggetti protetti attraverso il risarcimento del danno. Di conseguenza, chiunque, anche qualora non rivestisse la qualifica di interessato[550], potrebbe richiedere un risarcimento in caso di danno in conseguenza della violazione del Regolamento da parte del titolare o del responsabile del trattamento. Nello stesso senso sembra il disposto del considerando numero 146, il quale prevede che «il titolare del trattamento o il responsabile del trattamento dovrebbe risarcire i danni cagionati a una persona da un trattamento…»: nessun riferimento ad una particolare categoria di soggetti.

---

garantire tutela ai dati personali e non solo durante o dopo il trattamento, bensì addirittura in una fase pregressa», Greco L., *L'organigramma privacy: i soggetti del trattamento*, 2019, pag. 324.

[546] Secondo Bolognini L., Pelino E., *Codice della disciplina privacy*, 2019, pag. 444, la responsabilità degli autorizzati può aversi, comunque, ai sensi dell'articolo 2043 c.c.

[547] La norma stabilisce che «salva diversa volontà delle parti, il debitore che nell'adempimento dell'obbligazione si vale dell'opera di terzi, risponde anche dei fatti dolosi o colposi di costoro».

[548] Nello stesso senso Bilotta F., *La responsabilità civile nel trattamento dei dati personali*, 2019, pag. 459.

[549] Così anche Tosi E., *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale*, 2019 pag. 136; *contra*, Bolognini L., Pelino E., *Codice della disciplina privacy*, 2019, pag. 441; Bilotta F., *La responsabilità civile nel trattamento dei dati personali*, 2019, pag. 459.

[550] Ratti M., *La responsabilità da illecito trattamento dei dati personali*, 2019, pag. 775; Riccio G. M., Scorza G., Belisario E. (a cura di), *GDPR e normativa privacy*, 2022, pag. 725.

Tuttavia, è stato evidenziato in dottrina come quanto appena detto possa essere messo in discussione se si analizza il tenore letterale del quarto paragrafo dell'articolo 82 GDPR, il quale, nello stabilire la responsabilità solidale dei contitolari e dei titolari e responsabili, o dei responsabili, indica come soggetto legittimato a chiedere il risarcimento solamente l'interessato[551].

Analoghe perplessità emergono qualora si prosegua la lettura del considerando numero 146: questo, mentre inizialmente non limita la platea di soggetti legittimati a chiedere il risarcimento, ad un certo punto aggiunge che «gli interessati dovrebbero ottenere pieno ed effettivo risarcimento per il danno subito»[552].

Detto ciò, chi scrive ritiene che a prescindere dalle esposte indicazioni contrarie, il legislatore europeo abbia deciso di proseguire nel solco già tracciato dalla Direttiva madre[553]; ciò sarebbe confermato dal tenore letterale dell'articolo 82 GDPR, norma fulcro dell'impianto risarcitorio. Ne discende che chiunque subisca un danno a seguito di una violazione del Regolamento abbia diritto al risarcimento del danno ex articolo 82[554].

4.3 Elemento oggettivo

L'articolo 82 paragrafo 2 del Regolamento, nello stabilire le responsabilità del titolare e del responsabile del trattamento, descrive due diverse condotte punibili, l'una del primo ed un'altra per il secondo. Il titolare del trattamento risponde del danno causato (danno materiale o immateriale, vedasi paragrafo 4.5 dedicato al tema) da un trattamento non conforme al Regolamento; il responsabile invece, sempre premesso un danno causato da un trattamento per il quale era stato nominato, risponde qualora non abbia adempiuto agli obblighi a lui assegnati dal Regolamento, o nel caso in cui non abbia ottemperato alle legittime istruzioni impartitegli dal titolare del trattamento.

Si premette subito che per trattamento in violazione del Regolamento (o trattamento illecito) si intende una condotta del titolare contraria alle

[551] Truli E., *The General Data protection Regulation and Civil Liability*, 22 Giugno 2018, pag. 24

[552] Cordeiro M., *A Civil Liability for Processing of Personal Data in the GDPR*, European Data Protection Law Review, volume 5, questione 4, 2019, pag. 495.

[553] Cuffaro V., D'Orazio R., Ricciuto V., *Il codice del trattamento dei dati personali*, 2006, pag. 157.

[554] Barbierato D., *Trattamento dei dati personali e «nuova» responsabilità civile*, Responsabilità Civile e Previdenza, fascicolo 6, 1 Giugno 2019, pag. 3; Cordeiro M., *A Civil Liability for Processing of Personal Data in the GDPR*, 2019, pag. 496; Ratti M., *La responsabilità da illecito trattamento dei dati personali*, 2019, pag. 775.

prescrizioni regolamentarie, non assistita da cause di giustificazione[555]. Il GDPR non individua puntualmente i possibili trattamenti illeciti; piuttosto, attraverso una precisa scelta legislativa, pone l'articolo 82 GDPR come norma generale della responsabilità per i danni derivanti dal trattamento dei dati personali[556]. Ai sensi del considerando numero 146 del Regolamento, un trattamento siffatto può aversi quando questo non rispetta i principi ed i precetti esecuzione adottati in conformità ad esso, e alle disposizioni del diritto degli Stati membri che specificano disposizioni dello stesso GDPR. A queste norme, si aggiungono quelle previste dai codici di condotta espressamente richiamati dal Regolamento per determinati settori (ad esempio per le misure tecniche ed organizzative *ex* articoli 24, 25 e 32 GDPR)[557].

Sia faccia adesso un breve riferimento agli obblighi del Regolamento. Per quanto concerne i principi generali, il contenuto degli articoli 5 e 6 costituisce un primo fondamentale parametro di liceità del trattamento[558]: esso dovrà dunque essere lecito, corretto, trasparente; limitato rispetto alle finalità; svolto secondo il principio di minimizzazione; esatto; limitato ai tempi di conservazione; orientato all'integrità e alla sicurezza; ed infine basato sul principio di responsabilizzazione (quest'ultimo da leggersi in combinato disposto con gli articoli 24, 25 e 32 del Regolamento). Un altro principio, desumibile dalla lettura del Regolamento, è il principio di proporzionalità[559]. Altri principi sono poi previsti da norme successive, quali il principio del consenso (articoli 7, 8 e 9 del GDPR); della *data protection by design* e *by default* (articolo 25 GDPR); della sicurezza dei dati (articolo 32 GDPR).

---

[555] Gambini M., *Responsabilità e risarcimento nel trattamento dei dati* personali, in Cuffaro V., D'Orazio R., Ricciuto V., *I dati personali nel diritto europeo*, 2019, pag. 1044; Bilotta F., *La responsabilità civile nel trattamento dei dati personali*, 2019, pag. 454. Ragionando a contrario, Calabrese G., *La responsabilità civile da illecito trattamento dei dati personali*, 2022, pag. 124 individua il trattamento lecito, ricavandone in termini negativi il modello illecito: «il GDPR sanziona la mancata assunzione di questo atteggiamento proattivo, finalizzato a custodire, gestire e trattare i dati in un'ottica prudenziale. Il titolare non deve far necessariamente prevalere il proprio interesse economico-individuale rispetto a quello degli interessati ed è responsabilizzato in tal senso: un comportamento difforme assume gli estremi della condotta illecita che può determinare danni risarcibili ex art. 82».

[556] Gambini M., *Responsabilità e risarcimento nel trattamento dei dati* personali, 2019, pag. 1033.

[557] Tosi E., *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale*, 2019, pag. 87; Gambini M., *Responsabilità e risarcimento nel trattamento dei dati* personali, 2019, pag. 1033.

[558] Gambini M., *Responsabilità e risarcimento nel trattamento dei dati* personali, 2019, pag. 1034.

[559] Tale principio è previsto nel Regolamento sotto molteplici vesti: talvolta relativo al trattamento (vedasi ad esempio gli articoli 6 paragrafo 4 e 9 paragrafo 2, lettera g e j) talaltra alle sanzioni (vedasi ad esempio l'articolo 83 paragrafo 1), ecc.

Si hanno poi i doveri conformativi, quali l'obbligo di informativa trasparente all'interessato (articoli 12, 13 e 14 del GDPR)[560]; di notifica in caso di rettifica o cancellazione dei dati personali o di limitazione del trattamento (articolo 19 GDPR); di nomina del rappresentante di titolare o responsabile del trattamento (articolo 27 GDPR); obbligo di tenuta del registro delle attività di trattamento per le imprese con più di 250 dipendenti (articolo 30 GDPR); di cooperazione con l'autorità di controllo (articolo 31 GDPR); l'obbligo di notifica al Garante e di comunicazione all'interessato di *data breach* (articoli 33 e 34 GDPR); di procedere alla valutazione d'impatto (articolo 35 GDPR); dovere di consultazione preventiva (articolo 36); doveri relativi alla nomina del DPO (articoli 37 GDPR e seguenti); al trasferimento transfrontalieri dei dati (articoli 44 GDPR e seguenti).

Vanno poi rispettati i diritti dell'interessato, quali il diritto di accesso (articolo 15 GDPR); di rettifica (articolo 16 GDPR); alla cancellazione o oblio (articolo 17 GDPR); di limitazione di trattamento (articolo 18 GDPR); il diritto alla portabilità dei dati (articolo 20 GDPR); di opposizione (articolo 21 GDPR); a non essere sottoposto ad una decisione basata unicamente su un trattamento automatizzato (articolo 22 GDPR); diritto a proporre reclamo all'autorità di controllo (articolo 77 GDPR); diritto ad un ricorso giurisdizionale effettivo nei confronti dell'autorità di controllo o del titolare o del responsabile del trattamento (articoli 78 e 79 GDPR); di rappresentanza (articolo 80 del GDPR); diritto al risarcimento del danno (articolo 82 GDPR).

Come evidenziato nel terzo capitolo, il principio cardine del Regolamento è il principio di *accountability*. Assume dunque rilevanza la dimostrabilità dell'analisi di previsione del rischio. Parimenti, l'obbligo di dimostrabilità previsto dal suddetto principio è da integrare ad ogni obbligo o principio imposto al titolare ed al responsabile del trattamento. Dinanzi all'autorità di controllo o al giudice sarà sempre necessario poter dimostrare la conformità al Regolamento.

4.4 Natura della responsabilità

Nella retrospettiva operata al paragrafo 4.1 si è detto che la maggior parte della dottrina era concorde nel qualificare la responsabilità da illecito trattamento delineata dalla Direttiva madre e dalla relativa normativa d'attuazione in termini oggettivi ed extracontrattuali. In questo paragrafo si affronterà la questione relativa alla soggettività o oggettività del criterio di

[560] «…un generale dovere di trasparenza e puntuali obblighi informativi in capo al titolare, posti, in alcuni casi, in favore dell'interessato (quali quelli disciplinati dagli artt. 13 e 14 del Regolamento, che ampliano le informazioni indicate nella Direttiva 96/46/CE e nel Codice *privacy)* per assicurare un trattamento corretto e trasparente dei suoi dati personali», Gambini M., *Responsabilità e risarcimento nel trattamento dei dati* personali, pag. 1037.

imputazione della responsabilità delineata dall'articolo 82 del Regolamento, e la sua riconducibilità al rapporto contrattuale o extracontrattuale.

4.4.1 Tra responsabilità per colpa, aggravata e oggettiva

Innanzitutto, la *quaestio* introduttiva può essere riassunta sinteticamente in questo modo: se vada operata un'indagine circa l'elemento soggettivo del danneggiante, oppure se quest'ultimo possa essere condannato al risarcimento in tutti i casi in cui un soggetto patisca un danno derivante dal suo trattamento illecito di dati personali. Per operare tale analisi si raffronterà il regime derivante dall'articolo 82 GDPR alle categorie classiche della responsabilità oggettiva, della responsabilità per colpa, e della particolare responsabilità aggravata. Si procede adesso attraverso un brevissimo inquadramento degli elementi rilevanti ai fini della tesi delle appena menzionate categorie.

Innanzitutto, la responsabilità soggettiva sorge da un fatto proprio, e si rinviene sia nella responsabilità per inadempimento *ex* articolo 1218 del codice civile[561], sia in quella aquiliana *ex* articolo 2043 del codice civile, ed è fondata su almeno uno degli elementi tra dolo o colpa. Essa è difatti la regola generale su cui il legislatore del 1942 ha inteso fondare il criterio

[561] La norma non opera riferimenti in merito a dolo o colpa, ma autorevole dottrina è concorde nel sostenere la natura soggettiva del criterio di imputazione di questo tipo di responsabilità: «la responsabilità contrattuale deve ritenersi una responsabilità soggettiva, cioè fondata sul principio della colpa: responsabile in generale è il debitore che non esegue o non esegue correttamente la prestazione per dolo o colpa»…«La colpa, invece, non deve intendersi sul piano psicologico, ma quale nozione obiettiva», Bianca C. M., *Diritto civile. La responsabilità*, 2021, pag. 21.

Nella Relazione del Ministro Guardasigilli al Codice Civile, numero 561, si legge: «d'altra parte, è pure noto che a gravissime discussioni diedero luogo i concetti di caso fortuito e forza maggiore, cui faceva riferimento l'art. 1226 del codice del 1865: la più recente tendenza della dottrina era nel senso di identificare quel concetto con l'assenza di colpa, da parte del debitore, nella determinazione dell'evento da cui dipendesse l'inadempimento o il ritardo. Per questo nell'art. 1218, a dirimere ogni questione si parla puramente e semplicemente di causa non imputabile al debitore: la non imputabilità dell'evento, ossia l'assenza di colpa riguardo al verificarsi del medesimo e al conseguente impedimento ad adempiere, costituisce il risultato subiettivo, che deve concorrere con quello obiettivo dell'impossibilità della prestazione, perché il debitore inadempiente sia esente da responsabilità». Alcuni autori (Bianca C. M., *Diritto civile. La responsabilità*, Giuffrè Francis Lefebvre, 2012, pag. 24, e Torrente A., Schlesinger P., *Manuale di diritto privato*, 2019, pag. 447) distinguono la responsabilità contrattuale in responsabilità soggettiva ed oggettiva, partendo dalla distinzione tra obbligazioni di mezzi e di risultato, ma in entrambi i casi ammettono la prova liberatoria, definendola talvolta come «impedimenti non prevedibili né superabili alla stregua dello sforzo diligente dovuto», talaltra come «sforzo inesigibile». Nel senso di una responsabilità per colpa, consolidata giurisprudenza di legittimità: sentenze numero 6404 del 30 Ottobre 1986; numero 3450 del 8 Giugno 1984; numero 4236 del 20 Giugno 1983; numero 5035 del 21 Luglio 1983; 4088 del 15 Giugno 1988; 5143 del 12 Giugno 1987.

d'imputazione della responsabilità civile[562]. Sotto il profilo dell'onere probatorio, l'articolo 1218 c.c. stabilisce che è il debitore-danneggiante a dover provare che «l'inadempimento o il ritardo è stato determinato da impossibilità della prestazione derivante da causa a lui non imputabile». L'articolo 2043 c.c., letto in combinato disposto con l'articolo 2697 del codice civile[563], richiede invece che sia il danneggiato a dover provare di avere diritto al risarcimento.

La responsabilità oggettiva, al contrario, sorge in virtù di una relazione con il soggetto che ha commesso il fatto o con una determinata cosa animata o inanimata (fatto altrui), e non è propria né della responsabilità contrattuale, né di quella delineata dall'articolo 2043 c.c.[564], che esplicitamente indica i requisiti del dolo e della colpa ai fini dell'obbligo risarcitorio[565]. Può invece rinvenirsi in alcune specifiche norme (del codice civile e non solo[566]), nelle quali appunto, manca il requisito dell'elemento soggettivo come elemento necessario per la condanna al risarcimento[567]. Queste norme si rinvengono negli articoli 2049, 2053 (in merito al solo «vizio di costruzione») e 2054 comma 4 c.c. (per quanto concerne i soli «difetti di

[562] «Nel nuovo codice si è tenuta presente l'unità del criterio misuratore della colpa, sia contrattuale che extracontrattuale», Relazione del Ministro Guardasigilli al Codice Civile preceduta dalla Relazione al disegno di legge sul "Valore giuridico della Carta del lavoro", numero 794.

[563] Il primo comma dell'articolo 2697 stabilisce che «chi vuol far valere un diritto in giudizio deve provare i fatti che ne costituiscono il fondamento».

[564] Malgrado l'autonomia concettuale che sovente viene attribuita alla responsabilità oggettiva, si applicano, in quanto compatibili, le disposizioni sulla responsabilità extracontrattuale *ex* articolo 2043 c.c. In tal senso Bianca C. M., *Diritto civile. La responsabilità*, 2021, pag. 662; Franzoni M., *L'illecito*, 2004, pag. 600.

[565] «L'art. 2043 c.c. parrebbe lasciar intendere che il danno extracontrattuale sia risarcibile solo se l'atto che lo cagiona è «doloso o colposo». In realtà, è lo stesso codice a prevedere non poche ipotesi in cui l'autore risponde dell'evento dannoso anche in assenza di dolo e di colpa: si parla, in tali casi, di «responsabilità oggettiva» (in contrapposizione alla «responsabilità soggettiva», che è quella che ha invece, quale suo presupposto, il dolo o, quanto meno, la colpa del danneggiante)», Torrente A., Schlesinger P., *Manuale di diritto privato*, 2019, pag. 904.

[566] Per le ipotesi di responsabilità oggettiva introdotte da leggi speciali vedasi Torrente A., Schlesinger P., *Manuale di diritto privato*, 2019, pag. 906-907.

[567] Nella Relazione del Ministro Guardasigilli al Codice Civile, numero 795, si legge tuttavia che il principio della pura causalità «non si è accolto perché ritenuto ingiusto, antisociale e antieconomico, e tale da scoraggiare attività ed iniziative feconde». Malgrado ciò, negli anni la dottrina ha individuato dei casi di responsabilità oggettiva pura. Un esempio ne è la «responsabilità dei padroni e dei committenti» *ex* articolo 2049 c.c. Sul punto vedasi Alpa G., Bessone M., *La responsabilità civile*, Giuffrè Editore, Milano, 2001, pag. 331; Franzoni M., *L'illecito*, 2004, pag. 677; Bianca C. M., *Diritto civile. La responsabilità*, 2021, pag. 704.

produzione»)[568]. Il regime di responsabilità oggettiva è caratterizzato dall'impossibilità di produrre una prova liberatoria[569].

Proseguendo, la responsabilità aggravata è anch'essa circoscritta a predeterminate ipotesi, rinvenibili negli articoli 2047, 2048, 2050, 2051 e 2052 del codice civile. In questa, è possibile rinvenire un aggravamento della posizione del danneggiante. Questa gravosità è data innanzitutto dall'inversione dell'onere della prova, che impone al danneggiante di provare la sua non colpevolezza, al contrario di quanto stabilito dalla regola generale *ex* articolo 2697 comma 1 del codice civile. La prova liberatoria, inoltre, non si riduce alla mera dimostrazione della mancanza di colpa: essa varia a seconda della fattispecie, e costituisce un aggravio rispetto a quella importata dal generale criterio d'imputazione soggettiva[570]. In tutti gli altri casi, a seconda del tipo di rapporto intercorrente tra danneggiato e danneggiante, si applicheranno o le norme *ex* articolo 1218 c.c. e seguenti, o l'articolo 2043 c.c.

Tornando a quanto disposto dal GDPR, ad oggi, secondo la maggior parte dei commentatori[571], l'articolo 82 andrebbe interpretato in termini oggettivi. Tale dottrina però, non si riferisce alla causalità pura, ma ad un tipo di oggettività semipiena, che lascia uno spazio, per quanto angusto, alla prova liberatoria[572]. Anche la giurisprudenza si muove nello stesso senso. Nelle sentenze si nota come non si ritenga necessaria la prova di un certo

[568] La ricollocazione delle fattispecie nella categoria della responsabilità oggettiva è presa da Torrente A., Schlesinger P., *Manuale di diritto privato*, 2019, pag. 905 e ss. L'inserimento delle fattispecie che si trovano negli articoli 2047, 2048, 2049, 2050, 2051, 2052, 2053, e 2054 c.c. nelle categorie di responsabilità oggettiva o aggravata non è unanime. Vista la difficoltà di differenziazione delle suddette categorie alcuni autori hanno optato per una unificazione. A proposito vedasi Alpa G., Bessone M., *La responsabilità civile*, 2001, pag. 332, ove si parla di «esposizione al pericolo», oppure Bianca C. M., *Diritto civile. La responsabilità*, 2021, che distingue tra ipotesi di responsabilità aggravata, oggettiva e altre figure complesse di responsabilità oggettiva o aggravata.

[569] Franzoni M., *L'illecito*, 2004, pag. 599; Torrente A., Schlesinger P., *Manuale di diritto privato*, 2019, pag. 905 e ss.

[570] Torrente A., Schlesinger P., *Manuale di diritto privato*, 2019, pag. 907.

[571] *Ex multis*, Strugala R., *Art. 82 GDPR: Strict Liability or Liability Based on Fault?* European Journal of Privacy Law & Technologies (EJPLT), 2020, pag. 74; Barbierato D., *Trattamento dei dati personali e «nuova» responsabilità civile*, 2019, pag. 5; Camardi C., *Note critiche in tema di danno da illecito trattamento dei dati personali*, Jus civile, volume 3, 2020, pag. 795; Ragno F., *Il diritto fondamentale alla tutela dei dati personali e la dimensione transnazionale del private enforcement del GDPR*, Ordine internazionale e diritti umani, 2020, pag. 827; Tosi E., *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale*, 2019, pag. 111; Calabrese G., *La responsabilità civile da illecito trattamento dei dati personali*, 2022, pag. 129; Riccio G. M., Scorza G., Belisario E. (a cura di), *GDPR e normativa privacy*, 2022, pag. 725; Cordeiro M., *A Civil Liability for Processing of Personal Data in the GDPR*, 2019, pag. 498; Zanfir-Fortuna G., *Article 82. Right to compensation and liabilty*, 2020, pag. 1176; Bilotta F., *La responsabilità civile nel trattamento dei dati personali*, 2019, pag. 462.

[572] Vedasi nota 580.

connotato psicologico, ma ci si concentri piuttosto sulla ricerca della prova liberatoria[573].

Le tesi a sostegno di una siffatta qualifica sono molto diverse tra loro. Si evidenzia innanzitutto, la mancanza di riferimenti normativi ad elementi psicologici come la colpa. Un'altra ragione risiede nella pericolosità insita nell'attività di trattamento dei dati personali: questa condurrebbe ad una oggettivizzazione della responsabilità. Ancora, l'inversione dell'onere della prova devia dall'imputazione di tipo soggettivo, conducendo ad una presunzione di colpa e dunque di responsabilità salvo prova contraria. Infine, la prova liberatoria sarebbe così angusta da far propendere per una qualifica in termini oggettivi.

Non mancano soluzioni miste, che riconducono l'articolo 82 nuovamente nell'alveo dell'articolo 2050 del codice civile interpretato oggettivamente, assumendo come prova liberatoria il fatto del terzo imprevedibile ed inevitabile come il caso fortuito e la forza maggiore.

Nel tentativo di comprendere la natura del criterio di imputazione della responsabilità imposto dall'articolo 82 del GDPR, si ritiene si debba prendere in considerazione il fatto che la maggior parte degli ordinamenti europei abbiano inteso le categorie della responsabilità per inadempimento (*contractual liability*) e della responsabilità aquiliana (*non-contractual liability o tort law*) come clausole generali caratterizzate dalla colpa, mentre la responsabilità oggettiva venga circoscritta a tassative ipotesi[574]. Quest'ultima rappresenta dunque l'eccezione alla regola della colpa. La responsabilità da trattamento illecito di dati personali non può essere riportata alla categoria eccezionale della causalità pura: si è detto che questa è caratterizzata dall'assenza della prova liberatoria, cosa che invece, l'articolo 82 GDPR prevede espressamente («se dimostra che l'evento dannoso non gli è in alcun modo imputabile»)[575]. Non si ha dunque

[573] *Ex* multis, nella sentenza numero 355 della Corte d'appello di Potenza del 22 Giugno 2020, in merito al previgente assetto normativo, si scriveva «si è al cospetto di una legge speciale che fonda una ipotesi peculiare di responsabilità extracontrattuale, contraddistinta dalla natura oggettiva (colpa presunta) dell'illecito. Trattasi cioè di responsabilità inquadrata, per giurisprudenza consolidata, nelle ipotesi di responsabilità oggettiva, con relativa inversione dell'onere probatorio, a carico di colui che gestisce il trattamento dei dati personali…».

[574] «*Here, most European legal systems have adopted a 'two-track approach', according to which the instances of strict liability stand intellectually unconnected besides the traditionally liability for fault. Normally, strict liability is therefore regarded as exceptional and in need of a specific justification*», Basedow J., Hopt K. J., Zimmermann R. (edito da), con Stier A., *The Max Planck Encyclopedia of European Private Law*, Oxford University Press, 2012, pag. 1040.

In Italia, la questione inerente alla natura di clausola generale dell'articolo 2043 è stata oggetto di lungo dibattito. Per una ricostruzione si rimanda a Barcellona M., *Trattato della responsabilità civile*, Wolters Kluwer Italia, Milano, 2011, pag. 27 e ss.

[575] Sul tema vedasi Franzoni M., *L'illecito*, 2004, pag. 162: «sul piano sistematico dunque, alla colpa resta confermato il ruolo di regola, mentre agli altri criteri spetta quello di eccezioni. Senonché, questo rapporto non si traduce in una corrispondente regola

l'elemento che consente di classificare questo tipo di responsabilità come un'eccezione ai generali modelli di responsabilità fondati sulla colpa.

Alcuni autori, come si diceva, si rifanno ad una oggettività semipiena; nell'analisi di tali argomentazioni si segnala un argomento che depone in favore della non classificabilità in termini oggettivi (o quasi oggettivi) di questo tipo di responsabilità. Il Regolamento è «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», e l'articolo 1 (rubricato «oggetto e finalità») paragrafo 3, prevede che «la libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali»[576]. Emerge dunque un equilibrio tra le due finalità[577], con espresso divieto di preferire la protezione dei dati personali alla libera circolazione dei dati, e con l'indicazione, offerta dal considerando numero 170, di operare tale bilanciamento alla luce del principio di proporzionalità impresso all'articolo 5 del TUE; da ciò, si ritiene contro le finalità del Regolamento qualunque interpretazione delle norme dello

operazionale: in concreto si tende a risolvere il problema della responsabilità ricorrendo alle figure speciali; solo in un secondo tempo si ricorre alla colpa»; l'autore conclude affermando che la colpa viene impiegata come criterio finale di imputazione per tutti quei danni ingiusti che non trovano previsione nelle fattispecie tipizzate dal Legislatore. Nello stesso senso Alpa G., Bessone M., *La responsabilità civile*, 2001, pag. 205. Più recentemente, Bianca C. M., *Diritto civile. La responsabilità*, 2021, pag. 661: «la centralità della colpa quale elemento caratterizzante la generale figura dell'illecito esclude che la responsabilità civile possa essere ricondotta alla regola dell'antico diritto germanico: «chi fa un danno, deve risarcirlo». L'enorme potenzialità di danno che macchine e industrie hanno via via sviluppato ha reso sempre più pressante l'esigenza di una più incisiva tutela del danneggiato. Questa esigenza non ha però trovato risposta in una generale oggettivizzazione della responsabilità extracontrattuale. Il nostro ordinamento ha mantenuto il principio generale della responsabilità extracontrattuale basato sul dolo e sulla colpa. Si è però dato ingresso a specifiche previsioni di responsabilità oggettiva o aggravata in relazione ad ipotesi dove più si è avvertita la necessità di intensificare la tutela del danneggiato».

[576] Il rapporto tra i due obiettivi risulta anche dai considerando numero 9, 10, 12,13, 53, 123, 166 e 170.

[577] Calabrese G., *La responsabilità civile da illecito trattamento dei dati personali*, 2022, pag. 123.

Taluni ritengono che il Regolamento abbia come obiettivo primario la libera circolazione dei dati, e come fine secondario il diritto alla protezione dei dati personali. In tal senso vedasi Bravo F., *Il «diritto» a trattare dati personali nello svolgimento dell'attività economica*, Cedam, 2018, pag. 12: «uno degli aspetti innovativi sembra dato proprio dall'approccio volto ad enfatizzare maggiormente la dimensione della libera circolazione rispetto a quello teso ad esaltare la dimensione di tutela della persona rispetto al trattamento dei dati personali: ovviamente si tratta di dimensione, quest'ultima, che non scompare nell'impianto normativo, essendo ben presente nelle scelte di fondo del legislatore eurounitario, ma che è oggetto di una profonda opera di revisione, protesa ad incidere sul bilanciamento tra diritti e libertà "fondamentali" in conflitto».

Similmente, Piraino F., *Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, Le nuove leggi civili commentate, volume 2, 2017, pag. 375 e ss.

stesso contrarie all'equilibrio designato per detti obiettivi[578]. Secondo chi scrive, un'interpretazione dell'articolo 82 del GDPR in termini oggettivi o quasi, con conseguente assenza di prova liberatoria (o comunque prova liberatoria pressoché indimostrabile[579]), potrebbe costituire un freno alla libera circolazione dei dati. Chi già tratta dati personali, così come i possibili soggetti interessati ad entrare nel mercato dei dati, potrebbero essere disincentivati ad investire in questa nuova risorsa qualora sapessero di essere giudicati in termini puramente oggettivi (o quasi). Un tipo di responsabilità soggettiva, che tenga debito conto degli sforzi profusi, si pone più in linea con l'obiettivo della circolazione dei dati e con l'espresso divieto di sacrificarla in nome della protezione dei dati personali[580]. Inoltre, il sapere di non essere condannati qualora si abbia fatto tutto il possibile potrebbe essere uno sprone ulteriore per adempiere ai propri obblighi, mentre, la coscienza che gli investimenti (soprattutto economici) profusi nella protezione dei dati non verrebbero considerati, potrebbe indurre molti titolari del trattamento a non impegnarsi fino in fondo[581].

In aggiunta, diversi autori hanno ritenuto come sia ancora possibile rifarsi alla categoria della responsabilità aggravata in virtù dell'articolo 15 del vecchio codice privacy, e del relativo rimando all'articolo 2050 c.c.[582].

---

[578] «…oggetto della disciplina è l'attività di trattamento secondo il principio, proprio delle attività economiche, della libera circolazione dei dati personali nell'Unione. Tanto che - ed è in questo senso che il principio della libera circolazione dei dati personali assume tra le finalità dell'intervento comunitario un valore sistematicamente più pregnante rispetto a quello della tutela della persona - il paragrafo 3 dell'art. 1 RGDP si preoccupa di precisare che tale libera circolazione «non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali». Evidentemente, questa volta e definitivamente, con la forza dello strumento regolamentare nel tentativo di scongiurare ciò che, viceversa, si era verificato nel contesto di applicazione della precedente Direttiva comunitaria», Cuffaro V., D'Orazio R., Ricciuto V., *I dati personali nel diritto europeo*, 2019, pag. 53.

[579] Si fa riferimento alle teorie del criterio oggettivo del rischio di impresa, nate dagli anni sessanta in poi del secolo scorso, dui si dirà al paragrafo 4.4.4.

[580] In tal senso, Gambini M., *Responsabilità e risarcimento nel trattamento dei dati* personali, 2019, pag. 1058.

[581] *Contra*, Trimarchi P., *La responsabilità civile: atti illeciti, rischio, danno*, Giuffrè, Milano, 2021, pag. 304: «…in sintesi dunque: anche la responsabilità oggettiva per rischio, al pari della responsabilità per colpa, è rivolta allo scopo finale di costituire incentivi appropriati per l'adozione delle misure di prevenzione degli incidenti che siano economicamente giustificate: che abbiano, cioè, un costo, in termini non solo di danaro, ma – più in generale – di sforzo e disutilità, inferiore al beneficio in termini di riduzione del rischio di danno…».

[582] «Più affidabile risposta a tale istanza è, ad avviso di chi scrive, il combinato disposto dell'art. 82 con l'art. 2050 c.c.; rectius, con la migliore interpretazione della disposizione codicistica, che fa coincidere la «prova di aver adottato le misure idonee» non nella mera allegazione della massima diligenza esigibile, ma nella dimostrazione di un fatto "terzo" generatore del danno, munito dei caratteri di imprevedibilità ed inevitabilità propri del caso fortuito e della forza maggiore», commento di Sica S., 2021, pag. 893; Tosi E., *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale*, 2019, pag. 113; Riccio G. M., Scorza G., Belisario E. (a cura di), *GDPR e normativa privacy*, 2022, pag. 724.

Si analizza ora la sostenuta compatibilità tra l'articolo 15 del vecchio codice privacy e il GDPR. Il Regolamento non specifica in alcun modo il tipo di responsabilità che disciplina; peraltro, il decreto di armonizzazione ha abrogato[583], senza sostituirlo, l'articolo 15 e il relativo richiamo all'articolo 2050 del codice[584]. In definitiva, oggi né il GDPR, né il nuovo codice privacy, offrono riferimenti positivi pieni da cui derivare il tipo di responsabilità in oggetto: è qui che l'interprete assume un ruolo rilevante: questi dovrà integrare le norme della fonte europea (sovraordinata) con le categorie classiche del diritto nazionale non contrastanti con quanto stabilito dalla norma gerarchicamente superiore. Il tutto, si premette, in attesa di un intervento del legislatore o della giurisprudenza europea.

Nella vigenza della Direttiva madre e del vecchio codice privacy, la dottrina e la giurisprudenza avevano utilizzato come chiave interpretativa il richiamo all'articolo 2050 del codice civile operato dall'articolo 15 del vecchio codice privacy, optando, nella maggior parte dei casi, per una qualificazione in termini semi-oggettivi della responsabilità da trattamento illecito. Il nuovo codice privacy non riporta più un'indicazione simile, e il GDPR definisce solo gli elementi essenziali del modello di responsabilità. Secondo chi scrive dunque, il primo passo per comprendere se l'articolo 82 GDPR possa essere ancora ricondotto nell'alveo delle attività pericolose disciplinate dall'articolo 2050 c.c., è capire la *ratio* sottostante l'abrogazione dell'articolo 15 e la mancata riproposizione del riferimento all'articolo 2050 del codice civile nel nuovo codice privacy. Si procederà di seguito all'esame di alcuni passi dei lavori che hanno preceduto l'approvazione del decreto di armonizzazione che ha abrogato l'articolo 15 del vecchio codice privacy.

Innanzitutto, all'articolo 13 comma 3 della legge di delegazione europea numero 163 del 25 Ottobre 2017[585], che conferiva delega al Governo in merito all'adeguamento nella normativa interna al GDPR, si legge che:

---

[583] L'abrogazione si è avuta in forza dell'articolo 27, paragrafo 1, lettera a, numero 2.

[584] «In particolare, il legislatore italiano avrebbe potuto compiere l'opera di armonizzazione adottando alternativamente più tecniche normative. In primo luogo, avrebbe potuto indicare una norma di riferimento nell'ambito del Codice civile che specificasse il regime di responsabilità civile applicabile in caso di danni derivanti da illecito trattamento dei dati personali. In secondo luogo, avrebbe potuto fornire indicazioni interpretative in relazione alla disposizione di cui all'art. 82 del Regolamento. In alternativa, avrebbe poi potuto rinviare, senza ulteriori specificazioni, al contenuto dell'art. 82 del Regolamento in materia di responsabilità civile. L'approccio adottato nel d.lgs. 101 del 2018 è l'ultimo indicato: in materia di responsabilità civile il decreto rinvia alle disposizioni contenute nel Regolamento europeo. Su tali disposizioni si concentrerà, pertanto, la presente indagine», Ratti M., *La responsabilità da illecito trattamento dei dati personali*, 2019, pag. 773.

[585] Legge disponibile online al seguente link:

https://www.gazzettaufficiale.it/eli/id/2017/11/6/17G00177/sg#:~:text=La%20legge%20di%20delegazione%20europea%20indica%20le%20direttive%20in%20relazione,e%20del%20Senato%20della%20Repubblica

«nell'esercizio della delega di cui al comma 1 il Governo è tenuto a seguire, oltre ai principi e criteri direttivi generali di cui all'articolo 32 della legge 24 dicembre 2012, n. 234, anche i seguenti principi e criteri direttivi specifici: a) abrogare espressamente le disposizioni del codice in materia di trattamento dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196, incompatibili con le disposizioni contenute nel regolamento (UE) 2016/679…».

La domanda nasce spontanea: l'articolo 15 potrebbe essere stato abrogato perché incompatibile con l'articolo 82 del Regolamento? Proseguendo, la questione è posta negli stessi termini nella relazione illustrativa alla bozza del decreto che sarebbe poi diventato il d.lgs. 101/2018 (decreto di armonizzazione), in cui si scriveva:

«dal combinato disposto delle previsioni del legislatore delegante, dunque, in relazione alla finalità della specifica delega, si desume che sono rimesse al legislatore delegato: innanzitutto la potestà di verificare se e quali disposizioni vigenti e, segnatamente, quelle recate attualmente dal codice in materia di protezione dei dati personali, debbano essere espressamente abrogate per incompatibilità con il regolamento; poi, la potestà di verificare se e quali disposizioni di detto codice siano da modificare ma "limitatamente a quanto necessario per dare attuazione alle disposizioni non direttamente applicabili contenute" nello stesso regolamento, ed infine la scelta dello strumento tecnico-normativa più lineare ed efficace per realizzare detti risultati»[586].

Da quanto appena letto sembra che al legislatore delegato siano state attribuite due modalità di intervento: l'abrogazione per incompatibilità al Regolamento, e la modifica nell'ottica di piena attuazione dello stesso. Assume concretezza l'ipotesi di una abrogazione per incompatibilità. Continuando, nel Dossier del Servizio Studi della Camera dei deputati del 21 Maggio 2018, in merito alla disposizione dell'articolo 15 si è scritto che «è abrogata dalla riforma e ora sostituita dall'articolo 82 del Regolamento»[587]. Emerge in modo ancor più significativo la scelta del legislatore italiano in merito all'articolo 15 del vecchio codice: abrogarlo e sostituirlo. Tenendo a mente le due tecniche di intervento affidate al Governo, chi scrive ritiene che se quest'ultimo avesse ritenuto ancora idoneo l'articolo 15 e il relativo rimando all'articolo 2050 c.c., lo avrebbe lasciato immutato, o al massimo lo

[586] Relazione illustrativa disponibile online al seguente link:
http://documenti.camera.it/apps/nuovosito/attigoverno/Schedalavori/getTesto.ashx?file=0022_F001.pdf&leg=XVIII#pagemode=none

[587] Dossier del Servizio Studi della Camera dei deputati del 21 Maggio 2018, pag. 88. La questione è espressa in termini di abrogazione anche a pagina 146. Il dossier è disponibile online al seguente link:
https://documenti.camera.it/Leg18/Dossier/Pdf/gi0007.Pdf

avrebbe modificato per dare piena attuazione al Regolamento[588]. L'abrogazione è invece una scelta meno assimilabile ad un giudizio di idoneità o compatibilità della norma. Risulta più ragionevole credere che l'abrogazione sia intervenuta a seguito di un giudizio di incompatibilità con il Regolamento. Tale ipotesi sarebbe poi corroborata dalla espressione «sostituita dall'articolo 82 del Regolamento» contenuta nel dossier: non si ha un generico rimando all'articolo 82, ma una giustapposizione di questo sul vecchio articolo 15 e il relativo rimando all'articolo 2050 c.c.

Alla luce di quanto appena detto si ritiene di non poter più considerare la responsabilità da trattamento illecito di dati personali come una fattispecie di responsabilità aggravata da far rientrare nella clausola generale dell'articolo 2050 c.c. Pertanto, non si aderisce al filone di pensiero secondo cui i risultati ottenuti da dottrina e giurisprudenza relativamente all'articolo 15 del vecchio codice privacy, ed al relativo rimando all'articolo 2050 del codice civile, siano tutt'oggi riproponibili. Il legislatore italiano ha abrogato quella norma, e ciò impone all'osservatore una nuova valutazione dell'articolo 82 GDPR, che non tenga conto di quanto detto in merito alla disciplina previgente[589]. Si ammette che il silenzio del legislatore in merito

[588] Sempre nella relazione illustrativa, pagina 2, si legge: «ebbene, a seguito delle verifiche compiute è risultato che la massima parte delle disposizioni del codice è da abrogare espressamente per essere risultate incompatibili con quelle recate dal regolamento; … Altra e minore parte delle previsioni codicistiche nazionali è stata modificata in modo rilevante, in relazione a disposizioni del regolamento unionale non direttamente applicabili, e che segnatamente lasciavano spazi all'intervento degli Stati membri, in particolare tramite il legislatore nazionale».

[589] Un'altra ragione che impone un radicale ripensamento del regime di responsabilità è il cambiamento di paradigma importato dal Regolamento e il nuovo contesto tecnologico che si intende affrontare e gestire: «L'abrogazione di questa disposizione significa dover far riferimento esclusivo all'art. 82 del Regolamento, una disposizione inserita in un testo che risponde a logiche diverse dalla precedente direttiva 95/46. Nella sostanza, il legislatore europeo ha spostato il baricentro del sistema dal consenso informato dell'interessato al trattamento alla "responsabilizzazione" del titolare e del responsabile del trattamento, con l'obiettivo di prevenire in modo più efficiente il verificarsi di danni connessi alla circolazione incontrollata dei dati. Detto in altri termini, il controllo dell'interessato sulla circolazione dei propri dati è diventato solo uno dei modi in cui si possono prevenire trattamenti illeciti o violazioni dei dati. Uno strumento di prevenzione — controllo dell'interessato — peraltro del tutto residuale rispetto al sistema di controllo del rischio che il titolare e il responsabile devono predisporre e analiticamente documentare fin dalla genesi del trattamento. Prima ancora che sulla responsabilità nei confronti del singolo interessato, il Regolamento è centrato sulla "responsabilità generale del titolare del trattamento per qualsiasi trattamento di dati personali che quest'ultimo abbia effettuato direttamente o che altri abbiano effettuato per suo conto" che ha come immediata conseguenza il dovere del titolare di "mettere in atto misure adeguate ed efficaci ed essere in grado di dimostrare la conformità delle attività di trattamento con il presente regolamento, compresa l'efficacia delle misure" (così il Considerando 74)»…«In un'ottica sistematica, la sola presenza nell'ordinamento dell'art. 82 del Regolamento, senza alcuna previsione legislativa nazionale di coordinamento tra la regola europea (la vittima di un illecito trattamento o violazione dei dati ha diritto al risarcimento dei danni) e il sistema italiano della responsabilità civile, rimette in discussione la scelta, fatta dal legislatore nazionale dopo la direttiva 95/46, di inserire esplicitamente la tutela individuale nell'ambito

ad un'abrogazione così significativa lascia adito a dubbi, che non possono però essere risolti facendo finta che tale operazione legislativa non sia mai avvenuta.

Proseguendo, al fine di stabilire il criterio d'imputazione della responsabilità, si è interpretato l'articolo 82 GDPR alla luce del principio di *accountability*[590]. Si può affermare che se si interpretasse la responsabilità *ex* articolo 82 GDPR in termini oggettivi si rischierebbe di svuotare di contenuto il principio di responsabilizzazione[591]. Parte fondamentale di tale principio è il generale dovere di dare conto (di essere *accountable*) della conformità al Regolamento e di quanto fatto in quest'ottica. A cosa servirebbe, si sottolinea, dimostrare l'adeguatezza delle misure tecniche ed organizzative adottate, e gli sforzi profusi per farlo, se tutto ciò non venisse preso in considerazione. Inoltre, si evidenzia come il principio di *accountability* richiami la diligenza tipica di una responsabilità ad imputazione soggettiva (articoli 1218 c.c. e 1176 c.c. e 2043 c.c.)[592]. Suddetto principio, infatti, allorquando impone al titolare l'obbligo di adeguatezza delle misure, chiede a questi di valutare diversi fattori (rischi, natura dei dati, modalità di trattamento, contesto, costi d'attuazione ecc.); in questo modo sta fornendo criteri attraverso cui il titolare del trattamento deve modulare il proprio impegno[593]. In questo modo, vi saranno dei casi in cui al titolare del trattamento sarà chiesto poco, ed altri in cui invece verrà preteso uno sforzo maggiore, al limite (come si vedrà nel paragrafo 4.4.3) dello stato dell'arte e dei costi di attuazione. Chi scrive aderisce a tale orientamento.

---

della responsabilità civile extracontrattuale. In altri termini, l'interprete è sollecitato a ripensare profondamente il sistema di tutela civilistico in materia di illecito trattamento e violazione dei dati, in quanto ha come referente normativo il solo art. 82 del Regolamento, dopo l'intervento abrogativo del d.lgs. n. 101/2018. Più precisamente, non appare opportuno innestare la nuova norma europea nel solco della giurisprudenza e della riflessione teorica sviluppatasi nella vigenza della disciplina italiana previgente, pensata in una cornice normativa — quella della direttiva 95/46 — strutturalmente differente dal Regolamento 2016/679. Sembra più utile, invece, interrogarsi su quanto l'assetto normativo si sia modificato e verificare se — per una sorta di eterogenesi dei fini — non si siano determinate le condizioni per immaginare un sistema di tutela individuale più incisivo rispetto a quello precedente», Bilotta F., *La responsabilità civile nel trattamento dei dati personali*, 2019, pag. 446 - 447.

[590] A proposito del principio di *accountability* si è scritto che «costituisce una forza sotterranea che informa di sé pressoché tutti gli istituti del Regolamento. È il verso nella cui direzione occorre applicare e interpretare le norme nella materia de qua», Bolognini L., Pelino E., *Codice della disciplina privacy*, 2019, pag. 88.

[591] In altri termini Gambini M., *Responsabilità e risarcimento nel trattamento dei dati* personali, 2019, pag. 1057-1058. *Contra*, Zanfir-Fortuna G., *Article 82. Right to compensation and liabilty*, 2020, pag. 1176: «*this conclusion is also supported by the accountability principle, which provides that the controller is responsible for demonstrating compliance with the principles relating to the processing of personal data under the GDPR, meaning that any unlawful processing is imputable to the controller, regardless of intention, fault or negligence*».

[592] Calabrese G., *La responsabilità civile da illecito trattamento dei dati personali*, 2022, pag. 128.

[593] Si parla di scalabilità del principio di *accountability*. Nota 436.

Inoltre, è stato rilevato come il principio di *accountability* importi un principio di adeguatezza[594]. In particolare, riguardo alle misure tecniche ed organizzative non si richiede che queste siano perfette, piuttosto che siano adeguate[595]. In virtù di ciò non sarà obbligo del titolare del trattamento disporre tutte le misure possibili per evitare il danno, ma solo quelle adeguate in risultanza di una corretta analisi e previsione dei rischi operata *ex ante*. Nei casi in cui al soggetto agente viene imposto di adottare tutte le misure astrattamente possibili per evitare il danno, a prescindere dallo stato dell'arte e dalla sostenibilità economica, la responsabilità tende ad essere qualificata in termini oggettivi[596].

Ciò significa che il titolare del trattamento non risponde del danno non evitabile attraverso la giustapposizione delle misure adeguate, che sono le uniche obbligatorie. Non deve applicare tutte le misure possibili, ma solo quelle adeguate a prevenire i rischi, nei limiti dello stato dell'arte e dei costi di attuazione.

Già nella vigenza del vecchio codice privacy, nella valutazione della responsabilità alla luce dell'articolo 15, con relativo rimando all'articolo 2050 c.c., la giurisprudenza non si limitava a riconoscere le sole tradizionali esenzioni da responsabilità del caso fortuito e della forza maggiore, ma si spingeva all'indagine sulla diligenza prestata dal titolare del trattamento nella giustapposizione delle misure, riconoscendo dunque una prova liberatoria più ampia rispetto a quella del solo caso fortuito o forza maggiore tipica di un modello di responsabilità semi-oggettivo[597].

Da ciò, chi scrive evince come la categoria della responsabilità soggettiva rispecchierebbe più fedelmente la lettera del Regolamento. In ogni caso, va precisato come si faccia riferimento ad un tipo di colpa oggettiva, individuabile nel mancato rispetto di specifici obblighi comportamentali. Non si fa dunque riferimento alla colpa come connotato psicologico.

Inoltre, sebbene l'articolo 82 GDPR non faccia riferimento agli elementi della colpa e del dolo, l'articolo 83 del Regolamento, tra i criteri utili a commisurare la sanzione amministrativa, prende in considerazione i suddetti elementi relativi al comportamento del danneggiante. Secondo chi scrive, non vi è motivo per escludere l'ambito della colpevolezza dalla

---

[594] Tosi E., *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale*, 2019 pag. 131; Giovannangeli S. F., *La violazione di dati o data breach*, 2019, pag. 396, si esprime nello stesso senso, ma con altri termini: «efficacia, appropriatezza».

[595] «*The European rules impose a duty to implement appropriate technical and organizational security measures. This is an 'obligation of means'. These actors are not obligated to provide a perfect security»,* Wolters P. T. J., *The security of personal data under the GDPR: a harmonized duty or a shared responsibility?*, International Data Privacy Law, volume 7, numero 3, 2017, pag. 172; Calabrese G., *La responsabilità civile da illecito trattamento dei dati personali*, 2022, pag. 166.

[596] Gambini M., *Responsabilità e risarcimento nel trattamento dei dati* personali, 2019, pag. 1055.

[597] Ibidem, pag.1057.

responsabilità civile, da sempre incentrata sulla colpa[598], mentre viene espressamente prevista per quella amministrativa.

Da quanto appena visto sembrerebbe doversi rifiutare un tipo di impostazione in termini oggettivi (pieni e semipieni)[599]. Tuttavia, per stabilire opportunamente la natura del criterio di imputazione della responsabilità da trattamento illecito occorre l'analisi di ulteriori elementi, che vengono presi in considerazione nei prossimi paragrafi.

4.4.2 Responsabilità da inadempimento e da fatto illecito

Nel precedente paragrafo si è chiarito perché, secondo chi scrive, la responsabilità da illecito trattamento dei dati personali non possa fondarsi su un criterio oggettivo, o semi-oggettivo. Preferendo un'impostazione soggettiva, si è anche rammentato come questo tipo di imputazione della responsabilità sia rinvenibile egualmente nella responsabilità per inadempimento *ex* articolo 1218 c.c. e in quella da fatto illecito *ex* articolo 2043 c.c. Il presente paragrafo tenta di offrire una risposta alla riconducibilità della responsabilità *ex* articolo 82 GDPR allo schema contrattuale o a quello extracontrattuale.

Come sottolineato[600], durante la vigenza della Direttiva madre e del vecchio codice privacy, in merito alla questione in analisi, la dottrina maggioritaria era orientata sulla natura extracontrattuale della responsabilità da trattamento illecito[601]. Minoritario invece il filone di pensiero che ricollegava la responsabilità da trattamento illecito al modello di responsabilità contrattuale delineato dall'articolo 1218 del codice civile[602]. Ad oggi la dottrina prevalente favorisce un inquadramento in

[598] Su tale dogma si dirà nel paragrafo 4.4.4.

[599] Nello stesso senso Gambini M., *Responsabilità e risarcimento nel trattamento dei dati* personali, 2019, pag. 1051-1053; Ratti M., *La responsabilità da illecito trattamento dei dati personali*, 2019, pag. 789; Truli E., *The General Data protection Regulation and Civil Liability*, 2018, pag. 25.

[600] Tosi E., *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale*, 2019, pag. 49.

[601] Nota 489.

[602] Scognamiglio C., *Buona fede e responsabilità civile*, in Europa e Diritto Privato, fascicolo 2, 2001, pag. 360-361; Castronovo C., *Situazioni soggettive e tutela nella legge su il trattamento dei dati personali*, in Europa e Diritto privato, fascicolo 3, 1998, pag. 676 e ss. Gli autori si concentrano sulle qualifiche del titolare e del responsabile del trattamento (terminologia del GDPR), definendo il previgente assetto come una responsabilità da *status*.

termini extracontrattuali[603]. Tuttavia, come sottolineato[604], l'abrogazione dell'articolo 15 del Codice privacy ad opera del decreto di armonizzazione, può rappresentare un'opportunità per ripensare la riconduzione della responsabilità delineata dall'articolo 82 del GDPR all'una o all'altra categoria.

Innanzitutto, per quanto concerne la responsabilità contrattuale (*rectius*: da inadempimento), è viva e diffusa, sia in Italia che nei principali ordinamenti dell'Europa continentale[605], la concezione secondo cui sorga non soltanto nei casi di violazione di obblighi previsto da un contratto così come strettamente definito dall'articolo 1321 c.c. [606]. Secondo autorevole dottrina[607], infatti, la responsabilità da fatto illecito «nasce con l'obbligazione risarcitoria (art. 1173 c.c.)» mentre quella da inadempimento

[603] *Ex multis*, De Rada D., *La responsabilità civile in caso di mancato rispetto del GDPR. Privacy by default, privacy by design e accountability nell'ottica del Diritto Privato*, Federalismi.it, 18 Dicembre 2019, pag. 8; Zanfir-Fortuna G., *Article 82. Right to compensation and liabilty*, 2020, pag. 1168; Calabrese G., *La responsabilità civile da illecito trattamento dei dati personali*, 2022, pag. 168 fa riferimento ai principi del diritto extracontrattuale europeo (PETL); Tosi E., *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale*, 2019, pag. 55; Barbierato D., *Trattamento dei dati personali e «nuova» responsabilità civile*, 2019, pag. 3; Camardi C., *Note critiche in tema di danno da illecito trattamento dei dati personali*, 2020, pag. 795; Gambini M., *Responsabilità e risarcimento nel trattamento dei dati* personali, 2019, pag. 1053; Ragno F., *Il diritto fondamentale alla tutela dei dati personali e la dimensione transnazionale del private enforcement del GDPR*, 2020, pag. 836.

[604] Bilotta F., *La responsabilità civile nel trattamento dei dati personali*, 2019, pag. 452: «l'abrogazione dell'art. 15 Codice *Privacy* può quindi essere l'occasione per rimeditare le categorie ordinanti della relazione giuridica sussistente tra chi effettua un trattamento dei dati e coloro a cui i dati si riferiscono». Nello stesso senso Piraino F., *Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, 2017, pag. 389; Agrifoglio G., *Risarcimento e quantificazione del danno da lesione della privacy: dal danno alla persona al danno alla personalità*, Europa e Diritto privato, fascicolo 4, 2017, pag. 1300.

[605] Mazzamuto S., *Il contratto di diritto europeo*, G. Giappichelli Editore, Torino, 2020, pag. 334: «se nelle tradizioni francese (art. 1147 Code civil), tedesca (§ 276), italiana (art. 1218 c.c.) e spagnola (art. 1101 Còdigo civil) la responsabilità costituisce un effetto dell'obbligazione, in quella di *common law* la responsabilità – come si è già anticipato – è posta in presa diretta con il contratto»; Castronovo C., Mazzamuto S., *Manuale di diritto* privato, Giuffrè Editore, Milano, 2007, pag. 224.

[606] «La semplificazione dei dispositivi giuridici che sembra caratterizzare questa nuova epoca e che prende forma nella preferenza accordata agli automatismi non merita di essere applicata alla struttura della responsabilità contrattuale, della quale va invece ribadita la caratteristica di conseguire alla violazione di un vincolo di azione di contenuto determinato e finalizzato al conseguimento di un fine specifico quando tale violazione genera una perdita. Conviene continuare a designare tale vincolo di azione mediante il concetto di obbligazione o di obbligo e non tanto per fedeltà alle categorie della tradizione *civilian* quanto per la maggiore precisione concettuale che la categoria dell'obbligo assicura rispetto a quella del contratto. Peraltro, l'ancoraggio della responsabilità contrattuale al contratto farebbe segnare una regressione sul cammino della conoscenza in questa materia perché determinerebbe il collegamento tra l'assunzione volontaria del vincolo e la responsabilità che scaturisce dalla sua violazione», Mazzamuto S., *Il contratto di diritto europeo*, 2020, pag. 335.

[607] Franzoni M., *L'illecito*, 2004, pag. 12.

«è una conseguenza patologica di un preesistente obbligo inadempiuto (art. 1218 c.c.)». Secondo tale proposta, dunque, affinché vi sia responsabilità contrattuale, è necessario che l'obbligazione trasgredita preesista rispetto alla violazione, a prescindere dalla fonte, qualsiasi essa sia. Negli altri casi, la violazione del generale principio *del neminem laedere* condurrà al sorgere della responsabilità da fatto illecito *ex* articolo 2043 c.c.

Altri commentatori, sostenendo la medesima tesi in termini diversi, si rifanno ad «una pregressa relazione tra i soggetti e quindi di un programma specifico di comportamento: la responsabilità contrattuale si modella sul programma (di qui il limite della prevedibilità del danno, salvo dolo), mentre quella aquiliana tutela non già le aspettative per l'inadempimento, ma lo *status quo ante* l'illecito, ripristinandolo con l'eliminazione dei danni, anche imprevedibili»[608]. Anche qui si vede come l'importante non sia la fonte dell'obbligazione, o del programma specifico di comportamento, ma la sua preesistenza rispetto alla violazione; in caso contrario si avrà responsabilità da fatto illecito. Dello stesso indirizzo è anche la giurisprudenza, che si riferisce ad un «inesatto adempimento di un'obbligazione preesistente, quale che ne sia la fonte»[609].

Si procede di seguito all'enunciazione delle principali argomentazioni a sostegno della riconducibilità del rapporto tra titolare del trattamento e

[608] Gazzoni F., *Manuale di diritto privato*, Edizioni Scientifiche Italiane, Napoli, 2013, pag. 650.

[609] La giurisprudenza italiana risulta oggi quasi unanime e ciò si deve alla sentenza numero 14712 del 2007 delle Sezioni Unite della Corte di Cassazione, che esamina la questione della differenza tra responsabilità contrattuale ed extracontrattuale. In virtù della limpidezza del ragionamento della Suprema Corte, si ripropongono le esatte parole: «è opinione ormai quasi unanimemente condivisa dagli studiosi quella secondo cui la responsabilità nella quale incorre «il debitore che non esegue esattamente la prestazione dovuta» (art. 1218 c.c.) può dirsi contrattuale non soltanto nel caso in cui l'obbligo di prestazione derivi propriamente da un contratto, nell'accezione che ne dà il successivo art. 1321 c.c., ma anche in ogni altra ipotesi in cui essa dipenda dall'inesatto adempimento di un'obbligazione preesistente, quale che ne sia la fonte. In tale contesto la qualificazione «contrattuale» è stata definita da autorevole dottrina come una sineddoche (quella figura retorica che consiste nell'indicare una parte per il tutto), giustificata dal fatto che questo tipo di responsabilità ricorre più frequentemente in presenza di vincoli contrattuali inadempiuti, ma senza che ciò valga a circoscriverne la portata entro i limiti che il significato letterale di detta espressione potrebbe altrimenti suggerire. Pur non senza qualche incertezza, in un quadro sistematico peraltro connotato da un graduale avvicinamento dei due tradizionali tipi di responsabilità, anche la giurisprudenza ha in più occasioni mostrato di aderire a siffatta concezione della responsabilità contrattuale, ritenendo che essa possa discendere anche dalla violazione di obblighi nascenti da situazioni (non già di contratto, bensì) di semplice contatto sociale, ogni qual volta l'ordinamento imponga ad un soggetto di tenere, in tali situazioni, un determinato comportamento"..."Ne deriva che la distinzione tra responsabilità contrattuale ed extracontrattuale sta essenzialmente nel fatto che quest'ultima consegue dalla violazione di un dovere primario di non ledere ingiustamente la sfera di interessi altrui, onde essa nasce con la stessa obbligazione risarcitoria, laddove quella contrattuale presuppone l'inadempimento di uno specifico obbligo giuridico già preesistente e volontariamente assunto nei confronti di un determinato soggetto (o di una determinata cerchia di soggetti)».

interessato allo schema delineato dall'articolo 1218 c.c. e, in un secondo momento, a quello derivante dall'articolo 2043 c.c.

A sostegno del primo orientamento è stato segnalato che un ipotetico danno derivante da trattamento di dati personali in violazione di un obbligo di legge (trattamento illecito) costituirebbe un inadempimento ai sensi dell'articolo 1218 c.c. e ciò comporterebbe il sorgere della responsabilità prevista dall'articolo 82 GDPR in capo al titolare del trattamento[610]. Inoltre, è stato sottolineato come una delle caratteristiche del GDPR sia proprio la presenza di numerosi e minuziosi obblighi specifici diretti a prevenire il rischio ed evitare il danno, che costituirebbero il modello obbligatorio da rispettare[611]. Il Regolamento (*latu sensu* inteso), vista l'eterogeneità delle basi del trattamento previste ai sensi degli articoli 6 e 9, prevede dei doveri in capo al titolare a prescindere da un accordo tra questi e l'interessato (come nel caso previsto dalla lettera e dell'articolo 6, secondo cui, in assenza di consenso, è possibile trattare lecitamente i dati personali quando «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»). Ciò significa, che in virtù di quanto detto poc'anzi sulla generale ripartizione tra la responsabilità per inadempimento e quella aquiliana, sarebbe possibile rinvenire un rapporto obbligatorio anche nel caso in cui il trattamento non sia protratto sulla base del consenso, in quanto il Regolamento fissa una serie di obblighi anche in assenza di esso[612].

Sempre secondo tale orientamento, l'attività di trattamento dei dati personali è vincolata al rispetto degli obblighi imposti dal Regolamento, i quali delimitano i confini del rapporto giuridico qualificato entro cui si trovano titolare del trattamento ed interessato. In caso di violazione, si avrebbe dunque l'inadempimento di un obbligo specifico (o di un principio)[613]. Inoltre, può notarsi come con l'abrogazione dell'articolo 15 del vecchio codice privacy sia venuto meno l'unico riferimento alla responsabilità da fatto illecito.

Si è dunque affermato che l'avvio di un trattamento di dati personali determina il sorgere di un rapporto obbligatorio tra titolare ed interessato

---

[610] In tal senso Bilotta F., *La responsabilità civile nel trattamento dei dati personali*, 2019, pag. 450 e ss.; Piraino F., *Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, 2017, pag. 389 e ss; Zecchin F., *Molteplicità delle fonti e tutela dei diritti. Il danno non patrimoniale nella lesione della proprietà e dei dati personali*, Europa e Diritto Privato, fascicolo 3, 1 Settembre 2022, pag. 517.

[611] Piraino F., *Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, 2017, pag. 389.

[612] Bilotta F., *La responsabilità civile nel trattamento dei dati personali*, 2019, pag. 450 e 451; Piraino F., *Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, 2017, pag. 390. Sulla possibilità di individuare la responsabilità contrattuale anche in assenza di specifica volontà negoziale vedasi Mazzamuto S., *Il contratto di diritto europeo*, 2020, pag. 336.

[613] Zecchin F., *Molteplicità delle fonti e tutela dei diritti. Il danno non patrimoniale nella lesione della proprietà e dei dati personali*, 2022, pag. 517.

(formato dalle prescrizioni imposte dal Regolamento)[614], e il mancato rispetto dei doveri previsti conduce ad un inadempimento ai sensi dell'articolo 1218 del codice civile e quindi al risarcimento del danno cagionato ai sensi dell'articolo 82 del GDPR[615].

La dottrina che invece propende per la natura extracontrattuale della responsabilità da trattamento illecito si basa innanzitutto sulla natura degli interessi tutelati mediante l'articolo 82 GDPR[616]. Identità personale, riservatezza, protezione dei dati personali, rientrano nel novero dei diritti della personalità, che sono storicamente protetti mediante un tipo di tutela extracontrattuale[617]. I *leading case* che hanno portato al riconoscimento di

[614] Bilotta F., *La responsabilità civile nel trattamento dei dati personali*, 2019, pag. 452: «cancellato ogni riferimento alla natura extracontrattuale della responsabilità nascente da un illecito trattamento o violazione dei dati, possiamo oggi più coerentemente riconoscere che l'inizio di un trattamento dei dati segna il sorgere di un rapporto obbligatorio tra il titolare e il responsabile da una parte e l'interessato al trattamento dall'altro. Di conseguenza, il mancato rispetto dei doveri di comportamento che la stessa legge individua e conducono a un inadempimento e al successivo risarcimento dei danni, ai sensi dell'art. 82 del Regolamento, per il quale è centrale la "imputabilità" del fatto lesivo, esattamente come accade in base all'art. 1218 c.c.».

[615] In Bilotta F., *La responsabilità civile nel trattamento dei dati personali*, 2019, pag. 451, si segnala l'incoerenza manifesta di una classificazione in termini extracontrattuale di una responsabilità derivante da violazione di obblighi contrattuali: «se si pone mente alle vicende giudiziarie che hanno caratterizzato il contenzioso in materia di responsabilità da trattamento illecito dei dati, ci si accorge di quanto tale incoerenza sistematica si sia riflessa sull'operato delle corti. Ci si riferisce a tutti quei casi riguardanti la vulnerabilità dei sistemi informatici delle banche che hanno determinato una circolazione incontrollata delle informazioni dei correntisti. In questi casi — che non importa in questa sede analizzare nei dettagli — la cornice entro cui il trattamento dei dati si inseriva era quella contrattuale. Eppure, il trattamento dei dati, necessario e funzionale all'adempimento del contratto è stato considerato dai tribunali fonte di una responsabilità extracontrattuale ai sensi delle allora vigenti norme del Codice *Privacy,* che richiamavano l'art. 2050 c.c.. In tal modo, il carico probatorio del correntista risultava molto meno gravoso, poiché si doveva limitare ad allegare l'esistenza di un danno conseguente alla sottrazione da parte di terzi dei codici di accesso ai conti on line Secondo i giudici, sulla banca gravava l'onere di provare di aver posto in essere tutte le misure idonee a evitare che terze persone potessero appropriarsi dei codici di accesso, danneggiando così la sfera giuridica del correntista. Quello che ne risulta è una sorta di ircocervo giuridico: si prende in considerazione una vicenda contrattuale su cui si innestano obblighi accessori (di fonte legale) e si giunge a evocare una responsabilità extracontrattuale, in caso di inadempimento di tali obblighi secondari, capace di incidere profondamente sulla ripartizione dell'onere probatorio».

[616] «Interessi della persona già riconosciuti nella tradizione civilistica come oggetto di tutela extracontrattuale sono quelli attinenti alla vita (v. oltre), alla salute (n.69), alla libertà personale, alla libertà sessuale, all'identità personale, al nome e all'immagine, alla riservatezza, alla paternità morale delle opere dell'ingegno, ecc.» (note omesse), Bianca C. M., *Diritto civile. La responsabilità*, 2021, pag. 562.

[617] Per una ampia ricostruzione del riconoscimento e della tutela dei diritti della personalità vedasi Caso R., *La società della mercificazione e della sorveglianza: dalla persona ai dati. Casi e problemi di diritto civile*, 2021, pag. 99 e ss.; Alpa G., Resta G., *Le persone fisiche e i diritti della personalità*, in Sacco R., *Trattato di Diritto Civile*, Utet giuridica, Milano,

alcuni diritti della personalità, *in primis* il diritto alla riservatezza, apprestavano la tutela basata sul fatto illecito. Ad esempio, nella sentenza della Corte di Cassazione numero 2129 del 1975 sul caso della principessa Soraya Esfandiari si ricercava il fondamento normativo necessario per l'applicazione dell'articolo 2043 c.c.[618], poi ritrovato negli articoli 2, 3, 29, 41 comma 2, 14, e 15 della Costituzione[619]. Attraverso l'applicazione diretta delle norme della Costituzione, mutuata dall'esperienza delle corti germaniche (*Drittwirkung*[620]) si arrivò al riconoscimento del diritto alla riservatezza e alla sua tutela civile mediante l'articolo 2043 c.c.

Prestando attenzione all'odierna disciplina della protezione dei dati personali, è stato sottolineato che il contenuto della disciplina apprestata dal Regolamento, sebbene simile nell'articolazione degli obblighi al contenuto di un rapporto negoziale, non è idonea ad attrarre l'articolo 82 GDPR nell'orbita della responsabilità da inadempimento[621]. Si evidenzia a tal proposito la tendenza, segnalata in dottrina nel quadro della responsabilità civile in generale[622], di affiancare ai doveri generici riconducibili a quello del *neminem laedere*, obblighi di comportamento più specifici, collegati a *status* soggettivi e condizioni professionali dei soggetti agenti[623]. La scelta di prevedere obblighi di condotta tipici, articolati e complessi si deve all'intento

---

2019, pag. 203 e ss.; Castronovo C., *La nuova responsabilità civile*, Giuffrè Editore, Milano, 2006, pag. 53 e ss.

[618] «La recente giurisprudenza di questa corte, pur evolvendosi nel ravvisare nell'ingiustizia del danno, considerata dall'art. 2043 cod. Civ., l'accezione di danno prodotto non iure, (e cioè non giustificato), non abbandona l'altra accezione del contra ius, va le a dire, in quanto tale fatto incida su una posizione soggettiva attiva tutelata come diritto»...«Se, quindi, allo stato dell'evoluzione dottrinale e giurisprudenziale, non sussiste un sicuro criterio di individuazione di responsabilità che prescinda dalla situazione incisa dal comportamento illecito, la tutela di un diritto soggettivo alla riservatezza passa attraverso l'individuazione del suo fondamento normativo. Tanto più questa ricerca è obbligata, in quanto tale tutela impinge, è, sotto certi aspetti, limita la libertà di manifestazione del proprio pensiero: limitazioni che non possono essere poste se non per legge e devono trovare fondamento in precetti esplicitamente enunciati dalla Costituzione o da questa tratti mediante rigorosa applicazione delle regole di ermeneutica», Cass. 2129/1975.

[619] Già sul finire degli anni cinquanta si era sostenuta la possibilità di rinvenire come fondamento del fatto illecito non soltanto una norma attributiva di diritti, ma anche una serie di indici da cui potesse essere ricavata (indirettamente) la meritevolezza della protezione dell'interesse in questione. Si introduceva l'interpretazione dell'articolo 2043 c.c. come clausola aperta, con conseguente atipicità dell'illecito civile. Sul punto vedasi Giampiccolo G., *La tutela giuridica della persona umana e il c.d. diritto alla riservatezza*, Rivista trimestrale di diritto e procedura civile, 1958, pag. 458.

[620] Sul punto Alpa G., Resta G., *Le persone fisiche e i diritti della personalità*, pag. 298-299.

[621] Tosi E., *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale*, 2019, pag. 54.

[622] Di Majo A., *I cinquantanni del libro delle obbligazioni*, in Rivista Critica di Diritto Privato, 1992, pag. 170 e ss.

[623] Gambini M., *Responsabilità e risarcimento nel trattamento dei dati* personali, 2019, pag. 1083; Tosi E., *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale*, 2019, pag. 51-52. Entrambi gli autori si rifanno all'opera di Di Majo A., citata nella nota precedente.

di soddisfare esigenze di simmetria e armonizzazione all'interno dell'Unione, obiettivi tipici dello strumento regolatorio del regolamento comunitario[624]. Sembrerebbe dunque non potersi più indicare come criterio discretivo utile a distinguere la responsabilità da inadempimento da quella da fatto illecito l'esistenza di una pregressa relazione tra danneggiante e danneggiato.

Attenta dottrina ha rilevato come gli obblighi previsti dal GDPR siano di natura procedimentale, dunque non idonei a far sorgere l'aspettativa di una determinata prestazione: in particolare, Emilio Tosi ha definito la loro natura «procedimentale» e «metaindividuale»[625]; la tutela apprestata dal Regolamento non si risolverebbe nel soddisfacimento di una pretesa individuale nell'ambito di un rapporto obbligatorio, destinata a soddisfare l'esclusivo interesse della persona i cui dati sono trattati, ma sarebbe indirizzata alla tutela di interessi di rango costituzionale, quali identità personale, riservatezza e protezione dei dati personali (e di riflesso anche del mercato dei dati personali)[626]. Tale impostazione non è peraltro tesa ad escludere la configurabilità di un contratto tra titolare del trattamento e interessato[627], anche se occorre segnalare come il dato personale sia riconducile a diritti della personalità non liberamente disponibili se non nei limiti del regime di protezione previsto dal GDPR[628]. Alla luce di quanto sin qui esposto è possibile affermare che è la violazione della sfera giuridica dell'interessato, e segnatamente dei suoi diritti e libertà fondamentali, ad instaurare la responsabilità del titolare del trattamento (o del responsabile).

Tuttavia, si evidenzia come la disciplina apprestata dal Regolamento, che attribuisce la responsabilità da trattamento illecito a soggetti qualificati (titolare e responsabile del trattamento), si discosti dal modello della responsabilità «del passante»[629] non incentrato su una necessaria qualifica del soggetto agente[630]. Un altro elemento di specialità è dato dal riparto dell'onere probatorio, posto dagli articoli 5 paragrafo 2, e 82 del Regolamento in capo al soggetto danneggiante, mentre ai sensi dell'articolo 2043 c.c. è il danneggiato a dover fornire la prova di un danno ingiusto subito

---

[624] Tosi E., *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale*, 2019, pag. 52.

[625] Ibidem, pag. 55.

[626] Ibidem.

[627] Sul rapporto tra autonomia contrattuale e diritti della personalità vedasi Alpa G., Resta G., *Le persone fisiche e i diritti della personalità*, in Sacco R., *Trattato di Diritto Civile*, 2019, pag. 543 e ss.

[628] Tosi E., *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale*, 2019, pag. 55.

[629] Espressione utilizzata per descrivere i profili soggettivi della responsabilità da fatto illecito in Castronovo C., *La nuova responsabilità civile*, 2006.

[630] Tosi E., *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale*, 2019, pag. 52 e Gambini M., *Responsabilità e risarcimento nel trattamento dei dati* personali, 2019, pag. 1083.

A tal proposito potrebbe anche segnalarsi come la definizione di titolare del trattamento, gravato da un tipo di responsabilità generale, sia stata delineata con l'obiettivo di non limitare il numero di soggetti qualificabili come titolari.

come conseguenza di un'imprudenza, negligenza, imperizia o dolo (in linea con il disposto dell'articolo 2697 c.c.).

Inoltre, nell'ambito della responsabilità extracontrattuale la colpa rileva come «inosservanza della diligenza dovuta nei rapporti di relazione»[631]. Essa non va dunque intesa come nozione soggettiva o psicologica, ma come elemento obiettivo, che si parametra in base a parametri sociali o professionali di condotta[632]. Come la colpa contrattuale, anche quella del fatto illecito si specifica negli aspetti della negligenza, imprudenza ed imperizia. Particolarmente rilevante ai fini dell'elaborato è l'imprudenza, che si concreta nell'inosservanza da parte del danneggiante (titolare del trattamento) di cautele specifiche, giudicate secondo regole di esperienza, regole professionali o norme di legge[633]. La violazione di tali parametri oggettivi, nell'ambito della protezione dei dati personali, si concreta nel mancato rispetto dei precetti del Regolamento (*latu sensu*), e ciò determinerebbe la responsabilità per colpa del titolare del trattamento. In particolare, come si vedrà nel paragrafo 4.6, il principale parametro attraverso cui parametrare la diligenza (quindi la perizia, la prudenza, la perizia) è costituito dal principio di *accountability*.

In merito alle esimenti nella responsabilità da fatto illecito si annoverano l'incapacità del soggetto agente, il caso fortuito, la forza maggiore, lo stato di necessità, la legittima difesa, il consenso dell'avente diritto e l'esercizio di un diritto.

Per quanto concerne la responsabilità del titolare del trattamento giova descrivere brevemente le esimenti del caso fortuito e della forza maggiore. Queste due ipotesi racchiudono il medesimo significato: esse indicano l'evento non prevedibile né superabile con la diligenza dovuta (analogamente alla causa dell'impossibilità della prestazione nella responsabilità contrattuale)[634].

Pertanto, la violazione delle norme del Regolamento ad opera del titolare del trattamento, qualora non dovuta ad un evento non prevedibile o superabile con la dovuta diligenza, determinerà il sorgere della responsabilità prevista dall'articolo 82 GDPR.

Sempre in relazione al rapporto tra l'articolo 82 del GDPR e l'articolo 2043 c.c, tale ultima disposizione prevede l'ingiustizia del danno come requisito generale della responsabilità, mentre, nulla di simile viene esplicitato nella lettera dell'articolo 82 GDPR. Quest'ultimo si riferisce infatti soltanto alle regole da osservare, senza operare alcun riferimento al profilo della lesione della situazione giuridica soggettiva tutelata. A tal proposito la dottrina si è divisa tra chi ha ritenuto implicito tale criterio anche nell'impianto derivante dall'articolo 82 GDPR, e chi invece abbia attribuito alla specialità della disciplina prevista dal Regolamento valenza derogatoria,

[631] Bianca C. M., *Diritto civile. La responsabilità*, 2021, pag. 551.
[632] Ibidem, pag. 552.
[633] Ibidem, pag. 554.
[634] Ibidem, pag. 636.

con la conseguenza della non necessarietà dell'ingiustizia del danno ai fini dell'attivazione della responsabilità da trattamento illecito di dati personali[635]. I sostenitori di tale ultima posizione ritengono che l'ingiustizia del danno sia da considerarsi *in re ipsa*. La questione verrà affrontata più attentamente al paragrafo 4.5, ma risulta qui necessario precisare che chi scrive aderisce all'orientamento secondo cui sia necessario dimostrare l'ingiustizia del danno, come previsto generalmente dall'articolo 2043 c.c.

Chi scrive aderisce all'ultimo orientamento descritto. In virtù della natura degli interessi tutelati mediante l'articolo 82 e le altre norme del Regolamento, e in forza di quanto dimostrato in merito al generale *discrimen* tra responsabilità da inadempimento ed aquiliana[636], si ritiene che la responsabilità del titolare del trattamento vada valutata in ossequio al combinato disposto degli articoli 2043 c.c. e 82 GDPR. Si proseguirà l'elaborato mantenendo dunque una responsabilità extracontrattuale per colpa oggettiva.

Nel senso di una responsabilità extracontrattuale si muove anche la giurisprudenza[637].

4.4.3 Limiti: stato dell'arte e costi di attuazione

Avendo individuato il modello di responsabilità (extracontrattuale, tendenzialmente soggettiva), restano da esaminare le seguenti questioni: i limiti alla responsabilità del titolare-creditore-danneggiante, l'eventuale danno da risarcire e infine la consequenziale prova liberatoria.

Nel presente paragrafo si analizza come il Regolamento prenda in considerazione lo stato dell'arte e i costi d'attuazione. Il riferimento ad essi si trova in diversi punti del Regolamento: considerando 83[638], 4[639], 94[640],

[635] Sostenitori di tale ultimo orientamento, *ex multis*: Tosi E., *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale*, 2019, pag. 104 ; Messinetti D., *I nuovi danni. Modernità, complessità della prassi e pluralismo della nozione giuridica di danno*, Rivista Critica di Diritto Privato, 2006, pag. 543 e ss; Resta G., Salerno A., *La responsabilità civile per il trattamento dei dati personali*, in Alpa G., Conte G. (a cura di), *La responsabilità d'impresa*, Milano, 2015, pag. 660 e ss.

[636] Si fa riferimento alla citata opera di Di Majo A., 1992.

[637] Tra le pronunce recenti in cui si esplicita la natura extracontrattuale del rapporto vedasi Cassazione civile sez. VI, 16/09/2022, n.27267.

[638] «…Tali misure dovrebbero assicurare *un adeguato livello di sicurezza*, inclusa la riservatezza, *tenuto conto dello stato dell'arte e dei costi di attuazione* rispetto ai rischi che presentano i trattamenti e alla natura dei dati personali da proteggere…» (enfasi aggiunta).

[639] «Laddove la valutazione d'impatto sulla protezione dei dati indichi che i trattamenti presentano *un rischio elevato che il titolare del trattamento non può attenuare mediante misure opportune in termini di tecnologia disponibile e costi di attuazione*, prima del trattamento si dovrebbe consultare l'autorità di controllo…» (enfasi aggiunta).

[640] «Se dalla valutazione d'impatto sulla protezione dei dati risulta che il trattamento, in mancanza delle garanzie, delle misure di sicurezza e dei meccanismi per attenuare il rischio, presenterebbe un rischio elevato per i diritti e le libertà delle persone fisiche e il titolare del trattamento è del parere che *il rischio non possa essere ragionevolmente*

articolo 17 paragrafo 2[641], e soprattutto agli articoli 25[642] e 32[643]. Questi fattori vengono presi in considerazione in relazione all'adeguatezza ed alla opportunità delle misure tecniche ed organizzative (relative alla sicurezza e non solo[644]), e in rapporto ai rischi per i diritti e le libertà delle persone fisiche da attenuare.

Stato dell'arte e costi di attuazione sono stati efficacemente definiti come

> «i limiti normativi richiamati espressamente dal regolamento comunitario in parola, *all'obbligo di adeguatezza tecnica e organizzativa,* in prospettiva di analisi e gestione del *rischio tipico,* correlato all'attività specifica di trattamento effettuato, in attuazione del principio di responsabilizzazione: espressione dei più generali *principi di prevenzione e precauzione della responsabilità civile,* che concorrono a delineare il *rischio d'impresa* socialmente ed economicamente accettabile»[645].

---

attenuato in termini di tecnologie disponibili e costi di attuazione, è opportuno consultare l'autorità di controllo prima dell'inizio delle attività di trattamento» (enfasi aggiunta).

[641] «Il titolare del trattamento, se ha reso pubblici dati personali ed è obbligato, ai sensi del paragrafo 1, a cancellarli, *tenendo conto della tecnologia disponibile e dei costi di attuazione adotta le misure ragionevoli, anche tecniche*, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali» (enfasi aggiunta).

[642] «*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*…» (enfasi aggiunta).

[643] «*Tenendo conto dello stato dell'arte e dei costi di attuazione*, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, *il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate*…» (enfasi aggiunta).

[644] Di norma, la questione dello stato dell'arte e dei costi d'attuazione viene legata alle sole di misure di sicurezza, ma dal tenore letterale dei considerando e delle norme prese in esame non sembra potersi escludere la loro applicabilità anche agli altri tipi di misure. Nel prosieguo della trattazione si parlerà genericamente di misure tecniche ed organizzative.

A riguardo: «*the state of the art and the cost of implementation are also relevant considerations. They are included in article 25(1). Since article 24 and article 25(1) both cover any technical and organisational compliance measure, their scope is the same, meaning that these two additional factors always apply next to the factor of 'risk'*», Quelle C., *The 'risk revolution' in EU data protection law: We can't have our cake and eat it, too*, Tilburg Law School Legal Studies Research Paper Series, numero 17, 2017, pag. 9.

Nello stesso verso, con altri argomenti, Selzer A., *The Appropriateness of Technical and Organisational Measures under Article 32 GDPR*, 2021, pag. 123.

[645] Tosi E., *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale*, 2019, pag. 75. L'autore ne parla in riferimento al particolare criterio del rischio d'impresa, di cui si dirà nel prossimo paragrafo.

Da quanto appena riportato emerge come questi parametri siano stati posti per delineare i limiti di ciò può essere socialmente ed economicamente richiesto al titolare ed al responsabile del trattamento. Al di fuori di ciò, è da ritenere esente da responsabilità il soggetto tenuto ad apprestare le suddette misure[646].

Se da un lato può essere agevole individuare astrattamente tale limite (sforzo economico non socialmente accettabile), non risulta altrettanto semplice delineare concretamente lo sforzo economico richiedibile. Prima di procedere all'analisi dei due indicatori occorre porre due premesse: innanzitutto, il Regolamento pone la protezione dei dati personali sullo stesso piano della circolazione degli stessi, e ciò significa che l'una non è sacrificabile in nome dell'altra, ma occorre individuare se e dove queste sono in equilibrio tra loro. La seconda premessa è relativa ai due parametri: questi vanno esaminati sia congiuntamente che individualmente.

Per quanto concerne lo stato dell'arte, questo non viene definito dal Regolamento; tra le diverse soluzioni definitorie proposte si abbraccia quella secondo cui tale espressione, contestualizzata all'interno del GDPR, indicherebbe quelle misure basate su comprovate conoscenze, di uno stato avanzato di sviluppo tecnico, pronte ed adattabili nella pratica[647]. Il requisito dello stato avanzato di sviluppo tecnologico impone al titolare del trattamento un regolare controllo sulla corrispondenza delle misure adottate a quelle riferibili allo stato dell'arte.

Non presenta invece le medesime complessità definitorie il riferimento ai costi d'attuazione. Le questioni sono altre: i costi di *follow up* e la considerazione della situazione finanziaria del titolare del trattamento. Per quanto concerne i costi di aggiornamento, ci si è chiesti se questi rientrino nel riferimento ai costi di attuazione, o se oppure vadano considerati solo gli originali costi della prima applicazione della misura, senza dunque includere anche quelli relativi alla manutenzione o all'aggiornamento delle stesse. Chi scrive ritiene che non vi siano appigli normativi per abbracciare tale ultima tesi. Nei costi d'attuazione dovrebbero rientrare tutte le spese relative all'applicazione e al mantenimento delle misure, che devono sempre essere idonee a ridurre il rischio derivante dal trattamento. Il continuo monitoraggio delle misure è punto centrale del principio di *accountability*, e richiede dei costi, che vanno necessariamente

---

[646] Tosi E., *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale*, 2019, pag. 78. L'autore citato si esprime in tali termini dopo aver qualificato il criterio d'imputazione in termini semi oggettivi. Malgrado, dunque, si parta da un presupposto differente, si ritiene di poter interpretare lo stato dell'arte e i costi di attuazione nel medesimo modo: essi costituiscono limiti normativi alla responsabilità del titolare o del responsabile del trattamento.

[647] «*To summarize, the 'state of the art' means measures that are based on proven knowledge, of an advanced state of technical development, practically suitable, ready and available for technical implementation, but have not necessarily become established in practice yet*», Selzer A., *The Appropriateness of Technical and Organisational Measures under Article 32 GDPR*, 2021, pag. 123.

considerati ai fini dell'applicazione delle misure e ai fini dell'eventuale responsabilità del titolare del trattamento.

Per quanto concerne invece la questione inerente alla specifica situazione finanziaria del titolare del trattamento, il Regolamento non si esprime. Vi è chi ha sostenuto che questo fattore non vada preso in considerazione in quanto potrebbe esimere le piccole imprese ad attuare le misure più idonee; contrariamente, altri hanno sostenuto che va presa in considerazione la situazione finanziaria specifica del titolare del trattamento di modo da indurre questi ad attuare le più moderne misure di prevenzione del rischio. Altri ancora, affermano che più che la situazione finanziaria del soggetto che tratta i dati, vada considerato il beneficio economico derivante dal trattamento: dunque, se anche si trattasse di una piccola impresa, ma questa ottenesse importanti proventi dal trattamento di dati personali, sarebbero richiesti a questa anche misure dai costi elevati[648]. Secondo chi scrive, i costi d'attuazione andrebbero interpretati alla luce del succitato equilibrio tra protezione dei dati personali e circolazione degli stessi espresso dall'articolo 1 del Regolamento, e attraverso la lente del principio di adeguatezza imposto dal principio di *accountability*. Innanzitutto, non potendosi limitare la circolazione dei dati in nome della loro protezione, sarebbe contrario al Regolamento richiedere costi d'attuazione che possano portare i titolari del trattamento a non operare nel mercato; allo stesso tempo, il principio di adeguatezza non richiede la misura perfetta, ma solo quella adeguata ad evitare i rischi derivabili dal trattamento. Il limite sarebbe dunque, secondo chi scrive, consistente nei più alti costi d'attuazione sostenibili dal titolare *de quo*, purché comunque idonei a prevenire il rischio previsto.

Il principio di adeguatezza funzionerebbe così come limite minimo, in quanto non possono giustificarsi misure non idonee ai rischi previsti *ex ante*, ma anche come limite massimo, in quanto la lettera della norma è chiara: il titolare del trattamento deve apporre misure adeguate ai rischi previsti, nulla più gli è richiesto. Non sarebbe dunque scusabile il titolare del trattamento che appresti misure sostenendo costi che per lui sono massimi, se però, alla luce della sua analisi dei rischi operata *ex ante*, risulta che quelle misure non erano idonee a prevenirli. Sarebbe invece scusabile il titolare del trattamento che, malgrado si sia verificato un danno, abbia speso quanto più per lui possibile in misure tecniche ed organizzative che, in base alla sua valutazione *ex ante*, erano adeguate a prevenire i rischi derivabili da quel trattamento (si presuppone ovviamente che l'analisi dei rischi fosse protratta adeguatamente). In questo modo si ritiene di rispettare sia l'equilibrio tra circolazione e protezione dei dati fissato dall'articolo 1 GDPR, che il principio di adeguatezza imposto dal principio di *accountability*. Il primo poiché il limite dei costi ragionevoli non dovrebbe scoraggiare gli imprenditori che vogliono far uso dei dati personali. Il secondo perché

[648] Per il dibattito si rimanda a Selzer A., *The Appropriateness of Technical and Organisational Measures under Article 32 GDPR*, 2021, pag. 125.

l'adeguatezza delle misure è stata valutata a monte dal Legislatore europeo come *standard* più corretto per garantire sia la circolazione che la protezione dei dati personali, e chiedere più di questa ai titolari-imprenditori costituirebbe una violazione del suddetto principio.

Quanto appena detto conferisce al titolare del trattamento una grande discrezionalità nello stabilire cosa sia richiedibile e cosa no, in linea con la filosofia dell'*accountability*[649].

Maggiori perplessità emergono nel caso in cui il titolare *de quo* abbia gli strumenti per spingersi oltre la mera adeguatezza richiesta dal principio di *accountability*. Secondo chi scrive, il principio di adeguatezza proprio del principio di *accountability*, è il risultato della ponderazione del legislatore europeo, che ha come obiettivo il proporzionale bilanciamento tra circolazione dei dati personali e protezione degli stessi. È stato deciso a monte come la *mera* adeguatezza sia lo strumento più adeguato a bilanciare protezione e circolazione dei dati personali. Motivo per cui, richiedere più dell'adeguatezza potrebbe considerarsi contrario al Regolamento: non dovrebbe ritenersi che il titolare risponda per le misure più che adeguate che poteva predisporre ma non ha apposto.

Vi è inoltre chi ha ritenuto che il principio di *accountability*, nella parte in cui impone misure tecniche ed organizzative adeguate nei limiti dello stato dell'arte e dei costi di attuazione, costituisca una obbligazione di mezzi e non di risultato[650]. Concludendo, si afferma che lo stato dell'arte, ma soprattutto i costi di attuazione per ottenere le misure tecniche ed organizzative adeguate richieste dal principio di *accountability*, costituiscono dei limiti alla responsabilità del titolare del trattamento. Il costo d'impresa atipico, ossia irragionevole e sproporzionato, non rientra dunque tra i doveri precauzionali del titolare del trattamento-imprenditore[651]: esso interrompe il nesso causale previsto dall'articolo 82 GDPR («non gli è in alcun modo imputabile»)[652].

4.4.4 Responsabilità oggettiva da rischio d'impresa

Alla luce di quanto esposto finora, è possibile escludere che la responsabilità da trattamento illecito di dati personali rientri nella categoria

---

[649] «*The factor of cost and the discretion of the controller both raise questions with respect to the ways in which the fundamental rights of individuals can be limited*», Quelle C., *The 'risk revolution' in EU data protection law: We can't have our cake and eat it, too*, 2017, pag. 9.

[650] Van Alsenoy B., *Liability under EU Data Protection Law*, 2016, pag. 282; Calabrese G., *La responsabilità civile da illecito trattamento dei dati personali*, 2022, pag. 166; Wolters P. T. J., *The security of personal data under the GDPR: a harmonized duty or a shared responsibility?*, 2017, pag. 172.

[651] Tosi E., *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale*, 2019, pag. 41.

[652] Ibidem, pag. 75.

della responsabilità oggettiva, e sia più consono adottare un criterio soggettivo, che tenga conto degli sforzi profusi dal titolare del trattamento.

Ammettendo dunque la natura soggettiva del criterio d'imputazione della responsabilità *ex* articolo 82, va rilevato come in Italia, dagli anni sessanta in poi del secolo scorso, le attività d'impresa, specialmente se pericolose, sono state messe in relazione alla responsabilità oggettiva, in virtù del criterio del rischio[653]. Il GDPR sembra invece mettere in relazione l'attività di per sé pericolosa del trattamento dei dati personali e una responsabilità soggettiva caratterizzata dall'inversione dell'onere della prova, che trova nel principio di responsabilizzazione il suo cardine[654]. In questo paragrafo si dirà della applicabilità del criterio enucleato da tale risalente dottrina italiana all'ambito della protezione e circolazione dei dati personali; criterio che portò una notevolissima porzione della dottrina e della giurisprudenza italiana a configurare in relazione alle attività commerciali un criterio di responsabilità oggettivo, ma non nel senso di una causalità pura come descritta nel paragrafo 4.4.1 (per esigenze pratiche, si riporteranno solo quei profili di quella dottrina che appaiono rilevanti ai fini della tesi).

Come rilevato in precedenza, il legislatore del codice civile del 1942 ha mantenuto il principio ordinatore della colpa, se non in specifiche ipotesi di responsabilità oggettiva. Quanto detto non è scritto nel codice, ma è il risultato della ricostruzione sistematica operata dalla dottrina in analisi, la quale evidenziò come non fosse del tutto corretto affermare, come invece faceva la relazione al codice civile e la Corte di Cassazione, che non fosse stato accolto il principio di causalità pura[655]. Tale orientamento si proponeva

---

[653] Dialogo avviato da Trimarchi P., *Rischio e responsabilità oggettiva*, 1961.

[654] Nello stesso senso, ma previa qualifica in termini extracontrattuali, Barbierato D., *Trattamento dei dati personali e «nuova» responsabilità civile*, 2019, pag. 5: «è da ritenersi, comunque, più aderente allo «spirito» del Regolamento l'orientamento, che configura la responsabilità ex art. 82, come una responsabilità aggravata per colpa presunta, poiché tale qualificazione — che contempla il profilo soggettivo — risulta più coerente al principio di accountability e potrebbe rivelarsi, in un'ottica funzionale preventiva, più efficace nella valorizzazione del rimedio risarcitorio».

[655] «Il presente lavoro si propone di accertare se e come sia realizzato, nell'ordinamento giuridico italiano, un principio di responsabilità oggettiva per il rischio d'impresa. È ben vero che tale principio appare ufficialmente e autorevolmente negato nella relazione del Ministro Guardasigilli che accompagna il codice civile, e viene negato assai spesso nelle motivazioni delle sentenze della Corte di Cassazione. Tuttavia, se, al di là delle formule e delle dichiarazioni di principio, si guarda al diritto «in azione», si deve pur riconoscere che, almeno in qualche misura, l'imprenditore risponde oggettivamente del rischio di impresa», Trimarchi P., *Rischio e responsabilità oggettiva*, 1961, pag.1.

Nello stesso senso Rodotà S., *Il problema della responsabilità civile*, Giuffrè, Milano, 1967, pagine da 58 a 64, in cui riportano i pregiudizi storici, logici e ideologici che non permettevano di superare il principio di «nessuna responsabilità senza colpa».

Le prime analisi italiane in merito alla presenza di ulteriori criteri di imputazione della responsabilità oltre alla colpa si devono a Venezian G., in *Danno e risarcimento fuori dei contratti*, Opere giuridiche, volume 1, Roma, 1919, pagine 75 e seguenti, ove si criticava la dottrina di Von Jhering R., che erigeva la colpa a criterio unico e principe del sistema della

di offrire una giustificazione alla presenza di tali diversi criteri (responsabilità per colpa e responsabilità senza colpa) all'interno del codice civile. La ragione di tali ipotesi derogatorie rispetto al principio della colpa venne trovata nei profondi mutamenti socio-economici risultanti dalle rivoluzioni industriali e nella esigenza equitativa di risarcire il danneggiato «attribuendo il danno a chi trae profitto dall'attività nel corso della quale esso si è verificato»[656]. Si evidenziavano i frequenti incidenti sul lavoro, che, in base al criterio della colpa, non portavano quasi mai ad una condanna al risarcimento da parte dell'imprenditore, e si scriveva:

> «Relativamente a queste attività accadeva troppo spesso che il principio della responsabilità per colpa si rivelasse insufficiente ad assicurare la riparazione del danno. E non a causa di una difficoltà di prova: l'esercizio di un'industria comporta necessariamente il verificarsi di tutta una serie di incidenti inevitabili, nonostante l'impiego della massima diligenza. Talvolta, poi, data la complessità dell'organizzazione, la colpa a causa del danno si fraziona in corrispondenza della divisione del lavoro il 1000 piccole quote trascurabili, ciascuna insufficiente a giustificare una responsabilità del suo autore; talvolta, infine, si verificano danni causati dalla momentanea imprudenza di un lavoratore; ma si tratta di gesti mala accorti o di disattenzioni inevitabili, nella routine del lavoro quotidiano, e spesso scusabili. Si pensi che una non trascurabile percentuale degli infortuni sul lavoro è causata dalla disattenzione dell'operaio stesso che ne è vittima: se neppure il timore della lesione o della mutilazione è sufficiente ad evitare tali imprudenze, tantomeno sarà sufficiente la minaccia della sanzione civile nel caso che esse cagionino danno ad altri»[657].

Si aggiungeva inoltre, che in base a degli studi psicoattitudinali condotti oltreoceano,

> «si è osservato inoltre che, mentre la maggior parte dei lavoratori non causa mai danni, una minore parte se ne rende ripetutamente responsabile. E dallo studio di questi ultimi è apparso che gli incidenti da essi causati non erano attribuibili a colpevole leggerezza, ma piuttosto la loro costituzione psicofisica, che li faceva meno destri, o meno pronti nelle reazioni, o distratti, ecc. Contro questa naturale tendenza a causare incidenti (accident proneness) la minaccia della responsabilità per colpa è assai poco efficace, poiché quei soggetti non possono mutare la propria natura e soprattutto perché normalmente non conoscono questa loro particolare predisposizione».

responsabilità civile. Il giurista italiano notava come già nel diritto romano, alcune fattispecie, non lasciavano spazio ad alcuna prova liberatoria, a prescindere dalla colpevolezza dell'agente.

[656] Trimarchi P., *Rischio e responsabilità oggettiva*, 1961, pag. 2.

[657] Ibidem, pag. 13.

Così, le suddette ipotesi eccezionali si qualificavano in termini oggettivi[658], in virtù del fatto che l'imprenditore era il soggetto più in condizione di sopportare il costo dei rischi. Esso, il costo dei danni realizzabili, veniva incluso nella normale logica dei ricavi e delle perdite[659]. La stessa dottrina, ad oggi, in termini diversi, si esprime ancora in tal senso, affermando che:

> «in ogni caso l'entità del rischio va confrontata con l'utilità sociale della condotta alla quale esso inerisce, tenuto conto del costo di rimozione di esso: quanto più grandi sono l'utilità sociale e il costo di rimozione, tanto più grande il rischio giustificato. Nell'analisi economica del diritto è d'uso tradurre questi concetti in una formula che pone a confronto il valore atteso del danno (cioè: l'ammontare del danno moltiplicato per la sua probabilità) e il costo della sua prevenzione»[660] .

Tornando all'oggetto della tesi, non è mancato chi, espressamente o tacitamente, abbia ritenuto di applicare tale dottrina alla responsabilità derivante da illecito trattamento dei dati personali, concludendo si tratti di una responsabilità oggettiva da rischio d'impresa (di natura extracontrattuale)[661]. Di seguito si pongono le ragioni per cui non si ritiene corretto interpretare l'articolo 82 GDPR alla luce di detto orientamento.

Innanzitutto, la dottrina in analisi poggiava su un assunto: la non adeguatezza del principio della colpa a regolare in modo soddisfacente le relazioni post-industriali: i problemi che si mettevano in risalto consistevano per lo più in danni all'integrità fisica, derivante da incidenti non voluti sul lavoro[662]. Così si reinterpretavano le norme del codice, che in modo ambiguo si alternavano tra il principio della colpa e l'assenza di esso, alla luce dell'analisi economica dei profitti e delle perdite.

Chi scrive ritiene però che proprio le premesse che hanno permesso a tale dottrina di affermarsi, siano radicalmente diverse da quelle sottostanti all'articolo 82 GDPR, che si tenta di reinterpretare. Si prenda come primo

---

[658] Ibidem, individua i casi di responsabilità oggettiva da rischio d'impresa nelle fattispecie *ex* 2049, 2051, 2052, 2053 e 2054 c.c.

[659] «La responsabilità oggettiva ha anche e soprattutto la funzione di attribuire all'impresa la sopportazione del rischio ad essa pertinente, quale parte dei suoi costi, in modo da determinare la sopravvivenza delle sole imprese e dei soli metodi di produzione socialmente attivi», ibidem, pag. 9.

[660] Trimarchi P., *La responsabilità civile: atti illeciti, rischio, danno*, 2021, pag. 82. In nota l'autore fa riferimento alla "regola Hand", che prende il nome dal giudice americano Learned Hand, che la enucleò nel caso U.S. vs. Carroll Towing Co. del 1947.

[661] Ad esempio, Tosi E., *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale*, 2019; Camardi C., *Note critiche in tema di danno da illecito trattamento dei dati personali*, 2020; Barbierato D., *Trattamento dei dati personali e «nuova» responsabilità civile*, 2019.

[662] Da notare come l'opera di Trimarchi P., *Rischio e responsabilità oggettiva*, 1961, ruoti intorno al danno da cose.

esempio il tipo di danni che non si riusciva a risarcire in virtù del problema della colpa: erano danni inerenti all'integrità fisica, causati accidentalmente dai lavoratori, in virtù di mancanze proprie di cui non erano consci, e difficilmente superabili. Chi scrive ritiene che il discorso sulla protezione dei dati personali sia diverso. Come si vedrà meglio nel prossimo capitolo, oltre ai danni prodotti accidentalmente dai soggetti che effettuano il trattamento, ben più preoccupanti sono le violazioni effettuate volontariamente, sia da parte di chi tratta legittimamente i dati, sia da parte di chi se ne impossessa illegalmente. Questi danni sono difatti prodotti con dolo, e non in virtù di una inadeguata «costituzione fisica». Se dunque, in quelle situazioni, il principio della colpa (e del dolo) poteva risultare insufficiente, ben potrebbe prestarsi ai casi di violazioni commesse volontariamente, o in virtù di errori evitabili con un'attenzione maggiore, o con investimenti superiori, proprie delle attività inerenti ai trattamenti di dati personali.

Risalta anche la differenza dei rischi che si intende prevenire: i danni all'integrità fisica della persona segnalati dalla dottrina in questione, messa a rischio dalle rivoluzioni industriali, contro i danni alla personalità, posta in pericolo dalla rivoluzione digitale, che il GDPR tenta di evitare.

Proseguendo, il sistema della colpa non produceva l'effetto desiderato anche in virtù del frazionamento della responsabilità dovuto alla complessità dell'organizzazione del lavoro. Pertanto, tale risalente (ma ancora attuale) orientamento, proponeva di addossare tutti i rischi in capo ad un unico soggetto, il quale appunto era colui che dalla attività traeva maggiore beneficio: l'imprenditore. Tale questione, nell'ambito della protezione dei dati personali, è risolta a monte dal legislatore europeo: la ripartizione delle responsabilità (come visto al paragrafo 4.2.1), è chiaramente delineata, ed attribuita al solo titolare del trattamento (e in casi specifici al responsabile), motivo per cui non si incorre nel pericolo di una non risarcibilità dovuta a frazionamento della responsabilità.

Ancora, il criterio oggettivo del rischio d'impresa poggia sulla distinzione tra attività biologiche e attività d'impresa, di cui si scrive:

> «esclusa dal campo delle attività biologiche, la responsabilità per rischio si applica principalmente alle attività d'impresa ma non solo ad esse: si pensi all'uso di un autoveicolo non più presso un imprenditore, bensì presso un privato. La condizione, necessaria e sufficiente, perché la responsabilità per il rischio svolga la funzione descritta, è che si tratti di un'attività la quale sia frutto di una decisione economica, o si voglia comunque condotta base a criteri di economicità, e che presenti un minimo di continuità o di organizzazione. Inoltre l'attività deve presentare un rischio non del tutto irrilevante»[663].

Come si vedrà meglio nel quinto capitolo, alcuni rischi del trattamento derivano dall'utilizzo dei dati personali nell'ottica di una influenza socio-

[663] Trimarchi P., *La responsabilità civile: atti illeciti, rischio, danno*, 2021, pag. 311.

politica degli interessati, ad opera dei titolari del trattamento. In molti di questi casi, l'attività rilevante non è condotta in base a criteri di economicità: non vi è profitto, non si parla di «conto attivo e passivo»[664]; tale orientamento esclude l'ambito delle attività biologiche da quelle cui dovrebbe applicarsi il criterio oggettivo del rischio d'impresa poiché in queste non è possibile rinvenire la logica dei profitti e delle perdite, su cui poggia suddetto criterio di attribuzione della responsabilità. Ebbene, in molti casi, neppure nelle attività di influenza socio-economica degli individui, perpetrate attraverso il trattamento di dati personali, è possibile riscontrare una logica economica. Dunque, anche in questo caso, non sembra possibile applicare il criterio del rischio d'impresa in virtù di una discrepanza tra le sue premesse e quelle che giacciono alla base dell'articolo 82 del GDPR.

Chi scrive ritiene che la generale condivisibilità di cui ha goduto il criterio del rischio d'impresa si debba alla sua grande coerenza con il contesto socio-economico in cui è stata elaborata. In moltissimi casi risulta tutt'oggi pienamente condivisibile. Tuttavia, vi sono dei casi in cui potrebbe non apprestarsi adeguatamente, e un esempio è dato dalle attività biologiche che la stessa dottrina esclude dall'ambito applicativo del criterio oggettivo in esame.

Si ritiene che l'ambito della protezione dei dati personali sia da escludere in egual modo, ma per diverse ragioni. Questa dottrina nasce in virtù di una constatata cedibilità del principio della colpa in relazione ai cambiamenti post-industriali, che oltre a grandi innovazioni, importavano dei rischi, specifici, inerenti per lo più all'integrità fisica. Così, brillantemente, si rileggevano le norme del codice civile, di modo da adeguarle al mutato contesto. Ora, per quanto riguarda il GDPR e l'articolo 82, tale ragionamento non sembra potersi riproporre. Come evidenziato al paragrafo 2.2[665], il Regolamento nasce in virtù della accertata impossibilità di regolare in modo soddisfacente la circolazione e la protezione dei dati personali, principalmente a causa dell'avvento dei *big data* e dei nuovi modelli di circolazione dei dati. La rivoluzione digitale ha importato dei nuovi rischi, non affrontabili adeguatamente con le previgenti discipline. Così, il Legislatore europeo ha adottato nel 2016 il Regolamento.

Chi scrive ritiene che, in virtù del fatto che i rischi del trattamento sono stati presi in esame dalla legge europea, e che questa sia fortemente indirizzata ad essi (*risck-based approach*), non si possa ricercare all'esterno del Regolamento un criterio utile a gestire tali pericoli. Mentre il principio della colpa nasceva in epoca molto precedente alle relazioni industriali ed ai relativi pericoli, l'articolo 82 GDPR viene alla luce proprio per affrontare i moderni rischi derivanti dal trattamento; in virtù di ciò, non si ritiene possibile cercare di reinterpretarlo nuovamente alla luce di altri criteri.

[664] Ibidem, pag. 310.
[665] Note 193 e 194.

Il criterio del rischio è già presente del Regolamento, non si può dunque apprestarne un altro, esterno. Si dovrà dare luce a quello previsto dalla legge europea (la discussione prosegue al paragrafo 4.6).

4.5 Danno risarcibile

Ci si è fin qui limitati a ricordare come l'articolo 82 prescriva la risarcibilità del danno materiale e immateriale (patrimoniale e non matrimoniale). In questo paragrafo si specificherà in quali casi è possibile parlare di danno come presupposto del diritto al risarcimento ai sensi dell'articolo 82 del GDPR.

Innanzitutto, in merito alla realizzazione del danno, come si vedrà meglio a breve, gli interpreti si sono divisi tra chi ha considerato la mera condotta illecita sufficiente ai fini di una pretesa risarcitoria (aderente dunque alla concezione di danno-evento), e chi l'ha ritenuta non sufficiente, in quanto dalla norma emergerebbe la necessarietà di un effettivo danno, valutabile oggettivamente, subìto dall'interessato (aderendo così alla concezione di danno-conseguenza)[666].
Prima di addentrarsi nella questione, occorre evidenziare come il GDPR definisca il danno. A tal proposito soccorre il considerando numero 146, secondo cui: «il concetto di danno dovrebbe essere interpretato in senso lato alla luce della giurisprudenza della Corte di giustizia in modo tale da rispecchiare pienamente gli obiettivi del presente regolamento». In virtù di ciò si desume che il concetto di danno va interpretato in senso lato e che la misura del risarcimento non possa essere ristretta da questo o quell'ordinamento nazionale (si intende così evitare il fenomeno del c.d. *forum shopping*)[667]. Tuttavia, si concede che un'interpretazione pretoria del concetto di danno possa portare ad una diversa ampiezza delle regole di responsabilità e dell'ammontare del danno da risarcire[668]. Essendo dunque il concetto di danno altamente interpretabile, il GDPR, al considerando 85, ne propone degli esempi:

[666] La distinzione tra danno-evento e danno-conseguenza è stata introdotta dalla Consulta nella sentenza numero 184 del 1986, ed è stata ampiamente discussa nelle notorie sentenze gemelle della Cassazione del 2003 (numero 8827 e 8828 del 31 Maggio); dalla Consulta nella sentenza numero 223 del 11 Giugno 2003; nuovamente dalla Suprema Corte nelle c.d. sentenze gemelle di San Martino (numero 26972, 26973, 26974 e 26975 del 11 Novembre 2008). L'ultimo intervento incisivo si deve alla sentenza della Cassazione numero 7513 del 27 Marzo 2018, tutt'ora seguito dalla giurisprudenza.

[667] Riccio G. M., Scorza G., Belisario E. (a cura di), *GDPR e normativa privacy*, 2022, pag. 726; Ratti M., *La responsabilità da illecito trattamento dei dati personali*, 2019, pag. 781.

[668] Riccio G. M., Scorza G., Belisario E. (a cura di), *GDPR e normativa privacy*, 2022, pag. 726.

«provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata».

Tornando alla divisiva questione predetta, occorre premettere che non è tanto il danno patrimoniale a destare perplessità, quanto invece il danno non patrimoniale[669]. In virtù di ciò si proseguirà esaminando la sua risarcibilità.

Secondo autorevole dottrina[670], la violazione del diritto alla protezione dei dati personali non richiederebbe la prova di un danno effettivo subito da parte del danneggiato, in quanto, in caso di violazione delle norme del Regolamento (*latu sensu*), il danno andrebbe considerato in *re ipsa* (danno-evento). Questo pensiero pone le basi su diverse argomentazioni. Vi è chi, rifacendosi alla lettera dell'articolo 82 GDPR («evento dannoso») e alla funzione deterrente della stessa previsione, ricava che «non si possa negare un risarcimento del danno anche per il semplice fatto che si sia verificata una violazione della sfera informativa dell'interessato»[671]. Altri invece si rifanno (riassumendo) alla specialità della disciplina relativa alla protezione dei dati personali: questa, infatti, sarebbe posta a protezione di diversi beni (si parla di plurioffensività del trattamento illecito dei dati personali), danneggiabili dalla violazione delle norme poste a loro tutela, come il diritto alla riservatezza, all'identità personale, alla protezione dei dati personali, all'immagine e all'oblio[672]. In virtù di ciò, in caso di violazione delle norme poste a tutela di tali interessi, e ad eccezione delle mere incidenze bagatellari, l'interessato-danneggiato non dovrebbe provare (come invece accade nel regime comune ai fini dell'*an debeatur*) le effettive conseguenze dannose, valutabili oggettivamente, della violazione: «la lesione di un diritto fondamentale della persona come quello alla riservatezza e alla protezione

[669] Per danno non patrimoniale si intende una categoria unitaria, come descritta dalle c.d. sentenze di San Martino della Suprema Corte, numero 26972, 26973, 26974 e 26975 del 11 Novembre 2008, quindi comprensiva le varie voci di danno biologico, danno morale e danno esistenziale.

[670] Tosi E., *Trattamento illecito dei dati personali, responsabilità oggettiva e danno non patrimoniale alla luce dell'art. 82 del GDPR UE*, in Danno e responsabilità, volume 4, 2020, pag. 435; Bilotta F., *La responsabilità civile nel trattamento dei dati personali*, 2019, pag. 464; Ratti M., *La responsabilità da illecito trattamento dei dati personali*, 2019, pag. 779.

[671] Bilotta F., *La responsabilità civile nel trattamento dei dati personali*, 2019, pag. 464. Nello stesso senso Camardi C., *Note critiche in tema di danno da illecito trattamento dei dati personali*, 2020, pag. 798.

[672] Sul punto di rimanda alle parole dell'autore: Tosi E., *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale*, 2019, pag. 9 e ss.

dei dati personali non può mai considerarsi bagatellare e il risarcimento del danno è in *re ipsa* in quanto discende dal trattamento illecito non conforme ai precetti conformativi protettivi del GDPR»[673].

Secondo tale filone di pensiero, dunque, l'ingiustizia del danno sarebbe prevista *ex lege* a monte dal Legislatore europeo, e, coerentemente, si ripudia una soglia minima di risarcibilità, appunto in quanto una violazione delle norme poste a tutela degli interessi predetti non potrebbe condurre ad un danno bagatellare («il profilo della gravità della lesione rileverà esclusivamente sotto il profilo del *quantum debeatur*»[674]). La lesione di un diritto personale rileverebbe quindi «in sé e per sé, perché il danno consiste proprio nella lesione del diritto personale, e se non se ne potesse stabilire un ristoro, allora dovrebbe dirsi che l'ordinamento non è in grado apprestare tutela ex post ai diritti che più di altri protegge nella forma della inviolabilità: il che sarebbe un paradosso inaccettabile»[675].

Altra parte della dottrina[676], sostenuta da consolidata giurisprudenza di legittimità[677], ha invece sostenuto la necessità della prova di un danno oggettivamente apprezzabile (danno-conseguenza). Secondo questa impostazione, la mera violazione dei principi e precetti conformativi non basterebbe per conferire all'interessato il diritto al risarcimento del danno, potendo al massimo essere la base per una sanzione amministrativa[678]. Questi dovrebbe pertanto provare in giudizio il danno sofferto. Una prima motivazione suggerita in dottrina[679] riposa sul tenore letterale dell'articolo 82 paragrafo 1, il quale statuisce: «…un danno materiale o immateriale causato da una violazione del presente regolamento…»; emerge dunque che la violazione del Regolamento e il danno sono due eventi separati, e che uno

---

[673] Tosi E., *Trattamento illecito dei dati personali, responsabilità oggettiva e danno non patrimoniale alla luce dell'art. 82 del GDPR UE*, 2020, pag. 435.

[674] Tosi E., *Trattamento illecito dei dati personali, responsabilità oggettiva e danno non patrimoniale alla luce dell'art. 82 del GDPR UE*, 2020, pag. 436. Nella stessa direzione anche alcune corti di ultima istanza europee: «*see e.g. French Cour de Cassation, 94- 14.798, where the court found that the mere finding there was an invasion of privacy as provided by Art. 9 French Civil Code gives a right to compensation; and the Romanian court in Curtea de Apel Cluj, Decizia nr. 88/ A, where the court found that 'there are situations where the existence of damage is not required as one of the conditions to receive compensation. The violations of the right to respect for private life as they are detailed in Article 73(a) to (i) of the New Civil Code may justify compensation by themselves, without having the need to prove damage exists, being self- sufficient in order to obtain compensation as provided by the New Civil Code'*», Zanfir-Fortuna G., *Article 82. Right to compensation and liabilty*, 2020, pag. 1176.

[675] Camardi C., *Note critiche in tema di danno da illecito trattamento dei dati personali*, 2020, pag. 798.

[676] Gambini M., *Responsabilità e risarcimento nel trattamento dei dati* personali, 2019, pag. 1068.

[677] Nota 653.

[678] Riccio G. M., Scorza G., Belisario E. (a cura di), *GDPR e normativa privacy*, 2022, pag. 725.

[679] Gambini M., *Responsabilità e risarcimento nel trattamento dei dati* personali, 2019, pag. 1068.

(la violazione) è causa dell'altro (il danno). Un simile argomento letterale è stato proposto in merito al considerando numero 75[680], il quale ripropone la medesima distinzione concettuale tra trattamento (illecito) e danno, e al considerando 85[681], che lega alla mancata notifica all'autorità di controllo relativa ad una violazione di dati personali, alla possibilità di causare danni fisici, materiali o immateriali.

Inoltre, tale impostazione risulta confermata dalle Sezioni Unite, secondo cui la tesi del danno *in re ipsa* «snatura la funzione del risarcimento, che verrebbe concesso non in conseguenza dell'effettivo accertamento di un danno, ma quale pena privata per un comportamento lesivo»[682].

In questa prospettiva, la risarcibilità è ammessa solo previo accertamento di una soglia minima di gravità della lesione[683]. In tal senso, la Suprema Corte ha statuito che la risarcibilità del danno non patrimoniale non si sottrae alla verifica della gravità della lesione e della serietà del danno[684], dato che anche per tale diritto opera il bilanciamento con il principio di solidarietà derivante dall' articolo 2 della Costituzione[685].

---

[680] Considerando numero 75 «i rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale…»

[681] Considerando numero 85 «una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche…»

[682] Cassazione, sentenza del 15 luglio 2014, numero 16133. *Contra*, Bilotta F., *La responsabilità civile nel trattamento dei dati personali*, 2019, pag. 464: «l'obiezione, in base alla quale in alcun modo il risarcimento del danno si trasformerebbe in una sanzione civile, è destinata ad infrangersi contro due argomenti. Prima di tutto, l'interpretazione delle norme europee non può essere vincolata dal rispetto della dogmatica nazionale. In secondo luogo, dal punto di vista del funzionamento del sistema di protezione dei dati personali, l'esistenza di una sanzione civile, che si affianchi a quelle amministrative e a quelle penali, costituisce un ulteriore incentivo per il titolare e il responsabile a tenere alta la soglia di attenzione e così predisporre (e successivamente a tenerle sotto controllo e aggiornarle) le misure idonee a impedire la violazione dei dati. In altri termini, nella logica della *accountability,* la sanzione civile rafforza quel meccanismo di controllo su e autocontrollo da parte di chi esercita un potere (in senso sociale oltre che giuridico)».

[683] Riccio G. M., Scorza G., Belisario E. (a cura di), *GDPR e normativa privacy*, 2022, pag. 727.

[684] Cassazione, sentenza numero 16133 del 15 Luglio 2014.

Per la definizione dei concetti di gravità della lesione e serietà del danno si rimanda a Calabrese G., *La responsabilità civile da illecito trattamento dei dati personali*, 2022, pag. 176 e ss.

[685] Cassazione, sentenza numero 16133 del 15 Luglio 2014: «il danno non patrimoniale risarcibile ai sensi dell'art. 15 del d.lgs. 30 giugno 2003, n. 196 (c.d. codice della privacy) non si sottrae alla verifica di "gravità della lesione" (concernente il diritto fondamentale alla protezione dei dati personali, quale intimamente legato ai diritti ed alle libertà indicate dall'art. 2 del codice, convergenti tutti funzionalmente alla tutela piena della persona umana e della sua dignità) e di "serietà del danno" (quale perdita di natura personale effettivamente patita dall'interessato), che, in linea generale, si richiede in applicazione dell'art. 2059 cod. civ. nelle ipotesi di pregiudizio inferto ai diritti inviolabili previsti in Costituzione. Ciò in quanto, anche nella fattispecie di danno non patrimoniale di cui al citato art. 15, opera il bilanciamento (siccome pienamente consentito all'interprete

Pertanto, non ogni danno non patrimoniale sarebbe risarcibile, ma solo quello che supera la normale tollerabilità[686]. A tale indirizzo giurisprudenziale aderisce autorevole dottrina[687]. Secondo questa impostazione, il danno subito, risultato dalla violazione della normativa sulla protezione dei dati personali, non è *in re ipsa*, dunque non tutti i danni sono idonei a fondare una pretesa risarcitoria. Si sottolinea come la Corte di Cassazione abbia precisato che il danneggiato debba dimostrare in maniera analitica il danno sofferto, non ritenendo risarcibile una generica sofferenza derivante dal trattamento illecito dei suoi dati personali[688].

La questione è senz'altro complessa, e non risulta agevole aderire totalmente all'uno o all'altro orientamento. Arrivare a risarcire ogni forma di lesione, anche quella minima, condurrebbe ad un incremento incontrollabile di liti bagatellari a fronte di risarcimenti di lieve entità. D'altro canto tuttavia, richiedere al danneggiato di provare questo o quel danno allo stato d'animo, e richiedere a questi di convertirlo in una pretesa risarcitoria quantificata, porrebbe a serio rischio la tutela degli interessi che sono posti alla base del Regolamento. Secondo chi scrive, la soluzione non può che trovarsi *in medias res*, dunque nel bilanciamento dei primari interessi posti alla base del GDPR ai sensi dell'articolo 1 paragrafo 3 («la libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali»). Condannare i titolari del trattamento al risarcimento per aver causato danni non patrimoniali minimi, potrebbe condurre ad un

---

dal modo in cui si è realizzata nello specifico l'interpositio legislatoris) del diritto tutelato da detta disposizione con il principio di solidarietà – di cui il principio di tolleranza è intrinseco precipitato -, il quale, nella sua immanente configurazione, costituisce il punto di mediazione che permette all'ordinamento di salvaguardare il diritto del singolo nell'ambito di una concreta comunità di persone che deve affrontare i costi di una esistenza collettiva». Nello stesso senso, Cassazione, sentenza numero 17383 del 20 Agosto 2020; Cassazione, sentenza numero 16402 del 10 Giugno 2021.

[686] «La giustificazione della cosi modulata "soglia di risarcibilità" del danno non patrimoniale, dettata dall'esigenza di arginare la "proliferazione delle c.d. liti bagatellari", si rinviene – come affermato dalla citata sent. n. 26972 del 2008 – nel "bilanciamento tra il principio di solidarietà verso la vittima, e quello di tolleranza, con la conseguenza che il risarcimento del danno non patrimoniale è dovuto solo nel caso in cui sia superato il livello di tollerabilità ed il pregiudizio non sia futile. Pregiudizi connotati da futilità ogni persona inserita nel complesso contesto sociale li deve accettare in virtù del dovere della tolleranza che la convivenza impone (art. 2 Cost.)», Cassazione, sentenza numero 16133 del 15 Luglio 2014.

[687] Riccio G. M., Scorza G., Belisario E. (a cura di), *GDPR e normativa privacy*, 2022, pag. 727, specifica casi di lesione tollerabile: «quali, a titolo esemplificativo, la ricezione di telefonate commerciali indesiderate o di e-mail pubblicitarie (c.d. spamming). Tali lesioni sono, infatti, risarcibili nel solo caso in cui il danneggiato dimostri che tali condotte abbiano una natura, per dir così, persecutoria (ad esempio, nel caso di centinaia di telefonate promozionali) oppure che, effettivamente, la condotta del titolare o del responsabile abbia cagionato una lesione effettiva in termini di turbamento o di stress psico-fisico». Critica all'eccesiva soglia di tollerabilità stabilita dalla giurisprudenza in Bolognini L., Pelino E., *Codice della disciplina privacy*, 2019, pag. 444 e pag. 447.

[688] Cassazione, ordinanza numero 16402 del 10 Giugno 2021.

disincentivo al trattamento dei dati personali a fronte di risarcimenti modesti. Con ciò, accogliere la dottrina del danno-evento, potrebbe risultare in contrasto con gli obiettivi posti dal Regolamento. Chi scrive ritiene che gli autori che propongono un'interpretazione del danno come danno-evento ricerchino interpretazioni delle norme in un'ottica di tutela; tuttavia, questa, non sembra essere la lente apprestata dal GDPR, che pone la libera circolazione dei dati personali (quantomeno) al pari dei diritti e delle libertà fondamentali che possono essere messe a rischio in virtù del trattamento dei dati. Ciò, conduce chi scrive ad aderire al filone giurisprudenziale poc'anzi esposto.

4.6 Il rapporto tra il regime di responsabilità e il principio di *accountability*: la prova liberatoria

Innanzitutto, secondo quanto detto finora, la prova liberatoria del titolare del trattamento può consistere nell'inesistenza del danno; l'esistenza di un danno al di sotto della soglia di tollerabilità; la mancanza di nesso eziologico; l'applicabilità del regime di responsabilità diretta del responsabile.

Infine, si esamina il caso dell'esistenza di un danno tangibile, al di sopra della soglia di tollerabilità, e legato dal nesso eziologico alla violazione del Regolamento da parte del titolare del trattamento.

Poc'anzi si è detto che l'attività di trattamento è di per sé pericolosa, eppure si continua a sostenere la natura soggettiva del criterio di responsabilità. Già dagli anni sessanta, la dottrina italiana si è scontrata con il problema dell'irriducibilità tra rischio e colpa (ritenuto da alcuni «falso problema» poiché l'unico elemento rilevante sarebbe la prova liberatoria[689]). In quegli anni ci si rese conto dei significativi mutamenti socioeconomici introdotti dalle rivoluzioni industriali; da ciò emersero le lacune di un sistema, quello incentrato sulla colpa, non perfettamente

[689] «Riemerge, così, il falso problema dell'irriducibilità tra rischio e colpa. Quello che rileva in tale frangente è il contenuto della prova liberatoria, qualificata allo stesso modo da entrambi gli orientamenti. Il titolare e/o il responsabile del trattamento dei dati, per andare immune da responsabilità deve dimostrare il caso fortuito e di aver posto in essere quanto è previsto dal principio di accountability; vale a dire: una corretta gestione del rischio; di aver approntato tutte le misure tecniche necessarie, da valutare caso per caso (art. 35); l'adesione a codici di condotta (art. 40), la presentazione delle apposite certificazioni (art. 42), ecc. È da ritenersi, comunque, più aderente allo «spirito» del Regolamento l'orientamento, che configura la responsabilità ex art. 82, come una responsabilità aggravata per colpa presunta, poiché tale qualificazione — che contempla il profilo soggettivo — risulta più coerente al principio di accountability e potrebbe rivelarsi, in un'ottica funzionale preventiva, più efficace nella valorizzazione del rimedio risarcitorio», Barbierato D., *Trattamento dei dati personali e «nuova» responsabilità civile*, 2019, pag. 5.

applicabile ai rischi tipici dell'industria[690]. Il sistema della colpa è estremamente risalente, e se ne proponeva una nuova lettura alla luce dell'industrializzazione dei rapporti economici.

Oggi, alcuni autori, propongono una lettura dell'articolo 82 del Regolamento alla luce dei risultati ottenuti in quegli anni, periodo in cui fervente dottrina poneva rimedio ad incoerenze sistematiche imputabili al Legislatore. Si propone dunque di leggere l'articolo 82 attraverso il criterio del rischio, non enunciato dal Legislatore europeo. Di esso si trova traccia solo nell'articolo 2050 c.c. Dottrina odierna, rilevata la rischiosità dell'attività di trattamento dei dati personali, interpreta la natura della responsabilità del titolare del trattamento in termini oggettivi, talvolta facendo leva su argomenti riconducibili alla teoria del *cheapest cost avoider*[691], talaltra chiamando nuovamente in causa l'articolo 2050 c.c. ecc. L'eterogeneità delle argomentazioni supportanti la classificazione in termini semioggettivi del criterio d'imputazione suggerisce la grande incertezza in materia, o meglio, l'assenza di parametri indicativi significativi. A tal proposito, la scelta di espungere l'articolo 2050 c.c. dal nuovo codice privacy si rivela, secondo di chi scrive, infausta.

Un'interpretazione dell'articolo 82 del GDPR attraverso il criterio del rischio enucleato e discusso negli anni sessanta non risulta condivisibile per due ragioni. La prima è di tipo storico: quanto fatto dagli autori citati era sicuramente condivisibile in quanto il principio della colpa non era stato enucleato in un'epoca come quella in cui essi scrivevano, e risultava cedevole di fronte ai mutamenti post industriali[692]. Il mondo era radicalmente diverso e una rilettura delle norme del codice civile si riteneva necessario. Il GDPR invece, come sottolineato al paragrafo 2.2, nasce proprio poiché ci si è resi conto dei cambiamenti e dei rischi importati dalla rivoluzione digitale. L'articolo 82 del GDPR dunque, ponendo come premessa i rischi derivanti dal trattamento dei dati personali (si è discusso

[690] «Senonché, verso la fine del 1800, per effetto delle trasformazioni economico-sociali dovute allo sviluppo dell'impresa e, con questa, alle occasioni di danno, la colpa ha perso il ruolo di unico criterio informatore della responsabilità. Furono soprattutto gli infortuni sul lavoro a provocare la reazione dei giuristi all'osservanza di dogmi che il più delle volte si risolvevano nel creare vere e proprie aree di irresponsabilità. La legislazione speciale di quegli anni allontanò il problema che si ripresentò di attualità successivamente all' entrata in vigore del nuovo codice civile. Infatti, pur prevedendo la colpevolezza nella norma di apertura del libro IV, titolo IX, il legislatore ha inserito ulteriori figure di responsabilità, nelle quali essa non vi figura», Franzoni M., *L'illecito*, 2004, pag. 158.

[691] Enunciata in Calabresi G., *Concerning Cause and the Law of Torts: An Essay for Harry Kalven Jr.*, University of Chicago Law Review, volume 43, questione 1, Article 8, 1975, pag. 84.

[692] «Gli istituti tradizionali, ormai millenari, dimostrano la grande affidabilità e certezza nella regolamentazione dei rapporti, ma, allo tempo stesso, possono mostrare le inadeguatezze di un sistema creato e pensato nella finalità di tutelare esigenze sociali ed economiche diverse. Il diritto, dunque, e inteso come un sistema *vivo, mutevole, flessibile* che, in qualche modo, reagisce di fronte alla continua evoluzione della società», Marighetto A., *La colpa e il rischio*, Revista da Faculdade de Direito, 18 Luglio 2018, pag. 219.

nel capitolo 3 dell'approccio improntato al rischio), non deve essere «riletto» sotto una lente differente da quella fornita dal Regolamento stesso. Non può essere reinterpretato alla luce dei rischi propri dell'attività di trattamento, in quanto questi sono stati già considerati a monte dal Legislatore europeo. Non si ritiene possibile dunque utilizzare criteri estranei a quelli forniti dal GDPR (come a breve si dirà, il criterio principe è costituito dal principio di *accountability*). La seconda ragione è strettamente connessa alla prima e si basa sul comportamento del legislatore del 2018 (decreto di armonizzazione). La scelta del legislatore europeo è stata quella di non sbilanciarsi, e di fornire solo gli elementi essenziali della responsabilità, lasciando agli Stati membri la possibilità di declinare l'articolo 82 GDPR in base alle proprie categorie. Il legislatore del 2018, sul punto, ha ritenuto di abrogare l'articolo 2050 c.c., lasciando gli interpreti sprovvisti di un appiglio normativo quantomeno semplificatore. La suddetta norma avrebbe difatti rappresentato in modo soddisfacente quanto previsto dall'articolo 82 del Regolamento: in particolare avrebbe adeguatamente rispecchiato sia la natura dell'attività di trattamento dei dati personali (essendo un'attività rischiosa, sia l'articolo 2050 c.c. che l'articolo 82 GDPR prevedono un'inversione dell'onere probatorio), sia il contenuto del principio di *accountability* (sia il citato principio che l'articolo 2050 c.c. richiedono infatti la prova di aver adottato tutte le misure idonee ad evitare il rischio). Le modalità dell'abrogazione, tuttavia, impediscono di poggiare il contenuto dell'articolo 82 GDPR sull'articolo 2050 c.c. e impongono un'innovata riflessione.

Si cercherà adesso di riempire il contenuto dell'articolo 82 GDPR sotto il profilo della prova liberatoria. Si sottolinea in apertura di analisi, come il legislatore europeo si sia mosso sulla stessa direttrice della Direttiva madre, che richiedeva al titolare del trattamento (responsabile secondo il lessico della Direttiva) di provare che l'evento dannoso non gli fosse imputabile. Nell'analisi di tale *quaestio*, si terrà in considerazione il dettato dell'articolo 82, il modello di responsabilità per fatto illecito e il criterio di imputazione per colpa oggettiva come descritti in precedenza.

Innanzitutto, in merito all'onere della prova, *nulla quaestio*: è il titolare, del trattamento a dover provare che l'evento dannoso non gli è in alcun modo imputabile. Come visto in precedenza, tale onere probatorio costituisce un'eccezione rispetto alla ripartizione ordinaria delineata dall'articolo 2697 c.c., e risulta sovrapponibile a quella del non più richiamato articolo 2050 c.c..; quanto appena detto si pone in linea di continuità con l'abrogato articolo 23 della Direttiva madre e l'articolo 15 del vecchio codice privacy. A ciò si aggiunge il generico obbligo di dimostrazione proprio del principio di *accountability*. Di contro, il danneggiato, dovrà provare la violazione del Regolamento, il pregiudizio patito e il relativo nesso eziologico.

In merito alla prova liberatoria e al suo riferimento letterale («l'evento dannoso non gli è in alcun modo imputabile») vi è chi ha sostenuto che nulla

sia cambiato rispetto a quanto previsto dalla Direttiva madre, e che dunque si debba ancora trattare di *strict liability*[693]. Chi scrive ritiene che invece vada operata una nuova valutazione, sebbene si riconosca che il tenore letterale dell'articolo 82 GDPR si innesti nel solco tracciato dall'articolo 23 della Direttiva madre. Innanzitutto, l'imputabilità del danno al titolare richiesta dall'articolo 82 GDPR, autonomamente considerata, non è un elemento in grado di fornire risultati appaganti sul piano della prova liberatoria che questi deve fornire per non essere condannato al risarcimento del danno; occorre dunque riempire di significato tale espressione, e in assenza di indicazioni legislative, o di giurisprudenza europea occorrerà interpretare la norma alla luce del «principio dei principi», quello di *accountability*[694].

Come visto nel capitolo 3, tale principio impone dei doveri inerenti alla previsione e prevenzione del rischio mediante la giustapposizione di adeguate misure tecniche ed organizzative, volte a garantire e a dimostrare la conformità al Regolamento. A ciò si unisce una serie di obblighi specifici (obblighi informativi ex artt. 13 e 14, registro dei trattamenti ex articolo 30 ecc.). Attenta dottrina[695] ha sottolineato come il rispetto di tale principio costituisca la prova liberatoria, mentre la sua violazione conduce all'obbligo risarcitorio (si rammenta l'adesione all'interpretazione del danno come danno-conseguenza). La difficoltà relativa alla dimostrabilità dei comportamenti richiesti dal principio di *accountability* in molti casi differisce. Si prendano come esempio la già discussa comunicazione all'autorità di controllo *ex* articolo 36, e le adeguate misure di sicurezza *ex* articolo 32. Se la dimostrazione dell'avvenuta comunicazione è estremamente facile (con relativa non condannabilità al risarcimento del danno *ex* articolo 82), lo stesso non si può dire in merito alla adeguatezza di

[693] Van Alsenoy B., *Liability under EU Data Protection Law*, 2016, pag. 283.

[694] «Art. 5.2 e 24.1 GDPR: *adeguatezza e responsabilizzazione* sono, si ribadisce, i parametri fondamentali attraverso i quali riempire di contenuto l'onere della prova liberatoria di cui all'art. 82.3 gravante sul danneggiante…», Tosi E., *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale*, 2019, pag. 132; Calabrese G., *La responsabilità civile da illecito trattamento dei dati personali*, 2022, pag. 129: «l'*accountability* è un principio più ampio della responsabilità civile e, anzi, quest'ultima è solo uno degli strumenti residuali che concorrono a rendere la prima vincolante: la responsabilità civile, che consegue al trattamento illecito, unitamente all'obbligo di risarcire i danni causati agli interessati, si conforma come presidio di garanzia complementare al sistema di controllo (e sanzionatorio) affidato alle Autorità garanti nazionali»; similmente, Amore G., *Fairness, Transparency e Accountability nella protezione dei dati personali*, 2020, pag. 422; Gambini M., *Responsabilità e risarcimento nel trattamento dei dati* personali, 2019, pag. 1017.

[695] Calabrese G., *La responsabilità civile da illecito trattamento dei dati personali*, 2022, pag. 127; Tosi E., *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale*, 2019, pag. 132; «proclamare l'autonomia concettuale della responsabilizzazione rispetto alla responsabilità, non vuol dire escludere l'influenza della responsabilizzazione sulla responsabilità. Infatti, l'imputabilità, la cui ricorrenza è essenziale per la pronuncia di una condanna risarcitoria, può essere letta alla luce della accountability», Bilotta F., *La responsabilità civile nel trattamento dei dati personali*, 2019, pag. 460.

una misura tecnica (come un *firewall*) atta a prevenire ed evitare il danno. Esemplificando, si ponga l'ipotesi del danneggiato che richiede il risarcimento del danno lamentando un nocumento derivante da omessa comunicazione all'autorità di controllo *ex* articolo 36 GDPR.

Si ponga poi l'ipotesi di un correntista di una banca che lamenti di essere stato danneggiato a causa di una violazione dei suoi dati personali ad opera di un terzo non autorizzato (hacker) e che leghi a livello eziologico il danno subìto all'inadeguatezza del *firewall* posto dalla banca a protezione dei suoi dati personali. Entrambi questi obblighi sono integrati dal generale obbligo di dimostrabilità, perno del principio di *accountability*, che, come si è detto, ammanta l'intero ordinamento[696].

Se però nel primo caso al titolare basterà allegare l'effettuata comunicazione (ad esempio tramite PEC) per essere esente dal dover risarcire il danno, la seconda ipotesi richiede una prova liberatoria diversa, più complessa, che, in virtù del principio di colpevolezza impresso all'articolo 2043 c.c. volgerà sul rispetto del principio di adeguatezza della misura richiesto dall'articolo 32 GDPR, e sull'elemento soggettivo della non colpevolezza in merito alla realizzazione del danno ingiusto. Innanzitutto, l'adeguatezza non è un valore assoluto: la misura dev'essere adeguata rispetto al danno che può verificarsi nell'ambito di quel determinato trattamento. Come anticipato nel terzo capitolo, affinché la misura sia idonea, è necessario che sia stata predisposta tenendo correttamente in considerazione lo stato dell'arte e dei costi di attuazione, nonché la natura, l'oggetto, il contesto e le finalità del trattamento, come anche, e soprattutto, il rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche[697].

---

[696] Vi è chi ha intravisto una differente natura di tali obbligazioni, classificandole secondo le categorie delle obbligazioni di mezzi e di risultato delineate in Mengoni L., *Obbligazioni di mezzi e obbligazioni di risultato*, Rivista di diritto commerciale, fascicolo 5-6,1954. Vedasi a proposito Van Alsenoy B., *Liability under EU Data Protection Law*, 2016, pag. 273; Calabrese G., *La responsabilità civile da illecito trattamento dei dati personali*, 2022, pag. 166; Wolters P. T. J., *The security of personal data under the GDPR: a harmonized duty or a shared responsibility?*, 2017, pag.172. Sebbene la Corte di Cassazione abbia superato tale distinzione, si può ritenere che, in virtù di quanto si è detto in merito ai limiti del principio di *accountability* (stato dell'arte e costi di attuazione), esso importi un obbligo di mezzi: un obbligo di fare quanto economicamente e tecnicamente possibile. *Contra*, Bilotta F., *La responsabilità civile nel trattamento dei dati personali*, 2019, pag. 460, che ritiene sia di risultato: «in questo senso, la loro è un'obbligazione (di risultato), che non consiste nell'evitare in ogni caso una violazione dei dati, ma nel predisporre in modo trasparente e controllabile tutte le misure (tecniche, organizzative e giuridiche) che si ha ragione di ritenere idonee a impedire la violazione dei dati e nell'attivare tempestivamente l'autorità di controllo appena si sia verificata una violazione, per cercare in tal modo di contenere i danni».

[697] «Il legislatore europeo chiede che la sicurezza del trattamento "adeguata al rischio" sia assicurata da «misure tecniche e organizzative adeguate». Il valore da attribuire all'adeguatezza non è assoluto, ma deve essere circostanziato. In tale contesto, il principio assume i connotati di "efficacia, appropriatezza", "pertinenza", ma anche di capacità di

Secondo autorevole dottrina[698], richiamando un orientamento giurisprudenziale formatosi nella vigenza del vecchio codice privacy (con conseguente classificazione in termini oggettivi della responsabilità), se le misure fossero state idonee, il danno non si sarebbe affatto prodotto[699]. Abbracciando però una responsabilità di tipo soggettivo, si ritiene che per condannare il titolare al risarcimento si debba andare oltre la mera constatazione della realizzazione del danno. Riprendendo l'interpretazione del combinato disposto dell'articolo 2043 c.c. e del principio di *accountability*, e applicandola al caso del danno subito dal correntista della banca, ci si dovrà chiedere se il danno ingiusto è riconducibile al comportamento colposo o doloso di quest'ultima.

Si ponga che, nel caso richiamato, la banca abbia diligentemente scelto il responsabile del trattamento, affidandosi ad una società sviluppatrice di *firewall* di chiara fama. Che, in linea con la DPIA svolta, abbia individuato un *firewall* in grado di aggiornarsi automaticamente ogni qualvolta vi fosse un aggiornamento disponibile. La scelta di una società informatica di livello, la DPIA, e il sistema di aggiornamento automatico indicano che la banca non ha sottovalutato i rischi realizzabili (dunque la fase di previsione del rischio è stata rispettata). Oltre all'acquisto del *firewall*, la banca ha anche stipulato con la stessa società un programma di controlli periodici trimestrali: ogni tre mesi, quegli stessi esperti, devono valutare lo stato dell'arte del *firewall*, di modo da verificarne l'adeguatezza. Unitamente a questo tipo di monitoraggio esterno, la banca impiega uno dei suoi addetti IT al controllo saltuario degli stessi sistemi di *firewall*. Tutto ciò, in modo da avere un controllore interno ed uno esterno.

Dopo 10 giorni dall'ultimo aggiornamento del *firewall* operato dalla società esterna, un hacker riesce ad aggirare il sistema di sicurezza, e con i dati acquisiti cagiona un danno al correntista. In un caso siffatto la banca sarebbe responsabile? Come predetto, per non essere condannata a risarcire il danno, dovrebbe dimostrare di aver ottemperato al principio di *accountability*.

La previsione dei rischi può dirsi rispettata: c'è stata una DPIA e una conseguente scelta di una società adeguatamente esperta per far installare il modello più avanzato del *firewall*, che in quel contesto è il tipo di misura da apporre per evitare una fuoriuscita dei dati (dunque misura adeguata attraverso un giudizio *ex ante*). Proseguendo, il principio di responsabilizzazione richiede l'aggiornamento delle misure: la banca ha previsto l'aggiornamento automatico e il controllo trimestrale del sistema di sicurezza ad opera della società esterna, unito ad un controllo interno. Anche l'organizzazione relativa all'aggiornamento delle misure può dirsi rispettata. Da meditare che tali controlli possono costituire costi significativi

---

soddisfare il risultato atteso (di sicurezza, appunto)», Giovannangeli S. F., *La violazione di dati o data breach*, 2019, pag. 396.

[698] Commento di Sica S., 2021, pag. 893.

[699] Cassazione, sentenza numero 15733 del 18 Luglio 2011.

per la banca. Secondo l'orientamento giurisprudenziale e dottrinale poc'anzi citato, essendosi cagionato il danno al correntista, evidentemente l'organizzazione della banca non poteva dirsi idonea, e ciò condurrebbe alla condanna *ex* articolo 82 del Regolamento. Secondo l'interpretazione di chi scrive, invece, il danno può ben verificarsi anche quando la misura può dirsi idonea. L'adeguatezza si dà infatti in base ai rischi che possono essere previsti. Qualora il rischio sia imprevedibile, la misura potrà comunque dirsi adeguata, altrimenti si richiederebbe una misura perfetta, volta a prevenire tutti i rischi possibili, immaginabili e non,che il Regolamento non richiede[700].

Si valuti quindi la condotta della banca in virtù del combinato disposto tra l'articolo 2043 c.c. e il principio di *accountability*: in un caso di scuola così delineato potrebbe dirsi che la banca ha tenuta la diligenza richiesta dal principio di *accountability*, visto l'impegno dimostrato nel rispettare gli obblighi di prevenzione del rischio previsti dal Regolamento. La banca-titolare del trattamento avrebbe potuto fare di più? Ciò avrebbe significato richiedere interventi pressoché giornalieri per ottenere l'adeguamento dello stato dell'arte del *firewall* ad opera di controllori interni ed esterni a tempo indeterminato. Vi è da chiedersi però se questo non conduca a costi d'attuazione eccessivi. I limiti della diligenza del titolare del trattamento, e quindi i confini del rispetto del principio di *accountability*, sono rappresentati dallo stato dell'arte e dai costi di attuazione. Si ammetta anche che una banca possa sostenere economicamente la rincorsa del più alto grado di stato dell'arte, ma, ad una piccola o media impresa quanto si potrà chiedere? Si è visto nel paragrafo 3.3 come anche una piccola impresa, qualora svolga principalmente la sua attività attraverso Internet, possa essere chiamata al maggior grado di diligenza nel rispetto del principio di *accountability*. Tale principio, avendo come limiti lo stato dell'arte ed i costi di attuazione, funzionerà in diversa maniera rispetto a questo o quel titolare del trattamento. Chiaramente, la valutazione della sostenibilità dei costi andrebbe fatta caso per caso, ma non risulta irragionevole ritenere che nel caso di una piccola o media impresa non possa richiedersi più di quanto visto poc'anzi per la banca; quest'ultima potrebbe invece incorrere in condanna.

Si ponga ora lo stesso caso, con una variante. Una settimana dopo il controllo della società esterna, la stessa società produttrice del *firewall* invia alla PEC della banca una comunicazione con cui si avvisa che è stato individuato un *malware* in grado di violare il *firewall*, e che il sistema di aggiornamento automatico potrebbe non essere sufficiente. Sarà dunque necessario applicare un *software* aggiuntivo in grado di integrare il *firewall* e ciò potrà essere fatto o in sede di prossimo controllo trimestrale senza costi aggiuntivi, o anche subito su richiesta della banca, ma con un costo aggiuntivo. La banca-titolare del trattamento sceglie di aspettare il controllo trimestrale, ma sfortunatamente, attraverso il *malware* segnalato dalla società produttrice del firewall, un terzo cagiona un danno ai correntisti.

[700] Calabrese G., *La responsabilità civile da illecito trattamento dei dati personali*, 2022, pag. 166.

Applicando adesso le suddette regole sulla responsabilità da fatto illecito, secondo chi scrive non potrebbe in questo caso ravvisarsi la massima diligenza richiesta dal principio di *accountability*. La banca aveva difatti previsto e segnalato nella DPIA rischi elevati ai dati personali dei correntisti, e ciò le richiedeva un alto grado di attenzione. Da ciò, la banca avrebbe avuto l'obbligo di far installare l'integrazione del *firewall* immediatamente. Inoltre, in questo caso non è neppure ravvisabile il limite dello stato dell'arte, vista la comunicazione via PEC da parte della società con cui si avvisava la banca della possibilità di porre rimedio; lo stesso può dirsi per il rischio imprevedibile, in quanto vi era un avviso chiaro della società. Allo stesso modo, per quanto concerne i costi d'attuazione, non può dirsi raggiunto il limite del costo atipico, in quanto un pagamento *una tantum* sarebbe sicuramente sostenibile per una banca, e ragionevolmente anche per una piccola o media impresa, specialmente se si sono individuati elevati rischi per gli interessati nella DPIA.

In virtù dell'onere probatorio invertito, la banca dovrebbe provare che il danno ingiusto non si è realizzato per sua colpa. La colpa è uno *standard* oggettivo, individuabile nelle norme che definiscono il rapporto obbligatorio. La banca ha violato il principio di *accountability* (nello specifico aspetto della sicurezza dei dati), dunque è in colpa. La violazione colpevole del principio di *accountability* è la causa del danno ingiusto patito dall'interessato[701].

Ne risulta che in quest'ultimo caso, secondo chi scrive, sia la banca che la piccola o media impresa dovrebbero essere condannate al risarcimento ai sensi dell'articolo 82 GDPR e 1218 c.c.

Una prova liberatoria siffatta, tuttavia, non differisce più di tanto da quelle proposte da altri autori che, partendo da posizioni differenti (rapporto contrattuale; criterio semi-oggettivo o oggettivo da rischio di impresa), giungono comunque a non abbracciare il criterio della causalità pura e ad ammettere una prova liberatoria coincidente con il limite dello stato dell'arte e del costo sostenibile. Questo è uno dei segni di una carenza di coerenza tra i vari criteri di responsabilità del codice[702]. Nell'analisi pratica

[701] La formulazione del caso relativo al *firewall* e alla banca trae spunto da un caso realmente accaduto, ed analizzato, in modo diverso in Wolters P. T. J., *The security of personal data under the GDPR: a harmonized duty or a shared responsibility?*, 2017 e in Calabrese G., *La responsabilità civile da illecito trattamento dei dati personali*, 2022, pag. 166.

[702] «La situazione che oggi si presenta all'interprete può riassumersi così: un impianto legislativo saldamente ancorato, almeno a livello declamatorio, al principio della responsabilità per colpa, salvo poche e bene delimitate eccezioni; una giurisprudenza che segue questo modello, e che poi se ne discosta talvolta sul piano operazionale; una dottrina che mostra, nelle sue punte più avanzate, segnali di attenzione verso una responsabilità oggettiva ma fatica ad ancorare questa posizione ad appigli saldi sul piano teorico, facendo del lungo cammino della responsabilità civile «una storia di ricerca della propria legittimazione», neppure oggi pienamente raggiunta», Smorto G., *Il criterio di imputazione della responsabilità civile. Colpa e responsabilità oggettiva in civil law e common law*, Europa e Diritto Privato, fascicolo 2, 2008, pag. 445.

dei casi, non è facile dedurre alcune differenze relative alla responsabilità oggettiva e soggettiva: ad esempio la differenza tra assenza di colpa e caso fortuito. Proseguendo, una differenza che solitamente si evidenzia tra responsabilità contrattuale ed extracontrattuale, è relativa alla risarcibilità dei danni non prevedibili: la questione, tuttavia, sembra superata dalle indicazioni dei limiti dello stato dell'arte, dei costi di attuazione e dal principio di adeguatezza relativo ai rischi prevedibili operate dal GDPR, che sembrano richiedere la non responsabilità per danni imprevedibili, a prescindere dalla qualificazione del rapporto giuridico che si possa operare.

Già in passato è stato evidenziato come in certi casi sia difficile distinguere tra la responsabilità soggettiva e quella oggettiva in senso lato. A proposito si è detto:

> «Superato il vecchio principio della imprescindibilità della colpa, si evita di approdare a un principio di bipolarità tra colpa e rischio o addirittura a un principio generale di responsabilità oggettiva, che sempre più si configura come una scelta eccezionale. Al contrario la responsabilità per colpa si conferma estremamente flessibile e modulabile e adatta — proprio in ragione di tali qualità — a tessere le maglie di una sorta di «unbroken chain between both extremities of subjective and objective liability». In particolare la responsabilità per colpa si rivela idonea a regolare quella «zona grigia» nella quale gravitano situazioni di pericolosità di «of medium intensity» tra il «rischio normale» inerente ad ogni attività umana e il rischio abnorme che giustifica la strict liability.)»[703].

Il sistema attuale della responsabilità civile, con cui si è costretti a confrontarsi, pone l'interprete a difficoltà dovute alla scarsa coerenza dei criteri sottostanti le varie fattispecie di responsabilità (artt. 1218, 2043, 2049, 2050 c.c. ecc.). Si è tentato di superare tali difficoltà in diversi modi, che tuttavia soffrono di un altissimo grado di subiettività[704].Rimane dunque, come unica differenza con ricadute pratiche, il diverso termine prescrizionale dell'azione di risarcimento *ex* articolo 1218 c.c. e quella *ex* articolo 2043 c.c.

---

[703] Pellecchia E., *La responsabilità civile per trattamento dei dati personali*, Responsabilità Civile e Previdenza, fascicolo 2, 2006, pag. 225 e ss. L'autore si riferiva qui all'articolo 2050 c.c., interpretato in chiave soggettiva.

[704] Uno di questi viene riportato in Bigliazzi Geri L., Breccia U., Busnelli F.D., Natoli U., *Diritto civile*, Utet, Torino, 1991: «per superare l'*impasse* a cui conduce la dicotomia «responsabilità per colpa-responsabilità oggettiva» si è cercato di recuperare su basi nuove l'unitarietà del sistema della responsabilità civile, individuando il dato costante di tale sistema nel fatto dannoso, a cui corrisponderebbe un'articolata molteplicità di criteri di imputazione. Uno di questi criteri sarebbe appunto la colpa; altri criteri -- solo per comodità riconducibili al concetto di responsabilità per rischio, inteso come «espressione ellittica, comprensiva dei criteri diversi» -- sarebbero, a seconda delle ipotesi legislativamente considerate, quelli «della preposizione, del diritto reale o della disponibilità del bene - mezzo dell'evento dannoso, dell'esercizio di un'attività pericolosa».

In conclusione, si riassumono adesso i connotati della responsabilità fin qui esaminati. Si è detto che, dal punto di vista dei profili soggettivi, gli unici soggetti ad essere gravati dalla sanzione risarcitoria civile sono il titolare ed il responsabile del trattamento. Premessa di ciò è che si realizzi un danno non minimo conseguente ad una violazione del Regolamento (*latu sensu*), imputabile ad uno dei soggetti predetti. Il criterio d'imputazione si è detto soggettivo, sebbene la prova liberatoria risulti parecchio angusta. Il rapporto è di tipo extracontrattuale, dunque si applica l'articolo 2043 c.c., unitamente al metro di impegno imposto dal principio di *accountability*. Si richiede al titolare del trattamento di provare che il danno ingiusto non sia derivato da sua colpa. Nei termini di una responsabilità soggettiva da fatto illecito ciò significa che deve provare o l'assenza del danno ingiusto o l'assenza di colpa nella realizzazione dello stesso. Il nesso causale può essere reciso da un evento non prevedibile e non superabile se non attraverso uno sforzo inesigibile nei termini dello stato dell'arte e dei costi di attuazione.

Nel prossimo capitolo si esamineranno i rischi odierni derivanti dal trattamento dei dati personali, e si ragionerà sulla seguente questione: se il modello di responsabilità fin qui delineato, che a seconda di chi scrive è quello più aderente alla lettera del Regolamento, è un modello idoneo a perseguire gli obiettivi di circolazione e protezione dei dati personali.

Capitolo 5 - *Accountability* e la responsabilità nel contesto dell'Internet of Things

Nei capitoli precedenti si è argomentato che il principio di *accountability* è il criterio attraverso cui interpretare le norme del Regolamento. Questo, nelle sue disposizioni principali, gli articoli 24, 25 e 32, impone che il titolare del trattamento valuti diversi fattori (in un momento anteriore al trattamento) per modulare la giustapposizione delle misure tecniche ed organizzative. Questi fattori sono: ambito di applicazione, contesto e finalità del trattamento, natura del trattamento e, soprattutto, i rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche. Nella prima parte del presente capitolo si descriverà l'elemento del contesto ossia l'*Internet of Things*. In un secondo momento si descriveranno i rischi per gli interessati che da tale contesto derivano. Successivamente si offrirà un contributo sulle difficoltà presentate dall'*IoT* nel rispetto del principio di *accountability*. Infine, si proporranno delle riflessioni sulle ricadute sulla responsabilità prevista dall'articolo 82 GDPR, con i relativi problemi irrisolti.

5.1 Il contesto dell'*Internet of Things*

Nei paragrafi 1.3 e 2.5 sono stati offerti alcuni esempi di ambienti *smart*; questi sono stati definiti come insiemi di oggetti intelligenti capaci di identificare e/o essere identificati in modo univoco, interconnessi tra loro attraverso Internet (o senza Internet) e capaci di percepire la realtà fisica in molteplici modi, sia attraverso un *input* umano sia autonomamente. Gli esempi vanno dal semplice e biunivoco rapporto tra una scheda di rete di uno *smartphone* e un sistema di gestione del traffico (sistema Mobywit), ad una strada setacciata con sistemi di riconoscimento facciale (esempio della polizia gallese), ad un ambiente interamente interconnesso (progetto Sphere). In questo paragrafo si intende porre in evidenza il modello di circolazione dei dati generati in questi ambienti: essi, nella maggior parte dei casi sono destinati a fuoriuscire da tali contesti, per poi perdersi nel grande mare delle informazioni digitali globali. Si prenderà come punto di partenza l'illuminante dottrina sociologica che negli ultimi anni ha edotto gli addetti ai lavori sul modello di circolazione dei dati personali generati dall'*Internet of Things*, e sulle strategie e finalità che questo nasconde.

È già iconica l'espressione «capitalismo della sorveglianza», la quale indica un concetto complesso, che in questa sede verrà specificato solo per le parti rilevanti ai fini della presente trattazione[705]. In particolare, sarà utile a spiegare come i dati prodotti dagli *smart object* non siano utili soltanto agli utilizzatori, ma ad innumerevoli altri soggetti.

Per capitalismo della sorveglianza si intende un «nuovo ordine economico che sfrutta l'esperienza umana come materia prima per pratiche commerciali segrete di estrazione, previsione e vendita»[706], e si cercherà di spiegare la sua intima connessione con l'Internet delle cose. È ormai pacifico come le informazioni raccolte dagli *smart devices* circolino sia verso l'interessato, sia verso terze parti, quali ad esempio le case produttrici del *device* o i gestori delle varie applicazioni ecc.; queste informazioni vengono prodotte e scambiate ininterrottamente, vista la richiesta di risposte in tempo reale, fino ad uscire dai contesti in cui sono state prodotte[707]. Ciò è dovuto a diversi fattori.

Innanzitutto, la questione della sicurezza è fondamentale: studi hanno verificato che i dispositivi tipici dell'*IoT* sono molto inclini a falle nella sicurezza; ciò sarebbe dovuto a questioni meramente tecniche. Risulta ad oggi particolarmente complesso dotare tali oggetti di adeguate misure di sicurezza. La resistenza della batteria e le capacità dei processori vengono impegnate quasi totalmente dai servizi offerti[708]. Mentre *smartphone* e pc sono progettati per essere aggiornati costantemente da remoto al fine di adeguare le misure di sicurezza allo stato dell'arte, oggetti intelligenti come

---

[705] L'opera principale cui si fa riferimento è di Zuboff S., *The age of surveillance capitalism*, PublicAffairs, 15 Gennaio 2019, nella sua traduzione ad opera di Paolo Bassotti, Luiss University Press, Roma, 2019.

Tuttavia, il dialogo sul tema era già stato avviato da innumerevoli altre opere. *Ex multis*, Berners-Lee T., Hendler J., Lassila O., *The Semantic Web*, Scientific American,17 Maggio 2001; Floridi L., *The Fourth Revolution: How the Infosphere is Reshaping Human Reality*, Oxford University Press, 2014; Mayer-Schönberger V., Cukier K. N., *Big data: A Revolution That Will Transform How We Live, Work, and Think*, Houghton Mifflin Harcourt, 5 Marzo 2013; Pasquale F., *The Black Box Society: The Secret Algorithms That Control Money and Information*, Harvard University Press, 2015; Hildebrandt M., *Law as Information in the Era of Data-Driven Agency*, The Modern Law Review, volume 74, Gennaio 2016; Mantelero A., *Responsabilità e rishio nel Regolamento UE 2016/679*, Nuove leggi civili commentate, volume 1, 2017.

A queste opere va sicuramente aggiunto il caso Snowden, che ha mostrato al mondo quanti fino a quel momento era soltanto stato immaginato.

[706] Zuboff S., *The age of surveillance capitalism*, 2019. Tra le diverse definizioni proposte dall'autrice questa sembra la più pertinente nell'ambito della presente tesi.

[707] Govanella F., *Le persone e le cose: la tutela dei dati personali nell'ambito dell'Internet of Things,* in Cuffaro V., D'Orazio R., Ricciuto V., *I dati personali nel diritto europeo*, 2019, pag. 1216.

[708] Yang Y., Wu L., Yin G., Li L., Zhao H., *A Survey on Security and Privacy Issues in Internet-of-Things*, IEEE Internet of Things Journal, volume 4, numero 5, Ottobre 2017, pag. 1251.

braccialetti[709] o suole delle scarpe[710] vengono pensati per essere piccoli e leggeri, anche se ciò significa non dotarli di adeguati sistemi di aggiornamento[711]. Negli anni si sono verificati molti attacchi alle infrastrutture *IoT*[712]: ad esempio, nel 2013, è stato inserito un file (*worm*) all'interno di alcuni *smart object*, e da questi si è diffuso fino ad infiltrarsi in più di centomila oggetti intelligenti, quali *smart* TV, microfoni senza fili, frigoriferi, telecamere di sicurezza connesse ad Internet ecc., rubando i dati generati da questi apparecchi[713].

La circolazione smodata dei dati può aversi anche in virtù di quanto scritto a chiare lettere nelle informative fornite dai titolari del trattamento. Queste spesso sono tutt'altro che *user-friendly*[714]. Nel 2018, l'artista Dima Yarovinsky ha rappresentato il problema attraverso un'installazione in cui si raffigurava la lungaggine di tali documenti[715]. Ad esempio, per leggere i termini e condizioni di Instagram, compresi di informativa, si richiede un tempo medio intorno agli 86 minuti. L'informativa assumerebbe nella protezione dei dati personali un ruolo fondamentale, tant'è che è sempre necessario fornirla. La *ratio* si ritrova nella volontà di porre rimedio all'asimmetria informativa esistente tra titolare del trattamento e

[709] Si pensi ai braccialetti Fitbit, in grado di raccogliere diversissimi tipi di informazioni.

[710] Ad esempio, sono state progettate suole intelligenti che attraverso algoritmi riescono a capire quando il soggetto che le ha indossate è caduto (il progetto è relativo agli infortuni delle persone anziane derivanti da cadute). Queste sono in grado, tra le altre, di raccogliere informazioni sulla posizione del piede, o sulla velocità di spostamento attraverso l'accelerometro. Attraverso una raccolta sistematica di tali informazioni possono dunque dedursi informazioni rilevanti la salute del soggetto che le indossa, sia in caso di caduta, che non. Tali informazioni, se rivendute o scambiate possono assumere molto valore. A proposito vedasi, Zitouni M., Pan Q., Brulin D., Campo E., *Design of a Smart Sole with Advanced Fall Detection Algorithm*, Journal of Sensor Technology, volume 9, 2019.

[711] Peppet S. R., *Regulating the internet of things: first steps toward managing discrimination, privacy, security and consent*, Texas Law Review, 1 Marzo 2014, pag. 135.

Si segnala tuttavia che tali problemi possono essere considerati superabili. Regola d'esperienza insegna come le grandi *tech-companies* siano maestre nel creare oggetti sempre più piccoli e potenti.

[712] Tra le più recenti ed importanti si menzionano le botnet HEC, EnemyBot e Kaiji.

[713] Peppet S. R., *Regulating the internet of things: first steps toward managing discrimination, privacy, security and consent*, 2014, pag. 133.

[714] Il considerando numero 58 del GDPR stabilisce che «il principio della trasparenza impone che le informazioni destinate al pubblico o all'interessato siano concise, facilmente accessibili e di facile comprensione e che sia usato un linguaggio semplice e chiaro…». L'espressione *user-friendly* viene utilizzata nelle Linee guida sui cookies e gli altri strumenti di tracciamento del Garante italiano del 10 Giugno 2021. Le linee guida sono disponibili online al seguente link: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9677876

[715] Yarovinsky D., *I agree*, 2018. L'opera è visionabile attraverso qualsiasi motore di ricerca.

interessato[716]. Malgrado ciò, lo stato dell'arte degli studi comportamentali rappresenta un quadro in cui solo un esiguo numero di interessati legge l'informativa, e ancor più rari sono i casi in cui questi abbiano gli strumenti per comprendere questioni molto complesse come quelle relative alla protezione dei dati personali[717]. Ciò induce gli utilizzatori di app e dispositivi *smart* ad accettare (più o meno inconsciamente) l'attuale modello di circolazione dei dati[718]. Inoltre, è stato dimostrato come in molte app, il semplice *download* autorizza la raccolta e la modifica anche di particolari categorie di dati[719]. In altre invece, al solo fine di attivare l'app, si richiede il trattamento di dati personali non funzionali rispetto al funzionamento del servizio offerto.

Nel 2013, il Gruppo di lavoro *ex* articolo 29 ha rilasciato un parere relativo alle applicazioni scaricabili sui dispositivi intelligenti[720]. In questo si scriveva che i sistemi operativi che permettono il funzionamento dei dispositivi (iOS, Android ecc.) comprendono dei *software* o strutture di dati che vengono messi a disposizioni delle app che vengono scaricate sul dispositivo. Il mezzo attraverso cui ciò è reso possibile sono le API

---

[716] Celeste E., De Gregorio G., *Digital Humanism: The Constitutional Message of the GDPR*, Global Privacy Law Review, volume 3, questione 1, 2022, pag.15.

[717] Caggiano I. A., *Il consenso al trattamento dei dati personali nel nuovo Regolamento europeo. Analisi giuridica e studi comportamentali*, Osservatorio del diritto civile e commerciale, fascicolo 1, Gennaio 2018, pag. 91. L'opera citata sottolinea come la prestazione del consenso è spesso funzionale ad un determinato scambio (di merci, servizi ecc.). In questi casi il consenso viene prestato per via di euristiche o altre scorciatoie cognitive, a prescindere dalla qualità dell'informativa apprestata dal titolare del trattamento; inoltre, va constatata la vaga percezione del valore della privacy nella coscienza sociale. Questi fattori, uniti alla specificità delle informazioni fornite agli interessati, conducono all'asimmetria informativa che relega l'interessato in una posizione di debolezza rispetto a quella del titolare del trattamento.

[718] «Nel 2018, il mercato globale delle *smart home* è stato valutato 36 milioni di dollari, e ci si aspetta che raggiunga i 151 miliardi entro il 2023. Prendiamo in considerazione un solo dispositivo per le smart home, il termostato Nest, realizzato da un'azienda di proprietà della Alphabet, la holding di Google…raccoglie dati sul suo uso e sul suo ambiente, e utilizza calcoli e sensori per "imparare" i comportamenti di chi vive in casa. Le app di Nest, inoltre, possono raccogliere dati da altri prodotti interconnessi, come auto, forni, tracker per il fitness e letti…Pensate per il wi-fi e per la condivisione in rete, le banche dati intricate e personalizzate di questo termostato vengono caricate sui server di Google. Ogni termostato prevede una *privacy policy*, un "consenso sui termini del servizio" e un "consenso dell'utente finale", che rivelano conseguenze opprimenti in termini di privacy e sicurezza, per le quali le informazioni personali e i dati sensibili vengono condivisi con altri smart device, con persone sconosciute e parti terze allo scopo di effettuare analisi predittive poi vendute a soggetti non specificati», Zuboff S., *The age of surveillance capitalism*, 2019, pag. 16.

[719] Di Landro A. C., *Big Data. Rischi e tutele nel trattamento di dati personali*, Edizioni Scientifiche Italiane, Napoli, 2020, pag. 41.

[720] Parere numero 2 del 27 Febbraio 2013 sulle applicazioni per dispositivi intelligenti (WP 202). Disponibile online al seguente link:
https://www.garanteprivacy.it/temi/internet-e-nuove-tecnologie/app

(*application programming interface*), ossia delle interfacce che permettono alle applicazioni scaricate sia di comunicare con componenti del dispositivo in questione, sia con altri *softwares* contenuti in altri dispositivi, o contenuti in *servers*[721]. Attraverso tali interfacce, le applicazioni (e quindi le case produttrici) hanno accesso ai vari sensori che rendono *smart* i dispositivi: si menzionano «giroscopio, bussola digitale e accelerometro per la velocità e la direzione del movimento; fotocamere frontali e sul retro per acquisire filmati e fotografie; un microfono per le registrazioni audio. I dispositivi intelligenti possono anche contenere sensori di prossimità; inoltre, possono connettersi attraverso una moltitudine di interfacce di rete, tra cui Wi-Fi, Bluetooth, NFC o Ethernet. Infine, è possibile determinare con precisione l'ubicazione grazie ai servizi di geolocalizzazione»[722].

A causa di tale interoperabilità, i singoli dati prodotti vengono copiati ed elaborati in tutto il mondo. Sempre il Gruppo di lavoro, nel 2014, scriveva in merito alle API di alcuni *smart object*, in particolare degli oggetti indossabili (*wearable computing*), e si chiariva che «la disponibilità di un'API per dispositivi indossabili (ad esempio, Android Wear) contribuisce alla creazione di applicazioni da parte di terzi, i quali possono quindi accedere ai dati raccolti da tali oggetti»[723]. Ancora, l'Enisa (Agenzia dell'Unione europea per la cybersicurezza) ha spiegato come la maggior parte delle applicazioni

---

[721] «*With the growing popularity of the web of things, several enterprises and organizations, including software providers like Amazon, Spotify and Google published their business functions online as web application programming interfaces (APIs) that can be remotely accessed.....In the past few years, some reputable web APIs repositories, such as mashape and programmable web, reported the fast growth in the number of published web APIs and their users. APIs play a significant role in software development since developers can achieve their programming tasks more efficiently with the help of APIs*», Nawaz M. S., Ur Rehman Khan S., Hussain S., Iqbal J., *A study on application programming interface recommendation: state-of-the-art techniques, challenges and future directions*, Library Hi Tech, Emerald Publishing Limited, 2021, pag. 2.

[722] Parere numero 2 del 27 Febbraio 2013 sulle applicazioni per dispositivi intelligenti (WP 202), pag. 4.

Nello stesso senso l'Agenzia dell'Unione europea per la cybersicurezza (Enisa) nello studio *Privacy and data protection in mobile applications*. del Novembre 2017: «*mobile devices can typically have access to various types of personal/sensitive data (such as wellbeing, health, medical data) provided by users via various mobile apps. Furthermore, standard handheld devices embed many and various sensors (microphone, camera, accelerometer, GPS, Wifi, etc.) that generate very personal and various data and metadata (location, time, temperature), that can have unexpected privacy impacts. For example, it has been shown that users can easily be identified and authenticated from smartphone-acquired motion signals, such as accelerometer and gyroscope (inertial) signals provided by most commercial smartphones [6]. Similarly, it has been demonstrated that mobile devices can sometimes be tracked from the capacity of their battery*», pag. 11.

[723] Parere numero 8 del 16 Settembre 2014 sui recenti sviluppi nel campo dell'Internet degli oggetti (WP 223), pag. 5. Il parere è disponibile online al seguente link:

https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/201

installabili degli *smart objects* sono state progettate combinando funzionalità e banche dati appartenenti a soggetti terzi; questi terzi a loro volta possono accedere ai dati generati da tali applicazioni cui prestano supporto. Così, questi ultimi raccolgono i dati da molteplici diverse applicazioni utilizzate da diversi interessati in relazione a diversi servizi: «*for example, a user might give one app permission to collect his/her location, and another app access to his/her contacts. If both apps used the same third-party library, the library's developer could link these two pieces of data together*»[724].

Secondo chi scrive, l'*Internet of Things* potrebbe essere descritto come un organismo pluricellulare, in cui ogni cellula costituisce un singolo *smart environment*. Ognuno di questi ambienti è però, in un modo o nell'altro, connesso ed influenzato dall'altro[725]. Potrebbe proporsi come ulteriore esempio quello dell'IA *as a service* (AIaaS): si immagini una società del mercato dei dati che fornisce servizi di *cloud storage* a soggetti terzi che vogliano immagazzinare lì i dati che ottengono attraverso i loro sensori; questa società potrà affidare ad ulteriori terzi i servizi di *computing*; quindi, quelli relativi all'analisi dei dati che ivi vengono immagazzinati. In questi casi i dati prodotti dagli *smart object* dell'impresa Tizio vengono immagazzinati nella nuvola di Caio, ed analizzati da Sempronio. I dati risultanti delle elaborazioni prodotti da quest'ultimo verranno poi scambiati con ulteriori soggetti[726].

L'enorme quantità di sensori attualmente esistente rende acquisibili tantissime informazioni relative a quello che viene percepito come mondo reale. Spesso, le informazioni prodotte vengono conservate anche dopo il trattamento al fine di essere scambiate con alti dati provenienti da altri soggetti. Ad ampliare il fenomeno della circolazione incontrollata si aggiunge

---

[724] Enisa, *Privacy and data protection in mobile applications*, Novembre 2017, pag. 13.

[725] *«…it is already common for data to flow from users via a mobile app to the app's provider, then potentially on to other third-parties (e.g. payment processors). In practice, this environment represents an interconnected system-of-systems, of which data is a driver»,* Singh J., Cobbe J., Norval C*., Decision Provenance: Harnessing Data Flow for Accountable Systems,* IEEE Access, volume 7, 16 Dicembre 2019, pag. 6562.

[726] «*For example, it may not be clear to a developer how an external AI as a Service (AIaaS) model actually works or how reliable its predictions are. Similarly, it may not always be apparent where data provided by online services comes from, or how sensors are calculating and pre-processing data before feeding it to the next component. This loss of contextual integrity risks the inadvertent misuse of that data, perhaps losing crucial information regarding how it should be used, information about biases or sampling errors, or other potential problems that could continue to propagate throughout the wider ecosystem*», Norval C., Cobbe J., Singh J., *Towards an accountable Internet of Things. A call for reviewability*, in Crabtree A., Haddadi H., Mortier R. (edito da), *Privacy by design for the Internet of Things; Building accountability and security*, Londra, 2021, pag. 4. Disponibile online al seguente link: https://arxiv.org/abs/2102.08132

il fattore delle banche dati aperte attualmente disponibili online, da cui possono essere prelevati i dati da combinare con quelli prodotti dagli *smart object*, di modo da poter analizzare più dati dello stesso individuo o gruppo di individui, così da essere maggiormente precisi. Lo stesso può dirsi dei *social network*, in cui tutti i giorni gli utenti condividono pubblicamente e volontariamente informazioni di qualsiasi tipo, dalle più "sensibili" (stato di salute, stato economico ecc.) a quelle che a primo impatto potrebbero essere "innocue" (gusti musicali o sport preferito); tutte informazioni queste, che se analizzate combinatamente a quelle prodotte dai *device*, possono dire molto della personalità dell'individuo[727]. Quanto appena esposto viene definito *linkage* (o *sensor fusion*[728]), e può aversi anche tra due dati non personali tutelati adeguatamente in *dataset* differenti: magari in quei due sistemi sono perfettamente anonimi poiché non ricollegabili ad altri dati dello stesso interessato, ma se combinati insieme a dati contenuti in un altro *dataset* allora possono divenire dati personali[729].

Attraverso questa enorme mole di dati è possibile dunque generare dei profili. La profilazione è espressamente prevista dal GDPR, che all'articolo 4 la definisce come «qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica». Essa è possibile anche quando inaspettata: nel momento l'interessato potrebbe accettare termini e condizioni per il trattamento indotto dal ritenere sicuro il trattamento in virtù della tecnica di anonimizzazione, ma come si è visto ciò potrebbe essere inutile qualora vengano combinate le banche dati[730]. Dal *linkage* è possibile non solo l'identificazione di un individuo, ma anche la deduzione non prevista dallo

[727] Talvolta gli oggetti intelligenti sono direttamente collegati ai *social networks*. Vi è chi parla dunque di *social Internet of Things*. A proposito vedasi Ramón Saura J., Ribeiro-Soriano D., Palacios-Marqués D., *Setting Privacy "by Default" in Social IoT: Theorizing the Challenges and Directions in Big Data Research*, Big Data Research, volume 25, 2021.

[728] «*Sensor fusion is the combining of sensor data from different sources to create a resulting set of information that is better than if the information is used separately. A classic example is the creation of stereoscopic vision—including depth information—by combining the images of two offset cameras. A new piece of information—about depth—can be inferred from the combination of two other pieces of data, neither of which independently contains that new information*», Peppet S. R., *Regulating the internet of things: first steps toward managing discrimination, privacy, security and consent*, 2014, pag. 121.

[729] Ziegler S. (edito da), *Internet of Things Security and Data Protection*, Springer, Ginevra, 2019, pag. 33.

[730] Wachter S., *Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR*, Computer Law & Security Review, volume 34, 2018, pag. 442.

stesso di ulteriori informazioni, quali il comportamento in un ambito specifico[731]. Allo stesso modo possono dunque essere dedotti particolari categorie di dati.

L'interesse per le informazioni, ma soprattutto per i risultati che da queste possono derivare, ha fatto sorgere figure professionali impegnate esclusivamente nell'analisi e nello scambio dei dati. È il caso dei c.d. *data broker*, che raccolgono quante più informazioni possibili dalle fonti pubbliche per poi rivendere i risultati dell'elaborazione ai soggetti interessati[732]. Queste descritte sono alcune delle principali modalità che portano i dati generati negli ambienti di *Internet of Things* a fuoriuscire da essi e dal controllo degli interessati. Una volta che tale soglia viene varcata entrano in gioco le *Big data analytics*, che come introdotto nel paragrafo 1.4.1, servono ad estrarre informazioni dalle informazioni. In particolare, ciò che si tenta di ricostruire sono i modelli comportamentali degli individui, sia da un punto di vista commerciale, sia da uno di tipo socio-politico. Nella teoria del capitalismo della sorveglianza, i dati relativi a tali modelli costituiscono per le imprese dell'*IoT* il c.d. «*surplus* comportamentale»: ciò che si vuole delineare attraverso le *analytics* è la previsione dei comportamenti commerciali o socio-politici degli individui. Il risultato di tale ricerca verrà poi venduta ai soggetti interessati o per proporre pubblicità mirata, o per influenzare politicamente e socialmente gli individui[733].

È stato anche evidenziato come la dimensione individuale non sia l'unico oggetto di analisi dei grandi *player* mondiali. Ciò che si cerca di ricostruire oggi sono anche le tendenze collettive di gruppi: «va tuttavia rilevato come, in questi casi, non si sia in presenza di gruppi nel senso tradizionale del termine, ovvero di gruppi preesistenti (quali ad esempio le minoranze), bensì di aggregazioni a geometria variabile, creati dai titolari del trattamento mediante l'impiego di algoritmi»[734].

Il meccanismo tecnico sottostante a tale contesto è molto complesso. Esso spesso coincide con gli algoritmi, veri attori moderni, ma soprattutto

---

[731] Ibidem.

[732] Stanzione P., *I "poteri privati" delle piattaforme e le nuove frontiere della privacy*, Giappichelli, Torino, 2022, pag.191.

[733] «Il capitalismo della sorveglianza si appropria dell'esperienza umana usandola come materia prima da trasformare in dati sui comportamenti. Alcuni di questi dati vengono usati per migliorare prodotti o servizi, ma il resto diviene un *surplus comportamentale* privato, sottoposto a un processo di lavorazione avanzato nome noto come "intelligenza artificiale" per essere trasformato in prodotti predittivi in grado di vaticinare cosa faremo immediatamente, tra poco e tra molto tempo. Infine, questi *prodotti predittivi* vengono scambiati in un nuovo tipo di mercato per le previsioni comportamentali, che io chiamo mercato dei comportamenti futuri», Zuboff S., *The age of surveillance capitalism*, 2019, pag. 17.

[734] Mantelero A., *Responsabilità e rischio nel Reg. UE 2016/679*, 2017, pag. 153; nello stesso senso Di Landro A. C., *Big Data. Rischi e tutele nel trattamento di dati personali*, 2020, pag. 43.

futuri, dell'era digitale. Questi sono stati definiti efficacemente *black boxes*, in quanto è estremamente difficile guardarvi dentro, e anche se si riuscisse a farlo sarebbe molto complesso capirne le dinamiche[735].

Quanto detto finora rappresenta la deriva del modello di circolazione dei dati, che prende la forma di una sorta di nuovo capitalismo, il quale si nutre di quante più informazioni possibili. Il nesso tra esso è l'*Internet of Things* è fondamentale, ed è stato ampiamente dibattuto: «voglio infine sottolineare che per quanto possa essere possibile immaginare un internet delle cose senza il capitalismo della sorveglianza, è impossibile immaginare un capitalismo della sorveglianza senza l'internet delle cose. Ogni richiesta dell'imperativo della previsione richiede tale presenza pervasiva "che sa e che fa" nel mondo reale»[736]. Nei successivi paragrafi si cercherà di comprendere come si comportano in tal senso gli istituti dell'*accountability* e della responsabilità apprestati dal GDPR.

5.1.1 Il dato personale e l'identificazione nell'*Internet of Things*

Nel paragrafo 2.3 si è offerto un breve inquadramento del concetto di dato personale, declinandolo nei suoi quattro elementi fondamentali (informazione, relativa a, una persona fisica, identificata o identificabile). Nel citato parere del 2007 del Gruppo di lavoro[737], per capire se un dato potesse essere collegato ad una persona fisica, si indicava lo *standard* dell'insieme di mezzi ragionevolmente utilizzabili dal titolare del trattamento (linguaggio del GDPR) o da altri ai fini dell'identificazione[738]. Il Gruppo di lavoro, nell'affermare ciò, riprendeva quasi pedissequamente il dettato del considerando numero 26 della Direttiva madre[739]. Nel 2014, il Gruppo di

[735] Si distingue tra «*"real" secrecy, legal secrecy, and* obfuscation», Pasquale F., *The Black Box Society: The Secret Algorithms That Control Money and Information*, 2015, pag. 6.

[736] Zuboff S., *The age of surveillance capitalism*, 2019, pag. 218.

[737] Parere numero 4 del 2007 sul concetto di dato personale (WP 136).

[738] «Se, tenendo conto dell'"*insieme dei mezzi che possono essere ragionevolmente utilizzati dal responsabile del trattamento o da altri per identificare detta persona*", quella possibilità non esiste o è trascurabile, la persona non dovrebbe essere considerata "identificabile", e le informazioni non configurerebbero "dati personali". Il criterio dell'"*insieme dei mezzi che possono essere ragionevolmente utilizzati dal responsabile del trattamento o da altri*" deve in particolare tenere conto di tutti i fattori in gioco. Il costo dell'identificazione è uno di questi fattori ma non l'unico», WP 136, pag. 15.

[739] Il considerando numero 26 recitava: «considerando che i principi della tutela si devono applicare ad ogni informazione concernente una persona identificata o identificabile; che, per determinare se una persona è identificabile, è opportuno prendere in considerazione l'insieme dei mezzi che possono essere ragionevolmente utilizzati dal responsabile del trattamento o da altri per identificare detta persona; che i principi della tutela non si applicano a dati resi anonimi in modo tale che la persona interessata non è più

lavoro emanava le linee guida relative alle tecniche di anonimizzazione, che come già detto nel paragrafo 2.4, sono utili a privare il dato personale degli elementi che permettono l'identificazione dell'interessato, di modo da renderlo un dato non personale (che esulerebbe dall'ambito applicativo del Regolamento, in quanto questo si riferisce soltanto ai dati personali). Nello stesso anno però, sempre il Gruppo di lavoro, in un parere specificatamente dedicato all'*Internet of Things*, scriveva che in virtù della notevole quantità di dati processati negli ambienti *IoT*, anche i dati che sembrano anonimi possono considerarsi dati personali[740].

Il GDPR, nonostante questa indicazione del Gruppo di lavoro, ha riportando pressoché la medesima definizione di dato personale[741], ribadendo la medesima scelta: tutelare solamente i dati personali[742]. Tale opzione risulta però in contrasto con il riconoscimento del modello globale di circolazione dei dati personali e con la presa di coscienza espressa dal Gruppo di lavoro secondo cui, anche i dati anonimizzati (in certi contesti) devono essere considerati dati personali.

Già diversi anni prima dell'approvazione del GDPR si era evidenziata la cedevolezza del concetto di dato personale[743]. Nel 2000 ad esempio, si dimostrò come semplicemente partendo dai dati di genere, data di nascita e codice CAP, si era riusciti a reidentificare l'87% della popolazione

identificabile; che i codici di condotta ai sensi dell'articolo 27 possono costituire uno strumento utile di orientamento sui mezzi grazie ai quali dati possano essere resi anonimi e registrati in modo da rendere impossibile l' identificazione della persona interessata».

[740] «Inoltre è possibile che anche i dati relativi a persone il cui trattamento avviene solamente in seguito alla pseudonimizzazione o addirittura all'anonimizzazione debbano essere considerati come dati personali. Di fatto la grande quantità di dati trattati automaticamente nel contesto dell'IoT comporta rischi di reidentificazione», parere numero 8 del 2014 sui recenti sviluppi dell'*Internet of Things*, adottato il 16 Settembre 2014. Si sottolinea che, nonostante non sia recentissimo, costituisce tutt'oggi l'unico riferimento espresso dal Gruppo di Lavoro sull'*IoT*. Disponibile online al seguente link:

https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9196041

[741] «*Even though the WP29 opinion concerns the concept of personal data in the DPD, it will most likely remain significant for data protection compliance after the GDPR becomes effective, since as Advocate General Kokott has observed, 'the latter will not affect the concept of personal data.'*», Purtova N., *The law of everything. Broad concept of personal data and future of EU data protection law*, Law, Innovation, and Technology, volume 10, questione 1, 2018, pag. 6.

[742] Sulla tutela dei dati non personali si dirà più avanti.

[743] «Alcuni casi recenti – come lo scandalo di Netflix o di America Online o, ancora, le scoperte del *genome-hacker* Yaniv Erlich – hanno disvelato le "broken promises" della *privacy* nell'era digitale, dimostrando come sia possibile risalire all'identità di una persona attraverso l'estrazione e l'aggregazione di dati non identificativi», Ducato R., *La crisi della definizione di dato personale del dato personale nell'era del web 3.0*, in *Le definizioni nel diritto*, Atti delle giornate di studio 30-31 ottobre 2015, Fulvio C., Tomasi M., Università degli studi di Trento, quaderni della facoltà di giurisprudenza, numero 26, Dicembre 2016, pag. 145.

americana[744]. Nel 2006, la società statunitense America Online pubblicato un *database* contenente dati personali pseudonimizzati dei suoi utenti. Dopo pochi giorni dalla pubblicazione però, il New York Times mise in luce come fosse facilmente aggirabile la misura tecnica di protezione posta in essere, e come si potesse dunque reidentificare gli interessati. Nello stesso anno, anche Netflix peccava di diligenza, e pubblicava un *dataset* avente ad oggetto le valutazioni degli utenti relative ai prodotti audiovisivi offerti; i dati, ritenuti anonimi[745], vennero presto ricollegati agli interessati, grazie all'ausilio di altre banche dati disponibili online[746]. Ancora, nel 2013 un gruppo di ricerca del MIT, nell'ambito di un esperimento, ha con successo reidentificato i partecipanti all'esperimento a partire dai soli campioni di DNA anonimizzati e pubblicati online a fini di ricerca. La modalità era stata la medesima: con l'ausilio di un algoritmo, si aveva incrociato tali dati anonimizzati a quelli presenti in alcune banche dati disponibili online.

Alla luce di questi e altri famosissimi casi, appare problematica la scelta del GDPR di mantenere la dicotomia dato personale - dato anonimo[747]. Ad oggi, le capacità identificative sono di gran lunga superiori, e in dottrina ci si è chiesti se tale binomio abbia ancora senso di esistere. Per una risposta negativa, autorevole dottrina suggerisce come nell'odierno contesto tecnologico ogni dato possa essere considerato dato personale[748]. Come

[744] Sweeney L., *Simple Demographics Often Identify People Uniquely*, 2000.

[745] Furono pubblicati gli indirizzi IP degli utenti. Oggi, il GDPR prevede espressamente gli indirizzi IP come dati personali (considerando numero 30).

[746] «…combinando le informazioni rilasciate per il "Netflix Prize" con altri dati disponibili *online* (come quelli dell'"Internet Movie Database"), due ricercatori dell'Università di Austin hanno dimostrato la possibilità di re-identificare quei dati. In particolare, è stato osservato come le informazioni relative ai punteggi dei film non solo fossero "semplici" dati personali, ma si trattasse di dati in grado di rivelare condizioni particolarmente intime: sulla base di questo assunto nel 2009 è stata incardinata una *class action* nella corte del Distretto Nord della California. I ricorrenti sostenevano, infatti, che la condotta di Netflix integrasse la violazione delle *privacy policy* contenute nel sito e che il rilascio del *dataset* avesse creato uno stigmatizzante fattore "Brokeback Mountain". In altre parole, la conoscibilità dei dati relativi ai gusti cinematografici era idonea a svelare preferenze politiche, religiose e, financo, sessuali», Ducato R., *La crisi della definizione di dato personale del dato personale nell'era del web 3.0*, in *Le definizioni nel diritto*, 2016, pag. 162.

[747] Per una panoramica sulle soluzioni presentate dalla dottrina in una prospettiva comparata prima dell'avvento del GDPR vedasi Ducato R., *La crisi della definizione di dato personale del dato personale nell'era del web 3.0*, in *Le definizioni nel diritto*, 2016, pag.147 e ss.

[748] Purtova N., *The law of everything. Broad concept of personal data and future of EU data protection law*, 2018; Sweeney L., *Simple Demographics Often Identify People Uniquely*, 2000; Schwartz P. M., Solove D. J., *Reconciling Personal Information in the United States and European Union*, California Law Review, 2014; Ohm P., *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, UCLA Law Review, volume

rilevato in precedenza, lo *standard* da applicare per capire se un dato sia personale o meno è rappresentato dall'insieme di mezzi ragionevolmente utilizzabili dal titolare del trattamento o da altri, motivo per cui, l'esistenza o meno di un dato personale si rileva solo al termine della valutazione del contesto in cui avviene il trattamento. Può ben accadere che al momento della raccolta dei dati si ritenga che questi non siano ricollegabili, neppure indirettamente, ad una persona fisica, e che in un secondo momento, in virtù di ulteriori strumenti che permettono l'identificazione o per via di ulteriori soggetti che partecipano al trattamento, essi siano reidentificabili[749]. A ciò si aggiungerebbe la scarsa affidabilità delle tecniche de de-identificazione; infatti, in virtù della vastità di dati in circolo, sarebbe sempre possibile, in un modo o nell'altro, reidentificare gli interessati[750]. Ad esempio, attraverso un sensore capace di captare un aspetto della salute fisica dell'interessato, è possibile capire se questo si stia muovendo oppure no; in base alla velocità ed altri fattori è possibile determinare anche il tipo di trasporto che si sta utilizzando (bici, piedi, macchina, aereo ecc.). Il modello di spostamenti che alla lunga si genera è unico, e questo permette a chi è in grado di determinare anche solo pochi fattori in merito ad un individuo, di derivare l'intero modello di spostamenti del soggetto, sfruttando dunque anche tutti gli altri dati anonimi presenti nel *dataset* che fino al momento prima erano impossibili da ricollegare ad una persona fisica[751].

Non sarebbe dunque prevedibile *a priori* l'identificabilità della persona fisica, e ciò è dovuto principalmente alla grande capacità computazionale che caratterizza questi tempi. L'uomo, nella capacità di ricollegare un dato ad un individuo, è stato superato dal potere algoritmico di cui sono dotate le macchine odierne: il modo in cui la mente umana e i computer riescono a conferire identificabilità ad un dato è diversa. Un algoritmo di *machine learning* potrebbe riuscire lì dove la mente umana non prevede correlazioni tra dato ed individuo[752]. La palla è dunque passata ai calcolatori, che

57, 2010; Tene O., Polonetsky J., *Big Data for All: Privacy and User Control in the Age of Analytics*, Northwestern Journal of Technology and Intellectual Property, 2013.

[749] Purtova N., *The law of everything. Broad concept of personal data and future of EU data protection law*, 2018, pag. 7.

[750] Ohm P., *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, UCLA Law Review, volume 57, 2010, pag. 1740 e ss.

[751] Peppet S. R., *Regulating the internet of things: first steps toward managing discrimination, privacy, security and consent*, 2014, pag. 130.

[752] «*The way all computers attach meaning to data is different from human cognition, e.g. computers have a different language and process data faster. Humans – albeit with proper training and effort - can still follow how traditional computers make sense of data: these computers follow deductive models, rules and cases. However, how meaning is 'attached' to data by modern machines is beyond the grasp of human mind. The game-*

riescono ad andare ben oltre la nostra vista (sin anche quella dei loro stessi progettatori)[753].

Particolare attenzione viene prestata ai c.d. *smart environment*, di cui si è detto ai paragrafi 1.3 e 2.5, in relazione ad uno degli indicatori che permettono di qualificare una informazione come dato personale. Il Gruppo di lavoro aveva infatti affermato che può aversi dato personale anche quando, pur non trattandosi di dati afferenti ad una persona fisica, il trattamento di quei dati sia in grado di provocare un impatto, anche non importante, sugli interessi e sui diritti di una persona[754]. Spesso negli ambienti interconnessi i dati raccolti non riguardano direttamente delle persone fisiche, si pensi ad esempio alla quantità di energia elettrica consumata nelle *smart grid*[755]; eppure, è stato dimostrato come anche da questo genere di informazioni si possa agevolmente risalire a dati personali degli abitanti della *smart home*[756]. Collegare tale tipo di informazioni a determinate persone fisiche non è cosa intuitiva; tuttavia, in contesti *smart*, in cui vengono immagazzinati grandissime quantità di dati, dotati di grandi

---

changer is a new generation of data-processing algorithms based on machine learning. Machine learning is the ability of computer algorithms to learn from data and make predictions for new situations,86 and improve automatically through experience.87 The new algorithms are autonomous, i.e. self-learning, self-repairing, and self-managing and form the core of the modern approach to Artificial Intelligence ('AI'), a strand of computer science aimed to build computers as intelligent agents. The way advanced AI self-learning algorithms make sense of data is not transparent even for their designers. Hence, the new AI algorithms work as a black box that is truly beyond human cognition», Purtova N., *The law of everything. Broad concept of personal data and future of EU data protection law*, 2018, pag. 12.

[753] «*In effect, we can no longer say that some data has no meaning for we really have lost to computers the monopoly of deciding that. In fact, it is safer to assume that all data – the number and frequency of steps or key strokes one makes daily, the colour of one's eyes or even how many leaves grow on a tree – potentially has meaning, even if not for humans. Hence, everything is data and all data has meaning; hence, everything is or contains information»,* Purtova N., *The law of everything. Broad concept of personal data and future of EU data protection law*, 2018, pag. 12.

[754] Parere numero 4 del 2007 sul concetto di dato personale, pag. 11.

[755] «*Many utilities are providing third-party companies access to troves of smart meter data. For instance, a recent report highlights one utility's practice of requiring its customer to consent to sharing their data with third parties before permitting them to use an online web portal*», Chen D., Kalra S., Irwin D., Shenoy P., Albrecht J., *Preventing Occupancy Detection From Smart Meters*, IEEE Transactions on Smart Grids, volume 6, numero 5, Settembre 2015, pag. 2426.

[756] «*In other words, some information is perceived as relevant more easily, for instance, information 'generated' by (observing) people (e.g. administrative records of people's off-line lives, and digital records of online behaviour like websites visited, texts and images uploaded; information generated through use of 'smart' objects and devices like phones or fitness bracelets), or objects people interact with (their cars, homes, computers)*», Purtova N., *The law of everything. Broad concept of personal data and future of EU data protection law*, 2018, pag. 14.

capacità analitiche e della possibilità di compiere autonomamente delle azioni, bisognerebbe presumere che ciò sia possibile[757]; in altre parole, vista la non prevedibilità del grande potere delle macchine, si dovrebbe assumere che anche dati relativi alla temperatura di una casa o della velocità di una macchina[758] siano dati personali[759]. Anche un dato anonimo, così, potrebbe essere qualificato come dato personale[760]: in virtù di ciò è stato affermato che ad oggi, vista l'estensione del concetto di dati personale, «*everything is or at least contains information*»[761].

Altra parte della dottrina[762] ha invece criticato tale impostazione, sostenendo quindi che la qualifica di dato personale vada operata caso per caso, ben potendosi dunque esservi dati non personali. Nello specifico sono stati criticati due punti. Il primo riguarda la premessa secondo cui il contesto tecnologico odierno dovrebbe portare ad una presunzione di personalità del dato: si legge infatti come le potenzialità delle tecnologie di cui si parla sono ancora in larga parte inespresse, e di come non si abbia ad oggi un'analisi completa di tutti i dati prodotti[763]. Si mette anche in discussione il fatto che

---

[757] «*Fitness may not predict creditworthiness; driving habits may not predict employability. We don't know for sure. There is reason to expect, however, that everything may reveal everything enough to justify real concern*», Peppet S. R., *Regulating the internet of things: first steps toward managing discrimination, privacy, security and consent*, 2014, pag. 122.

[758] Da ricordare come per il Gruppo di lavoro dato personale può aversi a prescindere dalla natura del dato, dal suo contenuto e persino dal suo formato (pag. 11).

[759] «*However, when increasing amounts of data are gathered in real time from increasingly connected environments, intended to be used in automated decisionmaking about us, and we do not know how the autonomous self-learning and selfmanaging computers draw meaning from data, we should always reasonably assume that any information is likely to relate to a person, since we cannot eliminate this possibility with certainty*», Purtova N., *The law of everything. Broad concept of personal data and future of EU data protection law*, 2018, pag. 14.

[760] Recenti sviluppi rilevano l'elevatissima possibilità, prossima alla certezza, di reidentificare dati anonimi. A proposito vedasi Rocher L, Hendrickx J. M., de Montjoye Y.-A., *Estimating the success of re-identifications in incomplete datasets using generative models*, Nature Communications, volume 10, articolo numero 3069, 2019: «*using our model, we find that 99.98% of Americans would be correctly re-identified in any dataset using 15 demographic attributes. Our results suggest that even heavily sampled anonymized datasets are unlikely to satisfy the modern standards for anonymization set forth by GDPR and seriously challenge the technical and legal adequacy of the de-identification release-andforget model*».

[761] Purtova N, *The law of everything. Broad concept of personal data and future of EU data protection law*, 2018, pag. 10.

[762] In particolare, Gellert R., *Personal data's ever-expanding scope in smart environments and possible path(s) for regulating emerging digital technologies*, International Data Privacy Law, volume 11, numero 2, 2021, pag. 202.

[763] «*The development of smart cities and their fast-paced deployment is resulting in the generation of large quantities of data at unprecedented rates. Unfortunately, most of the generated data is wasted without extracting potentially useful information and*

l'anonimizzazione sia pressoché inutile (sull'assunto che, in virtù della quantità di dati disponibili, si arriverebbe a trovarne altri che, se combinati permettono l'identificazione dell'interessato). Secondo la concezione espressa poc'anzi, l'anonimizzazione sarebbe ormai un residuo obsoleto[764]; secondo l'impostazione in esame invece, va effettuata un'analisi in più. Diversi autori hanno sostenuto la dimensione socio-tecnica dell'anonimizzazione: più in dettaglio, si sostiene che non vada preso in considerazione solo lo stato dell'arte delle tecniche di anonimizzazione, ma necessita di considerazione anche l'ambiente in cui esse vengono applicate. Il fattore ambientale viene suddiviso in quattro elementi: *other data, infrastructure, governance,* e *agency*. Si devono dunque prima valutare fattori come l'esistenza di altri dati cui combinare quelli anonimi per arrivare alla soglia minima dell'identificabilità («*other data*»), il *design* a livello *software* e *hardware* delle strutture in cui avviene il trattamento («*infrastructure*»), l'impianto organizzativo e procedurale in cui avviene il trattamento e l'anonimizzazione, quindi chi tratta i dati, il come si trattano i dati, secondo quali fini ecc. («*governance*») e l'azione necessaria di una persona fisica in particolare («*human agency*»)[765]. Alla luce di questi fattori va valutata la anonimizzazione, che passa da essere un concetto esclusivamente tecnico (prima impostazione) ad essere un concetto da contestualizzare oltre la tecnica. La mera tecnologia non sarebbe sufficiente a far venire meno il dato anonimo, sarebbe sempre necessaria l'azione di un soggetto in grado di compiere l'operazione materiale del mettere insieme le varie banche dati utili alla reidentificazione. Ciò in cui le predette impostazioni convergono, è la conclusione secondo cui il concetto di dato

knowledge because of the lack of established mechanisms and standards that benefit from the availability of such data…Anecdotal data indicates that when smart city data is not used for learning and analytics in a short-term, it is unlikely that it would be used later. It is estimated that by 2012 only about 0.5% of all 2.8 Zettabytes (ZB) of stored data have been analyzed and 3% of them are labeled based on a study by IDC1. This highlights the challenge of potentially wasting hidden information in 99.5% of the generated data», Mohammadi M., Al-Fuqaha A., *Enabling Cognitive Smart Cities Using Big Data and Machine Learning*: *Approaches and Challenges*, IEEE Communications magazine, volume 56, numero 2, 2018, pag. 1.

Per una esposizione più generica dei limiti attuali del *reinforcement learning* e del *deep learning* vedasi Brooks R., *Machine Learning Explained*, MIT Rethink, 28 Agosto 2017; nello stesso senso Hildebrandt M., O'Hara K., *Life and the Law in the Era of Data-Driven Agency*, Edward Elgar, 2020, pag. 4.

[764] A proposito vedasi anche Foglia C., *Il dilemma (ancora aperto) dell'anonimizzazione e il ruolo della pseudonimizzazione*, 2019.

[765] Mourby M., Mackey E., Elliot M., Gowans H., Wallace S. E., Bell J., Smith H., Aidinlis S., Kaye J., *Are 'pseudonymised' data always personal data? Implications of the GDPR for administrative data research in the UK*, computer law & security review, volume 34, 2018, pag. 231.

personale è destinato ad espandersi insieme alle tecnologie dell'informazione[766].

Secondo chi scrive, la seconda impostazione, che salva la dicotomia tra dato personale e dato anonimo, sarebbe più in linea con l'impianto del GDPR, mentre la prima lo metterebbe a rischio[767]. Tuttavia, aderire ad una o all'altra tesi non dipende da una scelta interpretativa; se anche si dovesse assumere come presupposto la previa analisi dell'ambiente specifico in cui avviene il trattamento, la questione rimarrebbe puramente tecnica. In altre parole, se anche valutassimo la presenza di Tizio e Caio, che trattano i dati in un modello organizzativo definito, con la possibilità di raggiungere questa o quella banca dati disponibile online, e la contestuale volontà di reidentificare certi dati, bisognerebbe ad un certo punto stabilire se con i mezzi tecnologici a disposizione in quel momento e in futuro, Tizio e Caio saranno in grado di reidentificare i dati.

Anche ammettendo che oggi la risposta possa essere sia positiva che negativa a seconda del contesto, nulla impedisce di affermare che in due, cinque o dieci anni, si debba assumere che sempre, a prescindere dal contesto, i dati saranno dati personali in virtù della loro identificabilità. Alla luce dei contributi tecnici esaminati, con l'obiettivo di conferire significato all'impianto del GDPR imperniato sulla dicotomia dato personale – dato anonimo, si ritiene più corretto affermare che al momento in cui si scrive si debba aderire alla tesi della natura socio-tecnica dell'anonimizzazione; si ammette però che in breve il contesto tecnologico potrà mutare a tal punto da far venir meno il senso del dato anonimo, e quindi, specularmente, del dato personale. A quel punto andranno ricercati approcci ulteriori rispetto a quello binario del GDPR. Una proposta che ha goduto di ampia considerazione in dottrina è stata coniata negli Stati Uniti, dove si è proposto di diversificare la regolamentazione dei dati in base al rischio di identificazione degli interessati[768].

5.2 I rischi per l'interessato

[766] Gellert R., *Personal data's ever-expanding scope in smart environments and possible path(s) for regulating emerging digital technologies*, 2021, pag. 207.

[767] Purtova N., *The law of everything. Broad concept of personal data and future of EU data protection law*, 2018, pag. 17.

[768] Si fa riferimento alle *personally identifiable information*, in Schwartz P. M., Solove D. J., *Reconciling Personal Information in the United States and European Union*, 2014.

Descritto il modello di circolazione dei dati, si discute dei rischi che da esso derivano, e dunque del fattore principale che il titolare del trattamento deve prendere in considerazione nell'adattamento delle misure tecniche ed organizzative. I rischi che si esamineranno hanno delle radici comuni: l'insufficienza del concetto di dato personale, la carenza di trasparenza che caratterizza il contesto descritto finora e la profilazione. I rischi sono tantissimi. Si è scelto di analizzarne solo alcuni, relativi, alla discriminazione, all'autodeterminazione dell'individuo e alla collettività, perchèriconducibili all'ipotesi di danno non materiale indicata dall'articolo 82 GDPR[769].

5.2.1 La discriminazione

In Europa la discriminazione è vietata in ogni sua forma. Le fonti del divieto sono molteplici, sia a livello nazionale che sovranazionale: l'articolo 14 della Cedu, l'articolo 21 della Carta di Nizza, l'articolo 3 della Costituzione italiana, l'articolo 21 della Carta ecc., fino ad arrivare a normative di settore: ad esempio, l'articolo 8 dello Statuto dei lavoratori (Legge numero 300 del 1970) stabilisce che «è fatto divieto al datore di lavoro, ai fini dell'assunzione, come nel corso dello svolgimento del rapporto di lavoro, di effettuare indagini, anche a mezzo di terzi, sulle opinioni politiche, religiose o sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore».

Le forme di discriminazione attuabili attraverso il trattamento di dati personali sono molteplici: vi è la discriminazione più conosciuta legata a questioni relative al genere, al sesso, all'orientamento sessuale, alla razza ecc[770]. Vi sono però anche forme di discriminazione particolari, quale quella economica. In questo paragrafo si esporranno alcuni esempi di discriminazione operabile attraverso il trattamento di dati personali, in particolare quello automatizzato, che a causa della grande quantità di dati disponibili rischia di esacerbare un fenomeno già troppo diffuso[771].

---

[769] Per una visione sinottica dei rischi derivanti dall'*Internet of Things* vedasi Ziegler S., *Internet of Things Security and Data Protection*, 2019, pag. 25 e ss.

[770] Per una vasta serie di esempi di discriminazione perpetrata attraverso l'analisi dei dati vedasi Romeri A., Ruggieri S., *A multidisciplinary survey on discrimination analysis*, The Knowledge Engineering Review, 2012.

[771] «*The main issue with discrimination is that people are inherently judgemental and have prejudices. These aspects are deeply embedded in human nature and the law is not capable of changing that. People will always judge others based on their religious or political beliefs, their gender, their sexual preferences and their life choices. Notwithstanding that society must work on strategies to increase tolerance, society cannot hope to change the mind set of human beings and force them to be more tolerant. Therefore, people need privacy and tools to enforce it in order to not be subjected to discrimination, especially considering how the Court describes the devastating power of discrimination for the individual and for society*», Wachter S., *Privacy: Primus Inter Pares — Privacy as a*

Si pensi ad un datore di lavoro, che per scegliere se assumere o meno un candidato effettui delle indagini relative al suo stile di vita. Questo potrà agevolmente servirsi dei dati forniti (gratuitamente o meno) dai collettori di dati relativi alle attività fisiche dell'interessato[772]. Ad esempio, potrebbe ricercare delle informazioni relative alle abitudini di sonno del candidato (fornite per esempio da applicazioni come Fitbit): è stato difatti dimostrato come, partendo da un dato che indica mancanza di sonno, si possa inferire uno scarso benessere psicologico dovuto a tristezza, o generici problemi di salute fisica[773]. Il datore di lavoro potrebbe, sulla base di queste informazioni, decidere di non assumere il candidato. Le informazioni sul sonno potrebbero essere ottenute anche attraverso le analisi dei dati forniti dalle reti elettriche intelligenti: mediante la valutazione del consumo di energia durante la notte potrebbe infatti dedursi un irregolare ciclo sonno-veglia, e così anche possibili depressioni. Dai dati forniti da applicazioni come Deliveroo[774] invece, potrebbe dedursi pigrizia, o addirittura una dipendenza da alcol, che potrebbe portare ancora alla mancata assunzione.

La discriminazione può anche essere di tipo economico. Si pensi all'impresa assicurativa, che voglia offrire i suoi prodotti a determinati clienti: assicurazione sulla vita a persone particolarmente in salute o un'assicurazione per infortuni sul lavoro a chi svolge mansioni d'ufficio ecc. Per trovare il cliente migliore, ossia quello da cui trarre più profitto al minor grado di rischio, essi potranno fare affidamento ad esempio sui dati forniti da app come Fitbit: magari relativi all'attività fisica, in quanto chi svolge regolarmente esercizi si ritiene abbia un'aspettativa di vita maggiore; allo stesso tempo un soggetto che mantenga un battito cardiaco regolare e basso durante l'orario 09-18:00 potrebbe indurre ad immaginare un lavoro d'ufficio, perfetto per un'assicurazione sugli infortuni. Ancora, non si riterrà opportuno concedere un'assicurazione auto a chi dorme poco, poiché potrebbe causare più incidenti. Così come si potrà effettuare una perfetta discriminazione dei prezzi: chi indossa un Apple Watch potrebbe essere un soggetto abbiente, o comunque avvezzo a certi tipi di acquisti[775]. La discriminazione può anche essere legata a fattori come la razza,

---

Precondition for Self-Development, Personal Fulfilment and the Free Enjoyment of Fundamental Human Rights, 22 Gennaio 2017, pag. 11.

[772] «*With so many potential data sources providing relevant information about a potential employee, an employer could turn to any number of commercial partners for information about that employee*», Peppet S. R., *Regulating the internet of things: first steps toward managing discrimination, privacy, security and consent*, 2014, pag. 120.

[773] «*Lack of sleep-which a Fitbit tracks-has been linked to poor psychological well-being, health problems, poor cognitive performance, and negative emotions such as anger, depression, sadness, and fear*», Wachter S., *Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR*, 2018, pag. 442.

[774] Compagnia specializzata nella consegna di cibo a domicilio.

[775] In questi casi si parla di *willingness to* pay. A proposito Di Landro A. C., *Big Data. Rischi e tutele nel trattamento di dati personali*, 2020, pag. 107; Peppet S. R., *Regulating the internet of things: first steps toward managing discrimination, privacy, security and consent*, 2014, pag. 123.

l'orientamento sessuale o le disabilità. Qualora un datore di lavoro non volesse assumere un individuo in base ad una specifica religione potrebbe ad esempio esaminare i dati connessi alla posizione del soggetto e determinare se la domenica si trova in chiesa, o il venerdì in moschea. È da segnalare come talvolta tali enormi flussi di dati inducano all'errore. Si immagini il datore di lavoro che voglia evitare di assumere soggetti pigri e si rifaccia ai dati sulle attività fisiche: il fatto che un individuo non effettui esercizi potrebbe sì essere ricondotto alla pigrizia, ma potrebbe anche essere frutto di una predisposizione genetica avversa. Un altro esempio potrebbe essere quello relativo alle questioni di peso, in quanto l'obesità non può essere correlata solamente all'indolenza[776]. Si potrebbe voler valutare un candidato anche in base alle sue idee politiche, ed in quel caso basterebbe verificare i suoi spostamenti durante lo svolgimento di eventi politici; o magari licenziare in forza di un orientamento sessuale sgradito, ed in questo caso basterebbe verificare la cronologia del browser relativa ai siti pornografici[777].

Vi è anche la possibilità che la discriminazione promani da un algoritmo e non dall'essere umano che lo utilizza[778]. Si pensi al caso del *software* di Amazon deputato al reclutamento di personale, che privilegiava le assunzioni maschili a quelle femminili[779]. A proposito va distinto il processo algoritmico totalmente automatizzato da quello che vede la partecipazione dell'uomo. Fino ad ora si è trattato il tema della discriminazione derivante dall'uomo che si serve dell'analisi operata dall'algoritmo; vi sono però casi in cui il procedimento e la decisione discriminatoria non vedono un ruolo umano. Per questi ultimi casi il GDPR ha previsto la tutela *ex* articolo 22, mentre i primi rimarrebbero scoperti. La *ratio* si intravede nel ruolo umano, considerato come una sorta di salvaguardia: l'uomo potrebbe verificare quanto fatto dall'algoritmo e decidere autonomamente[780]; dunque, non vi sarebbe bisogno di prevedere

[776] Peppet S. R., *Regulating the internet of things: first steps toward managing discrimination, privacy, security and consent*, 2014, pag. 126.

[777] Wachter S., *Affinity profiling and discrimination by association in online behavioural advertising*, Berkeley Technology Law Journal, volume 35, 2019, pag. 19.

[778] «*Not many trust models have been proposed for Internet of Things and the majority of them try to prevent trust-related attacks without considering the social selfishness behavior of the objects. They assume that all objects have the same behavior in providing service under all circumstances. However, in the real world, objects might be discriminative in cooperation with the others based on their social relationships, service providers' remaining resources, and the type of services requested. Therefore, objects behave differently in different contexts*», Jafarian B., Yazdani N., Haghighi M. S., *Discrimination-aware trust management for social internet of things*, Computer Networks, volume 178, 2020, pag.

[779] Cataleta M., S., *Diritti umani e algoritmi*, Nuova Editrice Universitaria, Roma, 2021, pag. 35.

[780] « *After all, a positive characteristic of humans would be to learn from our mistakes. According to the tradition, Seneca would have said: errare humanum est, perseverare autem diabolicum. The prohibition introduced by the GDPR concerning automated decision-making processes would, therefore, recognize that machines can err*

una tutela per tali casi. Tuttavia, è stato segnalato come spesso il ruolo umano sia meramente passivo, e non si traduca in altro se non in una esecuzione pratica dei risultati forniti dall'algoritmo, ecco perché il Gruppo di lavoro ha precisato che potrà aversi un trattamento completamente anonimizzato anche nel caso si abbia un intervento umano ma questo non si risolva in alcuna «influenza effettiva sul risultato»[781]. Per quanto concerne invece i processi totalmente automatizzati va sottolineato come il *machine learning* possa condurre a inferenze inaspettate: in questi casi le macchine non eseguono precise regole di comportamento impartite *ex ante*, ma procedono rielaborando le istruzioni attraverso algoritmi di apprendimento adattivi, così da giungere autonomamente alla decisione[782]. Secondo alcuni si sarebbe di fronte ad algoritmi che producono altri algoritmi[783]. Se si aggiunge che è ormai riconosciuto come questi non siano neutrali[784], ecco che si giunge alla discriminazione operata esclusivamente dalla macchina[785]. Questo avviene solitamente per difetti relativi alla progettazione del codice, per lo più sconosciuti anche ai programmatori; questi, infatti, progettano

and cannot be fully trusted», Celeste E., De Gregorio G., *Digital Humanism: The Constitutional Message of the GDPR*, 2022, pag. 13.

[781] «Per aversi un coinvolgimento umano, il titolare del trattamento deve garantire che qualsiasi controllo della decisione sia significativo e non costituisca un semplice gesto simbolico. Il controllo dovrebbe essere effettuato da una persona che dispone dell'autorità e della competenza per modificare la decisione. Nel contesto dell'analisi, tale persona dovrebbe prendere in considerazione tutti i dati pertinenti», linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679 del 3 Ottobre 2017, aggiornati il 6 Febbraio 2018 (WP 251).

[782] Troisi E., *Decisione algoritmica. Black-box e AI etica: Il diritto di accesso come diritto a ottenere una spiegazione*, Jus Civile, volume 4, 2022, pag. 954.

[783] *«Every algorithm has an input and an output: the data goes into the computer, the algorithm does what it will with it, and out comes the result. Machine learning turns this around: in goes the data and the desired result and out comes the algorithm that turns one into the other. Learning algorithms – also known as learners – are algorithms that make other algorithms. With machine learning, computers write their own programs, so we don't have to»,* Domingos P., *The master algorithm: how the quest for the ultimate learning machine will remake our world*, Basic Books, New York, 2015, pag. 6.

[784] «*An algorithm's design and functionality reflects the values of its designer and intended uses, if only to the extent that a particular design is preferred as the best or most efficient option. Development is not a neutral, linear path; there is no objectively correct choice at any given stage of development, but many possible choices…As a result, "the values of the author [of an algorithm], wittingly or not, are frozen into the code, effectively institutionalising those values"*», Mittlestadt B. D., Allo P., Taddeo M., Wachter S., Floridi L., *The ethics of algorithms: Mapping the debate*, Big Data & Society, volume 3, questione 2, Luglio – Dicembre 2016, pag. 7.

[785] «*This potential poses a dark side: unsupervised learning, or learning without human intervention and structure, could learn from data that codifies unfavorable or damaging social constructs (codified discrimination) or create its own discriminatory inferences (inferential discrimination*», Tschider C. A., *Regulating the Internet of Things: Discrimination, Privacy, And Cybersecurity in the Artificial Intelligence Age*, Denver Law Review, volume 96, questione 1, 2018, pag. 96.

portando con essi tutti i loro *bias*[786], che involontariamente vengono immessi nel sistema: «ad esempio, un sistema di AI basato su dati storici finisce col negare la libertà vigilata molto più facilmente agli afroamericani e suggerisce più facilmente l'invio di forze di polizia nei quartieri ad alta densità afro-americana, giacché in media negli Stati Uniti gli eventi di criminalità attribuiti ad afro-americani sono più numerosi di quelli attribuiti ai bianchi, a parità di circostanze»[787].

Ancora, la Corte europea dei diritti dell'uomo, in merito all'interpretazione dell'articolo 8 della Cedu, ha specificato che per rispettare alcuni aspetti della vita privata degli individui occorra essere tolleranti in merito a diversi stili di vita e opinioni differenti. Tale principio è stato pronunciato anche in una sentenza relativa al rispetto dell'identità di genere, tutelabile dunque ai sensi dell'articolo 8 Cedu, in cui si scriveva:

---

[786] In letteratura sono stati distinti *biases* preesistenti, *biases* tecnici e *biases* emergenti: a proposito vedasi Friedman B., Nissenbaum H., *Bias in Computer Systems*, ACM Transactions on Information Systems, volume 14, questione 3, Luglio 1996. Nella citata opera in merito al *bias* preesistente si scrive che «*has its roots in social institutions, practices, and attitudes. When computer systems embody biases that exist independently, and usually prior to the creation of the system, then we say that the system embodies preexisting bias. Preexisting biases may originate in society at large, in subcultures, and in formal or informal, private or public organizations and institutions. They can also reflect the personal biases of individuals who have significant input into the design of the system, such as the client or system designer. This type of bias can enter a system either through the explicit and conscious efforts of individuals or institutions, or implicitly and unconsciously, even in spite of the best of intentions. For example, imagine an expert system that advises on loan applications. In determining an applicant's credit risk, the automated loan advisor negatively weights applicants who live in "undesirable" locations, such as low-income or high-crime neighborhoods, as indicated by their home addresses (a practice referred to as "red-lining")*». Per quanto riguarda il *bias* tecnico si scrive che «*arises from the resolution of issues in the technical design. Sources of technical bias can be found in several aspects of the design process, including limitations of computer tools such as hardware, software, and peripherals; the process of ascribing social meaning to algorithms developed out of context; imperfections in pseudorandom number generation; and the attempt to make human constructs amenable to computers, when we quantify the qualitative, discretize the continuous, or formalize the nonformal*». Infine, sul *bias* emergente: «*while it is almost always possible to identify preexisting bias and technical bias in a system design at the time of creation or implementation, emergent bias arises only in a context of use. This bias typically emerges some time after a design is completed, as a result of changing societal knowledge, population, or cultural values. Using the example of an automated airline reservation system, envision a hypothetical system designed for a group of airlines all of whom serve national routes. Consider what might occur if that system was extended to include international airlines. A flightranking algorithm that favors on-line flights when applied in the original context with national airlines leads to no systematic unfairness. However, in the new context with international airlines, the automated system would place these airlines at a disadvantage and, thus, comprise a case of emergent bias. User interfaces are likely to be particularly prone to emergent bias because interfaces by design seek to reflect the capacities, character, and habits of prospective users. Thus, a shift in context of use may well create difficulties for a new set of users*».

[787] Di Landro A. C., *Big Data. Rischi e tutele nel trattamento di dati personali*, 2020, pag. 197; nello stesso senso Tschider C. A., *Regulating the Internet of Things: Discrimination, Privacy, And Cybersecurity in the Artificial Intelligence Age*, 2018, pag. 99.

«No concrete or substantial hardship or detriment to the public interest has indeed been demonstrated as likely to flow from any change to the status of transsexuals and, as regards other possible consequences, the Court considers that society may reasonably be expected to tolerate a certain inconvenience to enable individuals to live in dignity and worth in accordance with the sexual identity chosen by them at great personal cost»[788].

Un algoritmo non discriminatorio dovrebbe dunque essere intriso di concetti come la tolleranza, l'apertura rispetto alle diversità. Allo stesso modo dovrebbe però avere dei limiti entro cui agire per arrivare alla decisione più conforme all'obiettivo prefissato. Serie perplessità emergono se si pensa alla difficoltà di inserire e bilanciare tali concetti utili al rispetto della vita privata con i limiti entro cui la macchina deve necessariamente agire per raggiungere il fine desiderato. Nell'ambito di trattamenti di dati personali completamenti automatizzati basati sul *machine learning*, ad esempio, l'algoritmo dovrebbe essere in grado di distinguere il genere biologico dall'identità di genere, che non risulta ad oggi limitabile neppure con l'ausilio dell'immaginazione, e così decidere in base alla corrispondenza o meno tra i due concetti complessi. Solo un perfetto bilanciamento tra apertura e criteri decisori assicurerebbe un algoritmo preciso non discriminatorio nel presente e nel futuro (va infatti rammentato che attraverso l'apprendimento automatizzato queste macchine dovranno adattarsi all'emersione di nuovi orientamenti sociali).

Come si è accennato poc'anzi, nell'ambito delle decisioni totalmente automatizzate il Regolamento offre la tutela *ex* articolo 22, che al primo paragrafo stabilisce: «l'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona»; al terzo paragrafo si prevede invece che l'interessato ha «il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione». Dunque, si impone un intervento umano. L'articolo 22 GDPR va letto combinatamente ad altre norme, in particolare gli articoli 13, 14 e 15 GDPR (ed alcuni considerando di cui si discuterà a breve) e di queste ne tratterà il paragrafo 5.3.4.

5.2.2 L'autodeterminazione

La dottrina del capitalismo della sorveglianza ha messo in evidenza come grazie all'*IoT* sia possibile esercitare diversi tipi di influenza sugli

[788] Caso Christine Goodwin contro Regno unito, sentenza numero 28957 del 1995.

interessati: in particolare un'influenza di tipo economico, una di tipo strettamente personale e una di tipo socio-politico[789]. La protezione dei dati personali è difatti strumentale rispetto alla tutela di altri diritti e libertà fondamentali[790].

Il tipo di influenza economica è sicuramente la più diffusa, non a caso si parla di capitalismo[791]. Il surplus comportamentale è nella maggior parte idoneo ad effettuare il c.d. *micro-targeting*. Attraverso la grande mole di dati processata non solo si riesce a comprendere i gusti degli interessati, ma anche a prevedere cosa vorranno acquistare di lì a poco[792], o un loro possibile cambio di gusti. A tal proposito vi è chi parla di società dell'anticipazione, in quanto le grandi compagnie riuscirebbero ad influenzare talmente tanto gli individui da indurli a determinati comportamenti[793].

Si ponga l'esempio di una rete elettrica intelligente: attraverso un'analisi dei dati relativi al consumo della rete che mostri un abbondante consumo nelle ore notturne, si potrebbe dedurre uno stato di insonnia o altri disturbi legati al sonno. Tali informazioni divengono preziose nel momento in cui vengono vendute, ad esempio, a compagnie farmaceutiche; queste saranno così in grado di inviare pubblicità mirata relativa a questo o quel farmaco idoneo a curare i disturbi del sonno[794]. In tale modo non solo

---

[789] L'autodeterminazione è un concetto complesso e scomponibile in diversi aspetti. Si è scelto di parlare di questi soli tre profili poiché ritenuti i più rilevanti ai fini della presente tesi.

[790] «*What does that mean for data protection law? It not only protects citizens' personal data and thus their human dignity and informational self-determination. Data protection is also absolutely essential for a living democracy. Without data protection, the citizens' autonomy is threatened, and without this, a democracy cannot function. In short: data protection is a condition sine qua non for democracy*», Boehme-Neβler V., *Privacy: a matter of democracy. Why democracy needs privacy and data protection*, International Data Privacy Law, volume 6, numero 3, 2016, pag. 228.

[791] Riferendosi alla natura immateriale dei dati, alcuni autori hanno parlato di capitalismo senza capitale: a proposito vedasi Haskel J., Westlake S., *Capitalism without capital*, Princeton University Press, 2018.

[792] «Nel campo della contrattazione a distanza, ricorre la battuta secondo cui Amazon sarebbe in grado di far recapitare un bene prima che venga ordinato: è stata in effetti depositata negli Stati Uniti proprio da parte di Amazon, il 24 Dicembre 2013, un brevetto (n. 8615473 B2) per un servizio di «*anticipatory package shipping*», che comporterebbe la collocazione di prodotti nel magazzino più vicino a colui che sarà verosimilmente l'acquirente di un certo bene, sulla base di una previsione effettuata tramite l'analisi delle precedenti esperienze di acquisto e di navigazione sul sito effettuate da tale soggetto, «interpretate» anche alla luce dei *data base* della notevolissima casistica detenuta dalla stessa impresa», Di Landro A. C., *Big Data. Rischi e tutele nel trattamento di dati personali*, 2020, pag. 107.

[793] Raffiotta E. C., Baroni M., *Intelligenza artificiale, strumenti di identificazione e tutela dell'identità*, BioLaw Journal, numero 1, 12 Aprile 2022, pag. 168.

[794] «*However, such private information is potentially valuable. As one example, analysing energy data can reveal irregular sleeping patterns, e.g., based on sporadic energy usage at night, which pharmaceutical companies could use to inform direct marketing campaigns of insomnia drugs*», Chen D., Irwin D., *Weatherman: Exposing Weather-based*

l'interessato sarebbe indotto a comprare questo anziché quel prodotto, ma potrebbe anche essere portato a credere di avere problemi che invece non ha: si pensi al *broker* che per seguire l'andamento della borsa internazionale resta sveglio durante la notte; questi magari non avrebbe bisogno di un prodotto contro l'insonnia, ma potrebbe iniziare a riflettere sulla questione, e magari, invogliato da un particolare sconto potrebbe essere indotto all'acquisto. Un tipo di influenza siffatta intacca il profilo dell'autodeterminazione commerciale.

Diverso è il caso del rischio a quel tipo di influenza afferente allo sviluppo e la realizzazione personale. Della questione si è occupata in diversi casi la Corte europea dei diritti dell'uomo in merito all'interpretazione dell'articolo 8 della Cedu, e dall'analisi dei suddetti casi emergono una serie di interessi la cui tutela trova fondamento nella protezione dei dati personali[795]. Si legge come lo sviluppo libero da costringimenti della personalità si possa avere solo in ambiente indisturbato e tollerante[796], in cui si possa esprimersi senza timore di sorta, soprattutto di discriminazioni. Uno sviluppo libero della personalità individuale è funzionale al mantenimento del pluralismo, elemento essenziale di una società democratica[797]. Affinché gli individui possano esprimere liberamente il proprio pensiero è necessario che questi abbiano formato il proprio carattere, le proprie convinzioni, e ciò non sarebbe possibile in un ambiente ipercontrollato, che minaccia discriminazioni. Il timore di tali conseguenze può indurre al conformismo; questo erode il pluralismo e di conseguenza il livello di democraticità di una società[798].

Privacy Threats in Big Energy Data, IEEE International Conference on Big Data, 11-14 Dicembre 2017, pag. 1079.

[795] Nella sentenza numero 22009 del 25 Febbraio 1997 della Corte europea dei diritti dell'uomo in merito al caso Z contro Finlandia si legge: «*in this connection, the Court will take into account that the protection of personal data, not least medical data, is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life as guaranteed by Article 8 of the Convention (art. 8)*».

In Wachter S., *Privacy: Primus Inter Pares — Privacy as a Precondition for Self-Development, Personal Fulfilment and the Free Enjoyment of Fundamental Human Rights*, 22 Gennaio 2017, sempre in merito alla Corte Edu si legge che «*since the Court has no exhaustive definition of what constitutes privacy, personality and the private life, jurisprudence only gives an indicative list of life aspects that are the to be free from monitoring (freedom) as they enable self-development and development of personality. Lifestyle, life choices and concepts and the way of life have to be protected from state intervention. Independent life choices require the free and unobserved development of own abilities…Therefore, privacy is crucial for the development of personality*».

[796] «*The scope of the right to respect for private life is such that it secures to the individual a sphere within which he can freely pursue the development and fulfllment of his personality*», caso Deklerck contro Belgio, sentenza numero 8307 del 1978 della Corte europea dei diritti dell'uomo.

[797] Wachter S., *Privacy: Primus Inter Pares — Privacy as a Precondition for Self-Development, Personal Fulfilment and the Free Enjoyment of Fundamental Human Rights*, 22 Gennaio 2017, pag. 5.

[798] Ibidem.

Come visto, la dottrina del capitalismo della sorveglianza si fonda sul presupposto che attraverso gli oggetti intelligenti sia possibile monitorare costantemente e in modo pervasivo gli individui, non solo gli interessati ma anche chi interagisce con loro (si pensi ai dati immagazzinati nei *clouds* dagli *smart glasses*[799] o dai braccialetti intelligenti[800], o dalle telecamere intelligenti). Il livello di monitoraggio è già elevatissimo, e aumenterà[801]: si pensi che attraverso i dati raccolti da uno *smartwatch* è possibile desumere le risposte emotive degli interessati rispetto alla vista di determinate immagini[802].

Chi scrive ritiene che sia possibile ravvisare una maggiorata consapevolezza nella collettività in merito alle capacità di monitoraggio degli *smart object*; ad esempio, ci si accorge sempre di più che le pubblicità che arrivano non sono solo relative alle ricerche operate attraverso il *browser*, ma anche conseguenti a quanto detto a voce (dunque magari riconducibili all'attivazione non desiderata del microfono dello *smartphone*[803]). Il sentimento di essere monitorati sta aumentando come mai prima. Le tendenze odierne non stupiscono: letteratura psicologica già da tempo ha indicato il carattere transeunte dei limiti del concetto di privacy, definendolo un complesso processo dinamico[804].

---

[799] A proposito di questi si è espresso l'Edps nel *Technology report* numero 1 (*smart glasses and data protection*), in cui si sottolineava che «*data protection issues may arise whenever individuals within visual range are recorded, as this may happen without their knowledge, the recordings may be used for further data processing e.g. submitted to third parties in a cloud computing environment. Such situations may occur when recorded data is shared through social networks*», pag. 6.

[800] In merito ai braccialetti Fitbit l'ex presidente del Garante italiano ha espresso serie perplessità in quanto tali prodotti appartengono adesso a Google, la quale potrà combinare i dati prodotti da tali oggetti a quelli già contenuti nei propri *databases*. Intervista disponibile al seguente link: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9177921#:~:text=L'acquisizione%20di%20Fitbit%20da,Garante%20della%20privacy%20Antonello%20Soro.

[801] In Zuboff S., *The age of surveillance capitalism*, 2019, si legge un'intervista ad un architetto di sistemi *IoT*, che dice: «l'IOT è inevitabile com'era inevitabile che la conquista del West arrivasse al pacifico. È il destino manifesto. Nel mondo, il novantotto per cento delle cose non sono connesse. Per questo le connetteremo. Può trattarsi dell'umidità del suolo. Può trattarsi del tuo fegato. In quel caso è il *tuo* IOT. Il passo successivo è che cosa fare con i dati. Li visualizzeremo, ne troveremo il senso, e ci faremo dei soldi. in questo caso è il *nostro* IOT».

[802] In tal senso l'intervista al presidente del Garante italiano. Intervista disponibile al seguente link:

https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9552323

[803] «*Also, users are increasingly getting used to the possibility of voice control, supported by voice analysis agents such as Siri, Google Now, or Cortana. However, users are less aware of the fact that the voice control feature is realized by a device that is always listening in – at least to react on the defined control terms such as "Hey Siri", "Okay Google", or "Hey Cortana" – and therefore has access to all spoken communication*», in questo modo si esprimeva l'Enisa nello studio *Privacy and data protection in mobile applications*, pag. 11.

[804] Altman I., *Privacy Regulation: Culturally Universal or Culturally Specific?*, Journal of Social Issues, volume 33, questione 3, 1977, pag. 66 e ss.

Si ritiene dunque che, in breve tempo, quello che oggi è solo un timore, potrebbe divenire consapevolezza. La letteratura sul tema del monitoraggio perpetrato attraverso strumenti riconducibili all'*Internet of Things* è ormai vasta e non potrà che espandersi. Una volta che sarà diffuso il sentimento di controllo generato da questi *smart environment* potrebbe assistersi ad una riluttanza ad esprimersi liberamente[805]. Se la privacy intesa come spazio personale in cui ritirarsi per maturare la propria personalità indisturbati è senz'altro da tutelare[806], altro è non esprimere liberamente la propria opinione per timore reverenziale e dunque conformarsi al *mainstream*.

Si è detto prima in merito alle discriminazioni attuabili grazie all'enorme quantitativo raccolto nei vari *databases* grazie all'*IoT* (e ai motori di ricerca e ai *social networks*); il timore di essere controllati e di conseguenza discriminati potrebbe portare al conformismo. Negli ultimi anni Italia si assiste ad un dibattito inerente al politicamente corretto, che in certi casi imporrebbe una determinata narrazione pena (nel caso di dichiarazioni pubbliche) gogna mediatica, con conseguenze negative dal punto di vista personale e professionale. Tale timore potrebbe nei prossimi anni emergere in relazione non tanto a pensieri espressi pubblicamente, ma ad inferenze relative a momenti di vita privata. Si pensi agli odierni *kindle*, capaci di connettersi ad Internet: cosa succederebbe se si sapesse che un determinato personaggio pubblico sta leggendo il *Mein Kampf* di Hitler o Il Capitale di Marx? Una semplice lettura, per passione accademica, per pura curiosità o per arricchimento culturale, potrebbe divenire un'arma a disposizione di chi voglia screditare quella persona, magari rovinandole la vita. Allo stesso modo, già qualche anno fa, il Gruppo di lavoro aveva avvertito in merito ai rischi derivanti dai servizi di geolocalizzazione, oggi propri di praticamente qualsiasi *smart object*[807]: *smartphone*, *smartwatch*,

---

[805] «*The individual becomes aware of the existence of a process of automated decision-making and can consequently direct her behaviour in light of this information. Therefore, freedom to develop one's personality and personal freedom, as translated in the GDPR, imply the recognition of the principle of informational self-determination of the data subject*», Celeste E., De Gregorio G., *Digital Humanism: The Constitutional Message of the GDPR*, 2022, pag. 15.

[806] In tal senso Westin A. F., *Privacy and freedom*, Atheneum, New York, 1966; Boehme-Neβler V., *Privacy: a matter of democracy. Why democracy needs privacy and data protection*, 2016, pag. 225: «*no one can reveal all aspects of his personality to all people. Society is characterized by distinct individualization of the person and by dense, manifold relationships with many different people. These extreme differences in personalities of the people who have to deal with one another make it difficult to develop an understanding and to tolerate differences. You can therefore not reveal everything to everyone. Some needs, interests, and worldviews must remain hidden in some areas so that the tolerance of others' is not overstrained and conflicts are avoided*».

[807] Parere numero 13 del 16 Maggio 2011 sui servizi di geolocalizzazione su dispositivi mobili intelligenti: «un dispositivo mobile intelligente è intimamente connesso a un individuo specifico. La maggior parte delle persone tende a tenere i propri dispositivi mobili molto vicini, dalle tasche o dalla borsa al comodino, vicino al letto. Succede raramente che una persona presti questi oggetti ad un'altra. Per la maggior parte, le persone sono consapevoli del fatto che i loro dispositivi mobili contengono una certa quantità di

tablet, suole intelligenti per le scarpe, *smart glasses* ecc. dotati di geolocalizzazione diverranno la normalità. A causa di ciò vi sarà un enorme quantità di dati in grado di rivelare le informazioni più sensibili: si pensi ai dati di geolocalizzazione relativi ad una donna che indichino che negli ultimi mesi si è recata più volte presso una clinica per aborti, o nella sede di un determinato comitato politico. A quel punto si dovrà decidere se recarsi presso la clinica e rinunciare alla propria riservatezza, ose spogliarsi di oggetti che faranno parte della propria *routine* pur di tutelare quello spazio vitale per lo sviluppo della propria persona. Oppure si immagini il pagamento elettronico attraverso app che indica che Tizio e Caio, colleghi, si trovano spesso al motel vicino al luogo di lavoro durante l'orario del pranzo[808]. Ragioni fondate permettono di credere che non si rinuncerà a questi oggetti: «*in theory, people express concern about their threatened privacy; but their practical behaviour is completely different. They are very open, even careless, with personal data. However, that is not an indication for a lack of appreciation for privacy*»[809].

Uno sviluppo libero della propria coscienza, della propria personalità, non è compatibile con tali preoccupazioni. È stato segnalato come le opinioni inusuali, minoritarie, persino devianti, siano necessarie in una società

---

informazioni molto personali, che vanno da messaggi e-mail a fotografie private, dalla storia di navigazione del browser a, ad esempio, una lista di contatti. Questo consente ai fornitori di servizi basati sulla geolocalizzazione di ottenere una panoramica approfondita di abitudini e modelli di comportamento del proprietario del dispositivo e di costruire profili dettagliati. Da un modello di inattività notturna è possibile dedurre il luogo preposto al sonno, e dal modello di un percorso regolare la mattina è possibile dedurre l'ubicazione del datore di lavoro. Il modello può includere anche dati ricavati dai modelli di spostamento di amici, sulla base del cosiddetto grafico sociale. 6 Un modello comportamentale può anche comprendere speciali categorie di dati, ad esempio se rivela visite in ospedali o luoghi di culto, la partecipazione a manifestazioni politiche o la presenza in altri luoghi specifici, magari che rivelino dati sulla vita sessuale dell'utente. Questi profili si possono utilizzare per prendere decisioni che influiscono in misura significativa sul proprietario. La tecnologia dei dispositivi mobili intelligenti consente il monitoraggio costante dei dati di localizzazione. Gli smartphone possono raccogliere permanentemente segnali da stazioni base e punti di accesso WiFi. Tecnicamente, il monitoraggio può avvenire segretamente, senza che il proprietario ne sia informato. Il monitoraggio può anche essere effettuato semi-segretamente, quando le persone "dimenticano" o non sono adeguatamente informate sul fatto che i servizi di localizzazione sono attivi o quando le impostazioni di accessibilità dei dati di localizzazione vengono modificate da "privato" a "pubblico". Anche quando le persone rendono intenzionalmente disponibili su Internet i propri dati di geolocalizzazione, attraverso servizi di posizionamento e geotagging, l'accesso globale illimitato pone nuovi rischi, che vanno dal furto di dati all'effrazione, o addirittura a episodi di aggressione fisica o stalking. Come per altre nuove tecnologie, un rischio rilevante insito nell'uso di dati di localizzazione è la function creep, o estensione indebita delle funzionalità, ossia il fatto che sulla base della disponibilità di un nuovo tipo di dati si possano sviluppare nuove finalità che non erano previste al momento della raccolta dei dati».

[808] Blumberg A., Eckersley P., *On locational privacy and how to avoid losing it forever*, Electronic Frontier Foundation, 2009.

[809] Boehme-Neβler V., *Privacy: a matter of democracy. Why democracy needs privacy and data protection*, 2016, pag. 226.

democratica, e affinché si realizzi questo è necessario che gli individui abbiano potuto sviluppare liberamente le proprie opinioni[810]. La riservatezza e la protezione dei dati personali sono strettamente funzionali alla possibilità di essere liberi ed autonomi: solo così le persone possono sviluppare i propri pensieri. Questo è uno degli aspetti della vita personale che si vuole tutelare attraverso il diritto alla protezione dei dati personali, e che il titolare deve tenere a mente durante il trattamento.

In linea con quanto argomentato, il Gruppo di lavoro nel parere sull'*IoT* faceva luce sull'impatto che i moderni *smart object* hanno sugli individui, evidenziando come la sorveglianza perpetrabile attraverso tali oggetti potrebbe esercitare una pressione sulle persone, conducendole a non tenere comportamenti non comuni, per paura che possano essere percepiti come anomalie[811].

Un altro tipo di influenza operabile riguarda poi l'autodeterminazione socio-politica. Celeberrimo il caso relativo alla società Cambridge Analytica, che durante le elezioni statunitensi del 2016 avrebbe favorito il politico Donald Trump utilizzando circa 87 milioni di dati provenienti da Facebook[812]. In quel caso erano stati raccolti i *likes*, a cui poi era succeduta una fase di influenza relativa alle convinzioni politiche degli utenti[813].

La fonte dei dati era stata in quel caso un *social network*; tuttavia, quanto accaduto può essere riproposto anche nell'ambito dell'*Internet of Things*.

Questa volta si tratta però di un'interferenza diversa rispetto a quella sull'autodeterminazione personale. Se in quest'ultimo caso è il sentimento di monitoraggio che rende complicato lo sviluppo della personalità, nel caso

---

[810] «*Social psychological studies show that committed minorities can change the majority's opinion.Such processes can only be initiated when people resist group pressure and actually contradict the majority opinion. Usually only people who have sufficient personal autonomy are successful in doing this*», Boehme-Neβler V., *Privacy: a matter of democracy. Why democracy needs privacy and data protection*, 2016, pag. 227.

[811] «Oltre a ciò, l'analisi basata su informazioni raccolte in un ambiente IoT potrebbe permettere di rilevare i modelli di comportamento e di vita della persona in maniera ancora più dettagliata e completa. Infatti, è probabile che questa tendenza abbia un impatto sul modo in cui la persona si comporta, così come è stato dimostrato che l'uso intensivo di telecamere a circuito chiuso ha effettivamente influenzato il comportamento dei cittadini negli spazi pubblici», Parere numero 8 del 16 Settembre 2014 sui recenti sviluppi nel campo dell'Internet degli oggetti (WP 223), pag. 9.

[812] Confessore N., *Cambridge Analytica and Facebook: The Scandal and the Fallout So* Far, New York Times, 4 Aprile 2018. Disponibile online al seguente link: https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html

[813] «*First, the case emphasises the relevance of big data for contemporary politics, be-cause of the influential narrative that data and analytics were crucial to effective political campaigning and electoral success. The controversy around CAL circles substantially around the issue if and how the company was able to influence individuals' voting behaviour*», Richterich A., *How Data-Driven research fuelled the Cambridge Analytica controversy*, The Open Journal of Sociopolitical Studies, 2018.

della influenza socio-politica il monitoraggio è solo una fase preliminare, che precede le diverse operazioni attraverso cui si perpetra la influenza.

Inoltre, al fatto che i cittadini non siano in grado di autodeterminarsi correttamente consegue che questi non possano partecipare al meglio alla vita del paese[814]. Da ciò deriva un forte pregiudizio per le società fondate sul potere popolare[815].

Attraverso gli *smart device* è possibile rilevare diversi tipi di informazioni rilevanti relative agli orientamenti sociali o politici dell'individuo: *in primis*, rilevano i dati concernenti la posizione, si è già fatto riferimento alla possibilità di derivare il credo politico di un soggetto partendo dalla sua presenza ad un evento politico ed incrociandolo con altri dati. Lo stesso potrà dirsi per i dati derivanti dai *kindle*. In questi casi, soggetti terzi, per propri interessi, potranno decidere di avallare le posizioni assunte dall'interessato, o di provare ad influenzarle contrariamente. Dai dati rilevati attraverso gli *smart object*, gli interessati potranno divenire oggetto di *microtargeting*: verranno inviate all'interessato contenuti volti a farlo rimanere nella sua bolla[816], o a farlo riflettere diversamente.

5.2.3 La dimensione collettiva della privacy

Nel paragrafo 5.1 si è messo in evidenza come talvolta la profilazione non sia effettuata a livello individuale, ma si riferisca piuttosto a gruppi più o meno definiti. Questi, in virtù delle decisioni che possono essere prese a seguito della profilazione rischiano pesanti discriminazioni.

Da questa premessa emerge chiaramente come la privacy non possa più essere oggi intesa nella sua anacronistica dimensione individuale. Occorre piuttosto considerare la sfera di interessi colpiti a seguito di violazioni della privacy. È stato fatto notare come al momento non esistano diritti *ad hoc* per i gruppi, come invece accade per gli individui, in quanto

---

[814] «*Manipulation can affect not just individuals but also create societal harm, as people's decisions can affect not just themselves but society as well. The Cambridge Analytica incident involved the use of personal data on a mass scale to influence people's decisions in the 2016 U.S. presidential election and in the United Kingdom's vote for Brexit*», Citron K., Solove D. J., *Privacy harms*, Boston University Law Review, 2022, pag. 847.

[815] «*Surveillance can create chilling effects on free speech, free association, and other First Amendment rights essential for democracy. Even surveillance of legal activities can inhibit people from engaging in them. The value of protecting against chilling effects is not measured simply by focusing on the particular individuals who are deterred from exercising their rights. Chilling effects harm society because, among other things, they reduce the range of viewpoints expressed and the degree of freedom with which to engage in political activity*», Solove D., J., *"I've Got Nothing to Hide and Other Misunderstandings of Privacy*, San Diego Law Review, volume 44, 2007, pag. 765.

[816] Espressione riconducibile a Pariser A., *The Filter Bubble: What the Internet Is Hiding from You*, Penguin, 1 Marzo 2012.

oggetto di studio non è l'interessato ma il gruppo astrattamente considerato[817].

Nelle pratiche algoritmiche di profilazione dei gruppi, l'individuo rileva solo nella sua qualità di essere attribuito a questo o quel gruppo, e da ciò deriva che il gruppo sarà soltanto l'immagine riflessa di un agglomerato di individui[818]. Oggetto di studio sono i comportamenti di soggetti non individuati, classificabili in gruppi in virtù di determinati indicatori (età, genere, religione ecc.)[819].

La questione diviene particolarmente problematica quando i dati raccolti siano inesatti o mancano informazioni importanti; da ciò possono infatti nascere discriminazioni importanti, in quanto gli algoritmi mostrano inferenze ed interpretazioni impreviste in merito agli interessati[820]. Come detto, la profilazione è strumentale a determinate decisioni, che in un modo nell'altro, attivamente o passivamente, genereranno un'influenza nella sfera dell'interessato, motivo per cui vengono considerate un rischio per le libertà personali degli individui[821]. Si ricerca dunque una tutela funzionale al riconoscimento della dimensione collettiva della privacy, al momento non riconosciuta dal Regolamento[822]. Il tema verrà ripreso al paragrafo 5.3.3.

5.3 Il principio di *accountability* nell'*Internet of Things*

In questo paragrafo si descriverà il modo in cui il principio di *accountability* si adatta all'*IoT*. In particolare, si vedrà come alcuni obblighi che in contesti normali potrebbero essere adempiuti senza troppe

[817] Mantelero A., *Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data* protection, Computer Law & Security Review, volume 32, 2016, pag. 20.

[818] Mittelstadt B., *From Individual to Group Privacy in Big Data Analytics*, Philosophy & Technology, volume 30, 2017, pag. 479.

[819] Di Landro A. C., *Big Data. Rischi e tutele nel trattamento di dati personali*, 2020, pag. 189.

[820] Mittelstadt B., *From Individual to Group Privacy in Big Data Analytics*, 2017, pag. 480.

[821] Ibidem.

[822] « a tal proposito, il quadro normativo esistente ed anche il regolamento non paiono essere adeguati ad affrontare i potenziali rischi e le problematiche legate a questo cambiamento di paradigma nella ricerca sociale questo è dovuto al fatto che il diritto alla protezione dei dati strutturalmente concepito come diritto individuale.se è vero che la dimensione sociale dello stesso è stata considerata dalle corti ed è alla base della disciplina adottare in materia, e tuttavia al titolare del diritto che si guarda principalmente in termini di tutela disattivazione della stessa», Mantelero A., *Responsabilità e rischio nel Reg. UE 2016/679*, 2017, pag. 152.

perplessità, negli *smart environment* risultano ardui da soddisfare. Inoltre, si evidenzierà come la disciplina sulla privacy e la tecnologia si fondano per conferire un'adeguata tutela agli interessati[823].

5.3.1 Il soggetto *accountable*: il problema dei ruoli

Il principio di *accountability* impone al titolare del trattamento di valutare determinati fattori per modulare l'apposizione delle misure tecniche ed organizzative. Nel quarto capitolo (paragrafo 4.4.2) si è paragonato tale sistema a quello predisposto dall'articolo 1176 c.c. Analizzati il contesto e i principali rischi derivanti dai trattamenti nell'*Internet of Things*, si cercherà adesso di mettere in evidenziare come si comporta il principio di *accountability* in tale contesto.

Il GDPR, in virtù del suo approccio *risk-based*, impone al titolare del trattamento di valutare i rischi derivanti dal suo trattamento. Nei trattamenti tipici dell'*Internet of Things* va però considerata la compresenza di diversi soggetti, alcuni qualificabili come titolari del trattamento e capaci di arrecare danno allo stesso interessato. L'opacità che permea tali ambienti crea due ordini di problemi: la perdita del controllo sui dati per l'interessato e la difficoltà di rispettare il Regolamento per il titolare del trattamento.

Innanzitutto, va esaminata la questione della relativa difficoltà di qualificare correttamente il titolare ed il responsabile. Essa è stata considerata tempo addietro dal Gruppo di lavoro nel già citato parere sull'*IoT* e su quello relativo alle applicazioni per dispositivi intelligenti[824]. Nel primo si spiegava come questi trattamenti vedono l'intervento combinato di diversi portatori di interessi, e si menzionavano i produttori dei *device*, i fornitori di servizi *hosting* come i *social network*, gli sviluppatori ed altri soggetti terzi portatori di ulteriori interessi[825]. Più nello specifico, le figure dei vari attori sono molto diversificate: si distinguono il *device manufacturer* che produce il dispositivo; il *device provider* che lo vende; il *network provider* che fornisce all'apparecchio le risorse di rete; il *platform provider* conferisce invece capacità di *storage*, di elaborazione, di gestione ecc. all'*application*

---

[823] «*There are two levels of intervention to solve the problem: privacy law and incorporation of privacy values and principles in the digital architectures. We must avoid the false belief that they are alternative means. Some years ago we have thought that law could represent an adequate way of approaching to the problem*», Guarda P., *Data Protection, Information Privacy, and Security Measures: an essay on the European and the italian legal frameworks*, Ciberspazio e diritto, Dicembre 2008, pag. 3. Disponibile online al seguente link:

https://core.ac.uk/download/pdf/150082461.pdf

[824] Parere numero 2 del 2013 sulle applicazioni per dispositivi intelligenti (WP 202). Parere disponibile online al seguente link: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf

[825] Parere numero 8 del 16 Settembre 2014 sui recenti sviluppi nel campo dell'Internet degli oggetti (WP 223), pag. 12 e seguenti.

provider, il quale sviluppa e distribuisce le app agli utilizzatori finali, sfruttando le risorse fornite dal *network provider*, dal *platform provider* e dal *device provider*[826]; a questi si aggiungono figure terze quali gli «altri soggetti terzi portatori di interessi»[827]. Non è facile distinguere correttamente chi di questi sia il titolare del trattamento, cosa quanto mai rilevante in quanto da ciò deriva il riparto di responsabilità esaminato al paragrafo 4.1.

Si ponga un caso semplice[828]. La società Alpha è produttrice e venditrice di un certo tipo di *smartwatch* (dunque *device manufacturer* e *device provider*) e in questo sono installate le applicazioni della stessa società Alpha (che è dunque anche *application provider*); uno di questi *smartwatch* viene acquistato da Tizio (interessato), che tra le varie applicazioni a disposizione utilizza molto quelle relative al *fitness*, quindi contapassi, rilevazione del battito cardiaco ecc.; i dati generati vengono immagazzinati nel *cloud* di proprietà della società Beta attraverso la rete fornita dalla stessa (*network provider*); sempre Beta mette a disposizione anche il servizio di analisi dei dati servendosi di algoritmi di *machine learning* (dunque sia *network provider che platform provider*). In un modello siffatto si hanno due attori, Alfa e Beta, che trattano i dati dello stesso interessato. Il rapporto che lega questi soggetti prende spesso le forme del contratto di *outsourcing*[829]. Si ponga che in tale accordo Alfa abbia definito i mezzi e le finalità del trattamento che Beta deve eseguire. La finalità consiste nell'invio all'interessato di un grafico che indica l'andamento del battito cardiaco; il mezzo è invece l'algoritmo di *machine learning* messo a disposizione da Beta[830]. Da quanto stabilito nel contratto, dunque, Alfa sarà il titolare del trattamento (avendo definito modalità e finalità) e Beta il responsabile, con consequenziale riparto di responsabilità. Ci si chiede se tuttavia sia corretto affermare che Alfa abbia determinato i mezzi del trattamento e quindi che sia il titolare del trattamento; secondo l'Edpb infatti «determinare le finalità e i mezzi equivale a decidere, rispettivamente, il «perché» e il «come» del trattamento». Tuttavia, secondo chi scrive, indicare lo strumento di questo o quell'algoritmo di intelligenza artificiale non è sufficiente a stabilire il come vada protratto il trattamento. È stata ampliamente sottolineata l'opacità che caratterizza tali algoritmi, inaccessibili nelle loro viscere e scrutabili solo in

[826] Qui ci si riferisce ai soli ruoli commerciali, come delineati nella appendice informativa alla raccomandazione ITU-T Y.4000, pag. 10. Raccomandazione disponibile online al seguente link: https://www.itu.int/rec/T-REC-Y.2060-201206-I/en; per una diversa qualifica dei ruoli vedasi anche la raccomandazione Y.4100, disponibile online al seguente link: https://www.itu.int/rec/T-REC-Y.4100/en; sulla distinzione dei ruoli si veda anche Hadzovic S., Mrdovic S., Radonjic M., *Identification of IoT Actors*, Sensors, volume 21, 2021.

[827] Parere numero 8 del 16 Settembre 2014 sui recenti sviluppi nel campo dell'Internet degli oggetti (WP 223), pag. 14.

[828] Si è scelto di rappresentare il *business model* numero 3 indicato nella raccomandazione ITU-T Y.4000 appena citata, pag. 11 dell'appendice.

[829] Mantelero A., *Processi di outsourcing informatico e cloud computing: la gestione dei dati personali ed aziendali*, 2010.

[830] In questi casi si parla di *artificial intelligence as a service* (*AIaaS*).

parte; essi sono infatti tutelabili attraverso il segreto industriale[831]. Ciò non consente al titolare del trattamento di conoscere esattamente come verranno trattati i dati, ma solo attraverso quale strumento.

Si è detto come il titolare del trattamento possa affidarsi soltanto a responsabili in grado di fornire adeguate garanzie relative all'implementazione di adeguate misure tecniche ed organizzative, e che esso è responsabile di tale scelta (si è detto della c.d. *culpa in eligendo*, cfr. paragrafo 4.2). Secondo l'Edpb le garanzie che il titolare deve valutare (per la cui mancanza sarà responsabile) sono solo quelle che il responsabile è in grado di dimostrare[832]. Quest'ultimo è senz'altro in grado di dimostrare il contenuto del proprio algoritmo coperto dal segreto industriale (o il contenuto del complesso di cui fa parte l'algoritmo in caso di brevetto), tuttavia è pienamente in diritto di non disvelarlo per tutelare le proprie aspettative commerciali. In un contesto in cui l'intelligenza artificiale è destinata ad essere la protagonista dell'analisi dei dati, ci si chiede se si debba chiedere al titolare del trattamento di affidarsi unicamente a soggetti che o disvelano i propri segreti commerciali (alquanto improbabile) o che non utilizzano algoritmi. Quest'ultima ipotesi non appare in sintonia con il menzionato equilibrio tra protezione dei dati personali e circolazione derivato dall'articolo 1 paragrafo 3 GDPR. Va da sé che se si concede al titolare del trattamento la possibilità di rifarsi a soggetti che mantengono il segreto sugli algoritmi, allora non lo si potrà dichiarare responsabile in caso di danni derivanti da un errore non conoscibile del codice. Qualora ad esempio un interessato fosse danneggiato per via di un errore nel rilevamento del battito cardiaco derivante da un'errata progettazione dell'algoritmo, non si potrebbe ritenere responsabile ai sensi dell'articolo 82 GDPR il titolare del trattamento, il quale non aveva la possibilità di accedere all'algoritmo. Il massimo grado di diligenza imposto dai rischi derivanti dal trattamento nell'*Internet of Things*, non può ovviamente richiedere al titolare del trattamento di fare ciò che non può, ossia conoscere i difetti ingegneristici dell'algoritmo segreto. In casi del genere non è possibile ritenere che il principio di *accountability*, che richiede al titolare di scegliere un idoneo responsabile del trattamento (art. 28 GDPR), sia stato violato; non è dunque ravvisabile il requisito della colpa necessario per la condanna. Se

[831] Sul rapporto tra protezione dei dati personali e segreto industriale si dirà al paragrafo 5.3.3.

[832] «*The guarantees "provided" by the processor are actually those that the processor is able to demonstrate to the satisfaction of the controller, as those are the only ones that can effectively be taken into account by the controller when assessing compliance with its obligations. Often this will require an exchange of relevant documentation (e.g. privacy policy, terms of service, record of processing activities, records management policy, information security policy, reports of external audits, recognised international certifications, like ISO 27000 series*)», linee guida 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR. Disponibili online al seguente link: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2020/guidelines-072020-concepts-controller-and_en

si condannasse il titolare del trattamento anche in questi casi, si dovrebbe allora parlare di responsabilità oggettiva. Per gli stessi motivi non potrebbe configurarsi la *culpa in vigilando*.

Appare dunque non scontato affermare che sia Alfa, il produttore dello *smartwatch*, a determinare i mezzi del trattamento. Questi sono infatti conoscibili nella loro interezza solo dal fornitore del *cloud*, Beta. A tal proposito non è mancato chi, nel dare lustro alla grande autonomia delle macchine, abbia ritenuto possibile classificare esse stesse come titolari del trattamento[833], o come responsabili del trattamento[834]. Ci si chiede tuttavia se, allorquando una società offra l'intelligenza artificiale come servizio, possa essere considerata contitolare del trattamento anziché responsabile.

---

[833] Alpa G. (a cura di), *Diritto e intelligenza artificiale*, Pacini giuridica, Pisa, 2020, pag. 283. Si sottolinea che chi scrive non aderisce a tale impostazione. Preziosi contributi sulla confutazione della tesi della riconoscibilità in capo al sistema di IA della qualifica di titolare del trattamento in Contaldi G., *Intelligenza artificiale e dati personali*, Ordine internazionale e diritti umani, 2021, pag. 1204: «questa tesi non sembra tuttavia reggere al riscontro degli elementi normativi. Innanzitutto essa si pone in contrasto con le risultanze dei lavori preparatori riportati nel primo paragrafo, dai quali emerge chiaramente la volontà delle istituzioni europee di escludere, nello stato di attuale elaborazione della maniera, qualunque forma di soggettività giuridica all'intelligenza artificiale. Vari elementi testuali del regolamento sulla protezione dei dati, poi, consentono di escludere la possibilità di assimilare il sistema di intelligenza artificiale al titolare del trattamento ai fini dell'applicazione del regolamento sulla protezione dei dati personali. Depone in tal senso, innanzitutto l'art. 4, par. 1, n.7, del GDPR, nel definire il titolare del trattamento, riferisce espressamente che è la «persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento». La disposizione, se da un lato include chiaramente nel novero dei titolari anche enti privi di una soggettività giuridica («il servizio o altro organismo»), sembra comunque richiedere un minimo di personificazione per assumere la veste di titolare del trattamento. In secondo luogo, milita nel senso di escludere la possibilità di identificare il titolare del trattamento con il sistema di intelligenza artificiale, l'art. 22 GDPR, che prevede che l'interessato può chiedere di non essere sottoposto esclusivamente ad una decisione automatizzata. Se il soggetto passivo, che viene influenzato da un determinato trattamento, può sempre chiedere di non essere assoggettato ad una decisione automatizzata, significa che il sistema di intelligenza artificiale deve essere concepito in modo da consentire, sempre e comunque, un intervento umano; ovvero l'intervento di un soggetto, con piena capacità giuridica, dotato del potere di escludere la macchina e di assumere le relative decisioni in sua vece. A ciò si aggiunga che le disposizioni del regolamento sulla protezione dei dati, allorché prevedono il potere delle autorità nazionali competenti di imporre talune sanzioni, riconnettono l'eventuale diversa graduazione della pena pecuniaria anche al carattere di volontarietà del comportamento dell'autore dell'illecito43. Le "decisioni" di un sistema di intelligenza artificiale, infatti, sono sempre il frutto di calcoli; esse non discendono mai da scelte discrezionali, indicative, come tali, di un certo atteggiamento psicologico. Deve quindi recisamente negarsi che, nell'attuale panorama giuridico, si possa concepire un sistema di intelligenza artificiale completamente automatizzato, tale da operare al di fuori di qualunque intervento umano».

[834] «Collocandosi in questa prospettiva e considerando che comunque il robot è dotato di una propria autonoma capacità di decidere, almeno in parte, su come raggiungere le finalità connesse ai trattamenti, ci si può chiedere se esso potrebbe almeno essere nominato dal produttore come responsabile sensi dell'art. 28 del GDPR», Pizzetti F., *Intelligenza artificiale, protezione dei dati personali e regolazione*, 2018, pag. 173.

Come si è detto poc'anzi, mentre Alfa decide sicuramente le finalità del trattamento, altrettanto non può dirsi per i mezzi, che quando coincidono con algoritmi coperti da segreto industriale rimangono in parte sconosciuti; gli unici a conoscere a fondo tali strumenti di trattamento sono le società che li producono e li immettono nel mercato (e in certi casi neppure loro). Alla possibilità di classificare i fornitori dei servizi di IA come contitolari osta però il fatto che la società che offre il servizio (nell'esempio Beta) non decide le finalità del trattamento, requisito della qualifica di titolare o contitolare del trattamento ai sensi dell'articolo 4 e dell'articolo 26 del Regolamento[835]. Vi sono dunque dei motivi per affermare che il titolare del trattamento sia Alfa, così come Beta; eppure, tali motivi possono essere contestati alla luce dell'opacità dei sistemi in cui *IoT* e IA si incontrano. Secondo chi scrive questo è uno dei casi in cui si rende difficile una lineare operatività del principio di *accountability*, nella sua particolare declinazione della scelta di un responsabile del trattamento adeguato. Conseguenze vi sono anche dal punto di vista della responsabilità: secondo l'impostazione predetta, la società Alfa, titolare del trattamento, non incorrerebbe in colpa e quindi non sarebbe condannabile. Altrettanto potrebbe dirsi di Beta, che nella sua veste di responsabile del trattamento non incorrerebbe nei suoi profili tipici di responsabilità. La causa dell'evento dannoso è riconducibile a Beta, eppure questa, nella sua specificità di responsabile del trattamento risponde solo o qualora non abbia dato seguito alle legittime istruzioni del titolare, o nel caso in cui sia venuta meno ai suoi obblighi specifici[836]. L'interessato danneggiato

[835] «Il titolare del trattamento deve decidere in merito alla finalità e ai mezzi del trattamento come descritto di seguito. Di conseguenza, il titolare del trattamento non può limitarsi alla sola determinazione della finalità: deve anche prendere decisioni in merito ai mezzi del trattamento» linee guida 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR, pag. 3.

[836] Chi scrive ritiene di non poter ricondurre l'errore nella progettazione dell'algoritmo nei doveri tipici del responsabile del trattamento. Ai sensi dell'articolo 28 paragrafo 3 GDPR si richiede che il responsabile «a) tratti i dati personali soltanto su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento; in tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico; b) garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza; c) adotti tutte le misure richieste ai sensi dell'articolo 32; d) rispetti le condizioni di cui ai paragrafi 2 e 4 per ricorrere a un altro responsabile del trattamento; e) tenendo conto della natura del trattamento, assista il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III; f) assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento; g) su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati; e h) metta a disposizione

non riceverebbe dunque alcuna tutela per il trattamento illecito dei suoi dati personali; potrebbe invece essere risarcito in altre forme[837].

La difficoltà dell'individuazione degli attori aumenta in casi particolarmente complessi, come quelli riconducibili ad esempio alle *smart car*, mentre, nell'esempio della banca descritto al paragrafo 4.6, non vi erano dubbi circa la qualifica di titolare e responsabile del trattamento. Il problema della qualificazione dei ruoli non è di poco conto. Nello specifico parere sull'*IoT*, il Gruppo di lavoro in diverse occasioni suggeriva la responsabilizzazione di tutti i soggetti coinvolti nel trattamento: ad esempio si richiedeva che tutti i soggetti coinvolti garantissero che i dati non fossero utilizzati per scopi non compatibili con quelli per cui si era prestato il consenso; o che tutti loro applicassero i principi di *privacy by design*. Tuttavia, non tutti sono tenuti al rispetto dei singoli doveri di *accountability*: i programmatori, ad esempio, sono classificabili solo come soggetti autorizzati ai sensi dell'articolo 28 paragrafo 3 GDPR, e ai sensi dell'articolo 29 devono attenersi alle direttive del titolare del trattamento, motivo per cui non saranno soggetti agli stringenti obblighi del GDPR, pur essendo gli unici a poter lavorare a fondo sugli algoritmi.

5.3.2. *L'Internet of Things* e i principi generali del trattamento

Al paragrafo 5.1.1 si è discusso dell'evanescenza del concetto di dato personale nell'ambito dell'*Internet of Things*. La capacità computazionali odierne rendono particolarmente difficile predire fin dove si spingeranno le *analytics* nella generazione di nuove inferenze e quindi di nuovi dati personali. Quanto appena detto crea non pochi problemi: l'interessato rischia di perdere il controllo dei suoi dati personali (e dunque della rappresentazione digitale della sua identità[838]) e il titolare del trattamento incontra difficoltà nel rispetto del principio di *accountability*. Questo, *in primis*, richiede il rispetto dei principi previsti dall'articolo 5 GDPR: liceità,

---

del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato. Con riguardo alla lettera h) del primo comma, il responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, un'istruzione violi il presente regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati».

[837] Per i rimedi civili in ambito di intelligenza artificiale vedasi Ruffolo U. (a cura di), *Intelligenza artificiale*, Giuffrè Francis Lefebvre, Milano, 2020, pag. 114; Alpa G. (a cura di), *Diritto e intelligenza artificiale*, 2020, pag. 435 e ss.

[838] «Le tecniche di raccolta dei dati e profilazione individuale, rese possibili dalle nuove tecnologie, determinano il rischio che l'io venga frammentato, a sua insaputa, in una molteplicità di banche dati, offrendo così una raffigurazione parziale e potenzialmente pregiudizievole della persona, la quale verrebbe così ridotta alla mera sommatoria delle sue proiezioni elettroniche», Resta G., *Identità personale e identità* digitale, Il diritto dell'informazione e dell'informatica, fascicolo 3, 2007, pag. 522.

correttezza, trasparenza; limitazione delle finalità; minimizzazione; limitazione della conservazione; di integrità e sicurezza. Ognuno di questi principi viene messo seriamente a rischio dalle nuove tecnologie. Di seguito si esporranno le principali problematiche in relazione a tali principi, e di contro, le misure che il titolare del trattamento deve apprestare per essere *accountable*.

Innanzitutto, l'articolo 5 GDPR prevede il requisito della liceità, senza però in alcun modo darne una definizione. La disposizione seguente tuttavia chiarisce la questione, essendo rubricata «liceità del trattamento». Malgrado quanto appena detto, gli *smart object* possono essere definiti apparecchi terminali ai sensi della direttiva 58/2002. Questa stabilisce apposite norme relativi agli apparecchi personali degli interessati (utenti o abbonati nella terminologia della direttiva) ed essendo *lex specialis* andrà applicata al posto del Regolamento[839]. Quest'ultimo, tuttavia, conserva il suo ambito applicativo in quegli spazi in cui avvengono i trattamenti dei dati: nei paragrafi 1.4.2 e 1.4.4 si è fatto riferimenti ai *luoghi* del *cloud* e del *fog computing*. Qualora dunque il trattamento non avvenisse nell'apparecchio terminale si applicheranno gli articoli 6 e 9 del Regolamento.

La direttiva 58/2002, al contrario del GDPR, non fornisce dettagliate specifiche sul consenso, limitandosi a statuire che l'interessato debba essere informato in modo chiaro e completo sugli scopi del trattamento prima che avvenga l'archiviazione delle informazioni (articolo 5). Tale dovere informativo verserà in capo a chiunque voglia accedere ai dati contenuti nel *device*[840].

Per quanto concerne i casi di applicazione del Regolamento, affinché il trattamento sia lecito, occorre che siano rispettate le prescrizioni previste dall'articolo 6 del Regolamento, rubricato per l'appunto liceità del trattamento». Ai sensi di detta disposizione, il trattamento sarà lecito solo qualora vi sia il consenso dell'interessato in relazione a specifiche finalità; qualora il trattamento sia necessario per l'esecuzione di un contratto; o sia necessario per l'adempimento di un obbligo legale; sia necessario per la salvaguardia di un interesse vitale; sia necessario per l'esecuzione di un compito di pubblico interesse; o sia necessario per il perseguimento di un legittimo interesse.

Sebbene nell'*IoT* assuma una certa rilevanza la liceità per necessaria conclusione del contratto, i prerequisiti del trattamento lecito che nell'ambito dell'*IoT* prestano le maggiori perplessità sono indubbiamente il consenso dell'interessato e il legittimo interesse del titolare del trattamento[841].

---

[839] In tal senso Giovanella F., *Le persone e le cose: la tutela dei dati personali nell'ambito dell'Internet of Things,* in Cuffaro V., D'Orazio R., Ricciuto V., *I dati personali nel diritto europeo,* 2019, pag. 1240, relativamente al futuro regolamento ePrivacy.

[840] Ibidem, pag. 1228.

[841] Ibidem, pag. 1226.

Trattando in primo luogo del consenso, può farsi riferimento ai pareri del Gruppo di lavoro relativi all'*Internet of Things* e alle applicazioni per dispositivi mobili. Nel primo documento si evidenziava il fatto che molti *smart object*, come lo *smartwatch*, pur essendo dotati dei più disparati sensori, non vengono percepiti dalla collettività come strumenti in grado di invadere la loro privacy, e ciò rende difficile per gli individui anche solo individuare l'esistenza del trattamento. Per ovviare a tale problema, il Gruppo di lavoro propone di utilizzare una segnaletica che sia visibile e che indichi all'interessato l'esistenza del trattamento[842], in ottemperanza al considerando numero 60[843]. Ad esempio, per i moderni *smart glasses*, si è scelto di attivare una luce a led bianca ininterrotta: studi hanno infatti segnalato come tale tipo di illuminazione sia quella che maggiormente cattura l'attenzione di chi ci si imbatte. In questo modo, gli individui che si trovano nel raggio d'azione degli occhiali intelligenti indossati dal portatore potranno venire a conoscenza del trattamento in atto[844].

Per quanto riguarda il consenso, il Gruppo di lavoro stabilisce che per essere libero non deve essere soggetto a ritorsioni quali penalizzazioni economiche o accesso limitato ai servizi delle capacità dei propri dispositivi[845]. Nelo stesso senso si è mosso l'Edpb, nel parere sulla proposta relativa al prossimo regolamento ePrivacy[846]

Sempre in merito al consenso, si richiede un tipo di consenso granulare, che riguardi dunque ogni accesso alle diverse applicazioni[847].

Proseguendo, può risultare difficile scorgere lo spazio per ammettere un trattamento sulla base del legittimo interesse in questi contesti: il legittimo interesse nasce per tutelare esigenze di natura economica del

---

[842] «La maggior parte degli osservatori non può distinguere un orologio normale da uno connesso e quest'ultimo può essere provvisto di telecamere, microfoni e sensori di movimento che possono registrare e trasferire dati senza che le persone ne siano al corrente e quindi senza che acconsentano a tale trattamento», parere numero 8 del 16 Settembre 2014 sui recenti sviluppi nel campo dell'Internet degli oggetti, 2014 pag. 8.

[843] Considerando numero 60: «i principi di trattamento corretto e trasparente implicano che l'interessato sia informato dell'esistenza del trattamento e delle sue finalità…».

[844] Intervista a Guido Scorza, componente del Garante italiano, nella videointervista di Flora M., *Rayban Stories: parliamo dei nuovi occhiali di Facebook*, minuto 10:25. Disponibile online al seguente link:

https://www.youtube.com/watch?v=HEzA9CPcpns&t=89s

[845] Parere numero 8 del 16 Settembre 2014 sui recenti sviluppi nel campo dell'Internet degli oggetti, 2014 pag. 26.

[846] «*The GDPR improves upon Directive 95/46/EC by not only requiring that consent be freely given but also providing further guidance as to what this means in practice. In particular, it provides that consent is not considered to be freely given in situations where the provision of a service is made dependent on an individual giving her consent to the processing of her personal data despite the fact that such processing is not necessary for the performance of that service*», parere numero 6 del 2017sulla proposta di regolamento sulla privacy e le comunicazioni elettroniche (regolamento e-privacy), pag. 17.

[847] Parere numero 8 del 16 Settembre 2014 sui recenti sviluppi nel campo dell'Internet degli oggetti, 2014 pag. 24.

trattamento, ma visti i seri rischi realizzabili nell'Internet delle cose, appare dunque difficilmente ammissibile la sua applicabilità. Sembra invece esserci la possibilità di ammettere il trattamento volto a finalità maggiormente rilevanti, quali la tutela della salute pubblica[848].

Volgendo lo sguardo al futuro, va segnalato come la proposta sul futuro regolamento ePrivacy, all'articolo 7, abbia escluso il consenso tra le basi necessarie per il trattamento dei dati[849]

Per quanto riguarda il principio di minimizzazione, il contrasto tra tale principio e l'obiettivo degli *smart objects* di ricavare sempre maggiori informazioni è ormai acclarato[850]. I dati raccolti devono essere minimi. Tale soglia è parametrata rispetto alle finalità del trattamento: affinchè sia rispettato tale principio possono essere trattati solo i dati strettamente necessari al conseguimento delle finalità previste. Il titolare del trattamento non deve trattare alcun dato che non sia strettamente necessario rispetto agli scopi. In tale direzione, il Gruppo di lavoro, nel parere dedicato all'*IoT*, tra le varie raccomandazioni fornite, suggeriva ai vari attori del trattamento di eliminare i dati grezzi ottenuti dagli *smart object* non appena estratti i dati aggregati rilevanti ai loro fini[851].

Come pratica utile a rispettare tale principio è stato proposto anche di tenere separate le informazioni derivanti dalle diverse fonti di dati: ad esempio, non andrebbero conservate degli stessi archivi le informazioni derivanti da sensori come quelli di Fitbit e quelle fornite dagli ospedali sulla salute dell'interessato, poiché, se combinate, sarebbero suscettibili di condurre ad informazioni molto sensibili[852].

Si è anche evidenziato come tali principi si pongano come un freno ai sistemi di intelligenza artificiale. Questi, infatti, fanno della ricerca di nuove inferenze tra i dati, e quindi della generazione di nuove informazioni, il proprio obiettivo, e un trattamento ancorato su finalità prestabilite rischierebbe di troncarne lo sviluppo[853].

---

[848] Giovanella F., *Le persone e le cose: la tutela dei dati personali nell'ambito dell'Internet of Things,* 2019, pag. 1227.

[849] Articolo 7: «i fornitori di reti e servizi di comunicazione elettronica possono trattare i dati delle comunicazioni elettroniche se: (a) necessario per realizzare la trasmissione della comunicazione, per la durata necessaria a tal fine, oppure (b) se necessario per mantenere o ripristinare la sicurezza delle reti e dei servizi di comunicazione elettronica o rilevare problemi e/o errori tecnici nella trasmissione di comunicazioni elettroniche, per la durata necessaria a tal fine».

[850] Giovanella F., *Le persone e le cose: la tutela dei dati personali nell'ambito dell'Internet of Things,* 2019, pag. 1222.

[851] Parere numero 8 del 16 Settembre 2014 sui recenti sviluppi nel campo dell'Internet degli oggetti, 2014, pag. 24.

L'eliminazione dei dati grezzi si ritiene necessaria in quanto questi dati vengono spesso riutilizzati a fini diversi da quelli della raccolta.

[852] Perera C., McCormick C., Bandara A. K., Price B., A., Nuseibeh B., *Privacy-by-Design Framework for Assessing Internet of Things Applications and Platforms*, The 6th International Conference on the Internet of Things, Stoccarda, Novembre 2016, pag. 85.

[853] Contaldi G., *Intelligenza artificiale e dati personali*, 2021, pag. 1206.

Nei trattamenti protratti in seno all'Internet delle cose risulta particolarmente complesso applicare tale principio in virtù della presenza di diverse fasi del trattamento. In particolare, in ogni fase e nel passaggio da una fase all'altra, deve essere sempre garantito che solamente il minimo ammontare di dati necessario al perseguimento delle finalità sia raccolto. A tal fine è opportuno orientarsi rispetto all'obiettivo dell'ultima fase del trattamento, che chiarirà il fine ultimo dell'intera catena del trattamento[854].

Il principio di minimizzazione dei dati è intrinsecamente correlato al *risk-based approach* del regolamento, in quanto dalla raccolta di una grande quantità di dati, non coerente rispetto alle finalità, potrebbe aversi un aumento non giustificato dei rischi realizzabili nei confronti dell'interessato[855]. Di tale principio si discuterà ancora al paragrafo 5.3.5.

Per quanto concerne il principio di esattezza (e aggiornamento), l'articolo 5 GDPR stabilisce che i dati personali sono «esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati». Dal disposto della norma emerge come l'esattezza vada parametrata rispetto alle finalità del trattamento; da ciò, un dato rappresentante il vero, ma non rispondente alle finalità per cui si sono raccolti i dati sarà inesatto. Ciò crea perplessità in merito alle analisi protratte con l'ausilio di sistemi di *machine learning* e intelligenza artificiale, le quali vengono utilizzate per ricavare quante più informazioni possibili, come se si trattasse di una «pesca a strascico»[856].

Affinché un dato sia esatto è necessario che non sia effetto da *bias*. Un dato potrà essere esatto in un determinato momento, ed inesatto in un altro. In virtù della combinazione tra dati che connota le *big data analytics* la combinazione di un dato esatto ad uno discriminante potrebbe portare a macchiare di pregiudizio anche il primo dato. Occorre dunque un costante monitoraggio della qualità dei dati, sì da verificare la loro rispondenza al reale e ai fini per i quali sono stati raccolti. Dalla inesattezza dei dati, come già visto, possono derivare seri rischi sia per gli individui che per le comunità[857], dunque il rispetto di tale principio assume una valenza particolare rispetto alla prevenzione dei rischi richiesta dall'*accountability*.

Sebbene le odierne tecnologie d'analisi siano molto precise nel predire comportamenti e altre informazioni personali, non di rado si assiste ad errori causati dagli algoritmi, soprattutto quelli di *machine learning*.

Anche il principio della limitazione della conservazione risulta particolarmente difficile da rispettare. Esso richiede che i dati personali vengano cancellati non appena più necessari al compimento delle finalità del trattamento; tuttavia, l'anonimizzazione viene equiparata alla cancellazione.

---

[854] Pizzetti F., *Intelligenza artificiale, protezione dei dati personali e regolazione*, 2018, 121.

[855] Ibidem, pag. 62.

[856] Ibidem, pag. 61.

[857] Ibidem, pag. 62.

L'anonimizzazione viene dunque utilizzata come strumento per continuare a lavorare sui dati, che, come detto, seppur anonimi e dunque meno preziosi, possono comunque essere molto utili. Mantenere dati dei *databases*, seppur anonimi, può portare, nel tempo, a inferenze sempre più profonde, tali da condurre all'identificabilità dell'interessato. Già il Gruppo di lavoro affermava che tali dati non possono essere conservati «in caso ve ne fosse bisogno». Le applicazioni installabili negli *smart objects* giovano di un grande quantitativo di dati presenti negli archivi storici, senza i quali non potrebbero funzionare a pieno[858].

Il modello di circolazione dei dati cui si assiste è volto proprio a questo, identificare, conoscere, e vendere. La dottrina del capitalismo della sorveglianza ha mostrato l'interesse dei grandi *players* sia nell'identificabilità del singolo, sia in quella di gruppi astratti. Nei confronti di questi ultimi, mancando un vero e proprio diritto alla protezione dei loro dati (paragrafo 5.3.3), potrebbe non porsi il problema della conservazione. Tuttavia, tali profili collettivi servono poi a trarre delle conclusioni, che si tramutano in decisioni (sui procedimenti decisionali automatizzati cfr. paragrafo 5.3.4) e in questi casi, come si vedrà, potrebbe richiedersi una certa tutela.

Anche il principio di finalità rischia di divenire inefficace senza un'attenta definizione degli scopi del trattamento. Spesso, infatti, da dati che possono sembrare in un primo momento di poco conto, può giungersi a nuovi dati, totalmente incoerenti rispetto alle finalità per cui si aveva raccolto i dati originali (si parla in questi casi di uso secondario dei dati)[859]. Anche qui, si constata come sia difficile improntare un sistema (*IoT*) volto ad ampliare le conoscenze in merito agli individui, nei limiti di quanto può ragionevolmente prevedersi nella fase iniziale del trattamento. Le *predictive analytics* sono l'ingrediente più importante per chi voglia generare profili comportamentali volti al *microtargeting*. Nel rispettare tale principio, il titolare del trattamento che voglia essere *accountable*, rischia di tagliare fuori una grossa parte delle risorse utili al suo mercato.

Grazie alle capacità di analisi dei moderni strumenti, anche partendo da dati personali comuni, può giungersi ad inferire dati particolari, dunque idonei a rivelare convinzioni religiose, filosofiche, appartenenza sindacale ecc. L'articolo 9 del Regolamento impone un divieto di trattamento dei dati particolari, salvo:

---

[858] Giovanella F., *Le persone e le cose: la tutela dei dati personali nell'ambito dell'Internet of Things,* 2019, pag. 1223.

[859] «Dati apparentemente insignificanti raccolti originariamente attraverso un dispositivo (ad esempio l'accelerometro e il giroscopio di uno smartphone) possono quindi essere utilizzati per ottenere altre informazioni con un significato completamente diverso (ad esempio le abitudini di guida della persona). Questa possibilità di ottenere dati da tali informazioni "grezze" deve essere presa in considerazione insieme ai classici rischi analizzati in relazione alla fusione dei sensori, fenomeno ben conosciuto in ambito informatico», parere numero 8 del 16 Settembre 2014 sui recenti sviluppi nel campo dell'Internet degli oggetti, 2014 pag. 9.

«a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1; b) il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato; c) il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso; d) il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato; e) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato; f) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali; g) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato; (C55, C56) h) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al paragrafo 3; (C53) i) il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale; (C54) j) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato».

Il problema che in relazione a tali dati può riscontrarsi nell'Internet delle cose è evidente: ben si potrebbe trattare lecitamente dati non particolari sulla base (ad esempio) della necessarietà per la conclusione di un contratto (articolo 6 paragrafo 1, lettera b)), e attraverso questi, mediante applicazione di tecniche analitiche, ricavare dati particolari per i quali non era stato originariamente chiesto il consenso esplicito o non era presente altra condizione di liceità de trattamento[860]. A nulla servirebbe

[860] Giovanella F., *Le persone e le cose: la tutela dei dati personali nell'ambito dell'Internet of Things,* 2019, pag. 1230.

inviare un'informativa ai sensi dell'articolo 14 GDPR. Le informazioni disvelate non possono più tornare segrete. Il Gruppo di lavoro esemplifica la questione del seguente caso:

> «L'impresa X ha sviluppato un'applicazione che è in grado di rilevare modelli d'uso di droghe, analizzando i dati grezzi dai segnali di un elettrocardiogramma generati da sensori commerciali comunemente a disposizione dei consumatori. Il motore dell'applicazione può estrarre informazioni specifiche dai dati grezzi dall'elettrocardiogramma che, in base agli esiti precedenti, sono collegati al consumo di droghe»[861].

In base a quanto appena detto il Gruppo di lavoro conclude stabilendo che in questi casi, vista la possibilità di estrarre dati particolari, andrà richiesto il consenso esplicito dell'interessato ai sensi dell'articolo 9 GDPR (o altra base del trattamento)[862].

Sull'applicazione di tali principi all'*IoT* va constatata l'antiteticità degli stessi rispetto alle prassi commerciali sottostanti la circolazione dei dati. Il carburante di tali sistemi è difatti rappresentato dai *Big Data*, difficilmente ricavabili mediante un'applicazione soddisfacente di tali principi. Il Regolamento, all'articolo 1 paragrafo 3, stabilisce che la circolazione dei dati non può essere inficiata per ragioni inerenti alla protezione dei dati personali; tuttavia, la mancata attuazione di tali principi genera una divulgazione di dati personali, anche sensibili, totalmente indiscriminata e non compatibile con l'ulteriore fine del Regolamento, ossia la protezione dei dati e delle libertà fondamentali. Il rispetto dell'articolo 5 GDPR, dunque, può concretizzarsi in importanti diminuzioni dei ricavi per i grandi *players*, ma ciò non può assolutamente costituire un espediente per ritenere che tali principi possano non essere rispettati fino in fondo.

Un altro problema che accomuna l'applicazione di tutti questi principi riguarda la moltitudine di ruoli rinvenibili nella catena del trattamento. Sebbene il considerando numero 78 stabilisca che «i produttori dei prodotti, dei servizi e delle applicazioni dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati allorché sviluppo nel progetto hanno tali prodotti, servizi e applicazioni», ciò non sarà per questi comunque vincolante[863]. Un modello di circolazione dei dati basato in buona misura su *software* non proprietari soffrirà dunque tale mancanza di responsabilizzazione. Gli sviluppatori potranno infatti essere al massimo qualificati come soggetti autorizzati al trattamento ai sensi dell'articolo 28 paragrafo 3 del Regolamento, e in virtù dell'articolo 29 GDPR rimarranno sotto la responsabilità del titolare del trattamento. Da ciò, deriva che questi

---

[861] Parere numero 8 del 16 Settembre 2014 sui recenti sviluppi nel campo dell'Internet degli oggetti, 2014 pag. 19.

[862] Ibidem.

[863] Giovanella F., *Le persone e le cose: la tutela dei dati personali nell'ambito dell'Internet of Things,* 2019, pag. 1238.

soggetti non sono vincolati al rispetto del principio di *accountability*, e al di là delle questioni attinenti al riparto delle responsabilità, ciò risulta particolarmente non costruttivo dal punto di vista della realizzazione di uno *smart object* in grado di soddisfare la protezione dei dati personali e delle libertà fondamentali. Tale questione si ricollega inesorabilmente al principio di *privacy by design*, di cui si dirà di seguito.

Per la trattazione del principio di trasparenza si è preferito dedicare un autonomo paragrafo (5.3.4).

5.3.3 L'*accountability* e il principio di trasparenza nell'*IoT*

Uno dei principi più problematici all'interno dell'*IoT* è quello di trasparenza, previsto principalmente all'articolo 5 paragrafo 1 GDPR: «i dati personali sono: a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»)». Come evidenziato, il modello circolatorio dei dati è parecchio complesso, e ciò, oltre ad essere un problema per l'interessato i cui dati vengono smarriti e sfruttati, costituisce un elemento problematico anche per il titolare del trattamento che voglia essere *accountable*.

La trasparenza costituisce all'interno del Regolamento la base su cui poggia l'effettivo esercizio dei diritti previsti dagli articoli 12 e seguenti[864]; una mancanza di trasparenza potrebbe dunque minare il controllo che l'interessato, attraverso quei diritti, può avere sui suoi dati.

Il principio in esame trova le sue norme di dettaglio principali negli articoli 13, 14 e 15 del Regolamento: la prima disposizione impone l'obbligo di informativa al momento della raccolta dei dati presso gli interessati; la seconda prevede invece un simile dovere informativo in capo ai terzi che abbiano raccolto i dati non direttamente dall'interessato; l'articolo 15 invece prevede il diritto di accesso ai dati durante qualsiasi momento del trattamento.

Applicare tali disposizioni agli oggetti *sensor-based* è fondamentale. Il già richiamato parere del Gruppo di lavoro sull'*IoT* faceva luce su alcuni problemi inerenti non solo la trasparenza del trattamento ma addirittura la sua conoscibilità. Gli oggetti indossabili soprattutto, hanno le sembianze dei più comuni oggetti tradizionali, orologi, occhiali da sole ecc. Tuttavia, questi sono sempre in grado di creare connessioni e di trasferire i dati personali dell'interessato. A proposito di ciò il Gruppo di lavoro suggeriva

[864] «*Thus, there is a clear relationship between the other individual rights the GDPR establishes—contestation, correction, and erasure—and the kind of individualized transparency it requires. This suggests something interesting about transparency: the substance of other underlying legal rights often determines transparency's substance.137 If one has a right of correction, one needs to see errors*», Kaminski M. E., *The right to explanation, explained*, Berkeley Technology Law Journal, volume 34, numero 1, 2019, pag. 213.

l'opportunità di apprestare una segnaletica adeguata effettivamente visibile agli interessati[865]. Si riportava l'esempio dell'indirizzo MAC[866]: questo viene reso disponibile da diversi *smart object* allo scopo di instaurare connessioni di utilità per l'interessato (ad esempio al *wi-fi*). Si pensi agli oggetti intelligenti indossabili, la raccolta di tali indirizzi MAC agevola la creazione di *fingerprint* e altri identificativi suscettibili di essere attribuiti a specifiche persone fisiche[867], e di essere utilizzati per diversi scopi, quali la *location analytic*[868]. In merito a tale tipo di raccolta dei dati si dirà meglio quando si affronterà il tema della *privacy by default* (paragrafo 5.3.5).

Nel momento in cui l'interessato è edotto in merito all'esistenza del trattamento, intervengono tutte le ulteriori informazioni descritte dagli articoli 13, 14 e 15 del Regolamento. Oltre al contenuto informativo di tali disposizioni, rilevano anche le modalità di consegna, ad esempio il Gruppo di lavoro scrive come queste andrebbero fornite direttamente all'oggetto stesso[869], ed ai sensi del considerando numero 39 devono essere facilmente accessibili comprensibili, e riportante con un linguaggio chiaro e semplice.

L'informativa, nei contesti riconducibili all'Internet delle cose, non è però cosa semplice. Innanzitutto, si segnala come in certi casi essa venga fornita solamente sul sito web dell'applicazione o del dispositivo, e non anche sul dispositivo stesso, e questo perché magari il *device* non è neppure fornito di un monitor che possa trasmettere l'informativa[870]. Anche qualora l'informativa fosse resa nelle forme più corrette, rimane da chiarire come il titolare del trattamento possa spiegare in modo semplice e chiaro questioni particolarmente complesse come la catena del trattamento, le modalità di trattamento in caso di trattamenti automatizzati, i rischi prevedibili, le inferenze possibili ecc. Offrire un'adeguata informazione in merito alle indicazioni incluse negli articoli 13 e 14 richiede un certo grado di tecnicismo, da contemperare con le esigenze di chiarezza necessarie per rendere effettiva e non lettera morta l'informativa. Oltretutto, il Garante si è raccomandato di non redigere informative troppo lunghe, suscettibili di distogliere l'interessato dalla volontà di leggerle[871].

---

[865] Parere numero 8 del 16 Settembre 2014 sui recenti sviluppi nel campo dell'Internet degli oggetti, 2014 pag. 8.

[866] La cui classificazione come dato personale è stata discussa al paragrafo 2.5.

[867] Parere numero 8 del 16 Settembre 2014 sui recenti sviluppi nel campo dell'Internet degli oggetti, 2014 pag. 10.

[868] Per essa si intende l'analisi utile alla determinazione delle correlazioni tra l'individuo e i singoli luoghi in cui si trova.

[869] Parere numero 8 del 16 Settembre 2014 sui recenti sviluppi nel campo dell'Internet degli oggetti, 2014 pag. 20.

[870] Giovanella F., *Le persone e le cose: la tutela dei dati personali nell'ambito dell'Internet of Things,* 2019, pag. 1229.

[871] In merito alla possibilità di inserire una dashboard dalla quale controllare i dati si scrive che «può essere un modo efficace di dimostrare che le "informazioni sulla privacy" costituiscono un elemento necessario e parte integrante di un servizio anziché un lungo elenco di termini legalistici», Linee guida sulla trasparenza ai sensi del regolamento

Ancora, il Gruppo di lavoro, nelle linee guida sulla trasparenza, consiglia di fornire una dichiarazione separata nei casi più complessi, da accompagnare rispetto all'informativa; in questo separato documento il titolare del trattamento dovrà chiarire senza ambiguità le conseguenze del trattamento[872]. Sebbene si cerchi in questo modo di offrire un'informazione migliore, si rischia di gravare l'interessato del trattamento di un materiale informativo vasto e complesso. Per quanto concerne invece l'accessibilità, si vuole dare all'interessato la possibilità di capire immediatamente dove trovare le informazioni utili a comprendere le dinamiche del trattamento; a proposito di ciò il Gruppo di lavoro suggerisce alcune modalità: «dichiarazione/informativa sulla privacy stratificata online, in FAQ, mediante pop-up contestuali che si attivano quando l'interessato compila un modulo online oppure, in un contesto digitale interattivo, attraverso un'interfaccia chatbot, ecc.»[873].

Per quanto riguarda le app invece, l'informativa andrebbe posta già nello *store*, quindi comunicata prima ancora del *download*[874].

Ancora, per garantire un maggiore controllo dei dati, dev'essere data agli interessati la possibilità di accedere e modificare i dati direttamente sul posto prima che questi vengano inviati al titolare del trattamento[875]. Utili a tal proposito possono essere le c.d. notifiche *push*, che segnalano direttamente all'interessato eventuali informazioni da conoscere.

A. *Automated decision making*

Tali norme relative al principio di trasparenza divengono di particolare complessità interpretativa nell'ambito dell'*IoT*, caratterizzato dai trattamenti perpetrati attraverso procedimenti decisionali automatizzati, cui il GDPR dedica un'apposita disciplina[876]. Attraverso specifiche disposizioni volte a rendere il trattamento quanto più trasparente possibile si tenta di mitigare i rischi derivanti dalla *black-box society*[877], evitando il che

2016/679 adottate il 29 novembre 2017 ed emendate l'11 aprile 2018 (WP 260), pag. 7. Disponibili online al seguente link:

https://www.garanteprivacy.it/regolamentoue/trasparenza

[872] Ibidem.

[873] Ibidem.

[874] Ibidem.

[875] Parere numero 8 del 16 Settembre 2014 sui recenti sviluppi nel campo dell'Internet degli oggetti, 2014, pag. 25.

[876] «Per scongiurare tali rischi il principale strumento è costituito dalla trasparenza, principio che trova collocazione nel GDPR e nel codice della privacy, ma che, calato nel contesto degli algoritmi e dell'intelligenza artificiale, fatica ad essere concretamente ed efficientemente applicato», Sandulli S., *Algoritmi, trasparenza ed effettività del consenso*, Jus civile, volume 5, 2021, pag. 1533.

[877] Espressione riconducibile a Pasquale F., *The Black Box Society: The Secret Algorithms That Control Money and Information*, 2015.

la macchina prenda il sopravvento sull'uomo[878]. Di seguito si proverà ad evidenziare le difficoltà relative al garantire il principio predetto negli ambienti di *IoT*, proseguendo nell'esempio del paragrafo precedente.

Si prosegue nell'esempio proposto nel precedente paragrafo, relativo allo *smartwatch* e ai servizi di IA di terzi. Come predetto, i dati generati dallo *smartwatch* di Tizio vengono immagazzinati ed elaborati nel *cloud* di Alfa. Una volta terminato il trattamento per cui i dati sono stati raccolti, essi vengono anonimizzati, perfettamente in linea con quanto stabilito dal GDPR[879]. I dati generati attraverso quelle specifiche app dello *smartwatch*, una volta anonimizzati, vengono conservati in *dataset* specifici nel *cloud* di Alfa, ognuno dedicato a questa o quell'app. Il complesso dei *dataset* anonimi viene così messo a disposizione di terze parti, tra cui istituti di credito.

Tizio necessita di un mutuo per aprire l'attività dei suoi sogni, e si rivolge ad un istituto di credito (che è tra quelli che raccoglie informazioni presso Alfa). La banca, nella sua attività di analisi preventiva relativa alla concessione o meno del credito, si affida ad un algoritmo non proprietario di *credit scoring*, che esamina la posizione del richiedente (in questo caso Tizio) e assegna a questi un punteggio da uno a cento relativo alla sua affidabilità. Per i soggetti che ottengono un punteggio da 1 a 33, il finanziamento viene negato; per chi ottiene un punteggio tra 34 e 66 il credito viene concesso con tassi di interesse elevati; a chi ottiene invece uno *score* tra 67 e 100 viene assegnato il finanziamento con tassi agevolati.

Nel caso di Tizio il punteggio è di 50, dunque l'algoritmo gli attribuisce il finanziamento, ma con tassi d'interesse elevati.

Essendo nell'ambito di un trattamento totalmente anonimizzato, ai sensi dell'articolo 22 GDPR Tizio viene informato del fatto che i suoi dati sono stati trattati in via autonoma dall'algoritmo. Tizio, sfruttando il meccanismo di tutela apprestato dall'articolo 22 GDPR, richiede dunque l'intervento del dirigente della banca[880], di modo che questi possa verificare il corretto funzionamento del meccanismo di *credit scoring*, per escludere errori. Oltre alla logica dell'algoritmo, tra le varie informazioni che vengono fornite a Tizio, vi è la spiegazione secondo cui l'algoritmo non reputa affidabili gli

[878] «Garantire che l'uomo possa comprendere la macchina persegue infatti una palese finalità`: assicurare che l'intelligenza artificiale sia – e rimanga – strumentale rispetto a quella umana. Ciò attiene al nucleo essenziale del concetto filosofico e del principio giuridico della dignità dell'uomo», Messinetti R., *La tutela della persona umana versus l'intelligenza artificiale. Potere decisionale dell'apparato tecnologico e diritto alla spiegazione della decisione automatizzata*, Contratto e impresa, volume 3, 2019, pag. 869.

[879] In virtù del principio di limitazione della conservazione espresso all'articolo 5 GDPR, al termine del trattamento i dati non possono essere conservati di modo da permettere l'identificabilità dell'interessato. L'anonimizzazione viene dunque utilizzata per continuare a lavorare sui dati, che seppur anonimi e dunque meno preziosi, possono comunque essere molto utili.

[880] «Qualsiasi riesame dovrebbe essere effettuato da una persona che dispone dell'autorità e della competenza adeguate per modificare la decisione», linee guida del 6 Febbraio 2018 sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679, (WP 251), pag. 30.

individui sotto i 40 anni, con contratto a termine (dati forniti da Tizio al momento della richiesta del finanziamento); oltre a ciò, Tizio viene informato del fatto che l'algoritmo si nutre anche dei dati (anonimizzati) conservati da diversi soggetti che rendono disponibili le proprie banche date, tra cui Alfa. Così, ricollegando Alfa alla casa madre del suo *smartwatch*, ed intuendo che possano essere stati trattati anche i suoi dati così raccolti, richiede l'accesso ai sensi dell'articolo 15 GDPR, di modo da capire come ha funzionato l'algoritmo nel suo caso specifico.

Così scopre che il *credit score* che gli ha attribuito elevati tassi d'interesse è stato ottenuto attraverso un calcolo statistico[881]: in particolare, l'algoritmo ha valutato innanzitutto lo storico dei clienti della banca sotto i 40 anni, con contratto a termine e provenienti dai quartieri a sud della città, residenza di Tizio, per valutare che tipo di affidabilità debitoria presentino, valutando così il gruppo entro cui potrebbe essere incluso Tizio.

Una volta ottenuto lo *score* di tali soggetti, la banca utilizza i dati anonimi ottenuti da Alfa e una serie di altri soggetti proprietari di banche dati anonime, e attraverso un algoritmo proprietario ricava da questi alcuni *pattern* comportamentali. Innanzitutto, tali profili comportamentali non sono riferibili a individui, dunque rimangono dati anonimi, ma sono relativi l gruppo di soggetti che potrebbero avere meno di 40 anni, di sesso maschile, residenti nei quartieri del sud, in cui l'algoritmo ritiene di poter includere Tizio.

Attraverso l'analisi dei dati relativi al battito cardiaco, sono stati individuati nei *dataset* i soggetti con un'età indicativa tra i 35 e i 55 anni. Grazie alle informazioni concernenti la posizione, non abbastanza specifica da permettere l'individuazione o l'individuabilità (magari perché si aggiorna ogni duecento metri), si è individuato un gruppo riconducibile a quella porzione di popolazione abitante i quartieri a sud (durante la notte la posizione rimane ferma in quelle zone). Incrociate tali informazioni con quelle concernenti il battito cardiaco, si è compreso che, sempre a livello statistico, quel gruppo di individui presenta un basso livello di attività fisica giornaliera (gli individui tra i 35 e i 55 anni individuati si spostano poco durante il giorno). In più si ricava come quelle zone siano particolarmente movimentate durante l'orario notturno: l'app del contapassi segnala spostamenti di diversi soggetti (anonimi) in quelle ore e il battito cardiaco di

[881] «*In the area of machine learning, several algorithms are used, which could also be referred to as ways of calculating desired predictions with the use of data. Many of these algorithms are statistical methods and most of them are based on so-called 'regression methods'. These are the most widely used statistical techniques for calculating the influence of a set of data on a selected outcome. For example, consider calculating the average influence of drinking alcohol on life expectancy. Using existing data, the average amount of alcohol a person drinks is compared to their life expectancy. Based on these calculations, life expectancy can be calculated and predicted for other persons simply by taking into consideration the amount of alcohol a person drinks, assuming a correlation exists*», Agenzia europea dei diritti fondamentali, *#BigData: Discrimination in data-supported decision making*, 30 Maggio 2018, pag. 4.

diversi individui lascia intendere l'utilizzo di sostanze stupefacenti o il consumo di alcolici sempre durante le ore notturne. Analizzando tali dati, e anche altri provenienti da altre banche dati, relativi ad un periodo di tempo medio-lungo (ad esempio un anno), l'algoritmo completa la profilazione di gruppi di individui.

Da ciò la macchina deduce che i soggetti che abitano quei quartieri a sud, tra i 35 e i 55 anni, conducono uno stile di vita poco coniugabile con il profilo di persona cui la banca vorrebbe affidare finanziamenti; chi ha progettato il codice ha fatto in modo che questi soggetti ottenessero uno *score* basso, poiché riteneva fossero persone inclini alla vita mondana, e quindi con medio-basse possibilità di pagare il debito contratto con la banca.

Da tale esempio, semplicistico per ovvie ragioni, risulta chiaramente come attraverso informazioni anonime ed apparentemente innocue, inerenti aspetti riconducibili al c.d. *quantified self*, possano derivare decisioni fortemente lesive[882].

Nel caso del *credit scoring*, come detto, Tizio ha diritto alla tutela *ex* articolo 22 del Regolamento. La disposizione menzionata stabilisce al primo paragrafo che «l'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona». Il secondo paragrafo prevede tre eccezioni a tale divieto, ed una è rappresentata dal consenso dell'interessato. In questo caso, ai sensi del terzo paragrafo, il titolare del trattamento «attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione». Infine, al quarto paragrafo, si impone un limite al trattamento automatizzato, e si prescrive che non può basarsi sui dati particolari «a meno che non sia d'applicazione l'articolo 9, paragrafo 2, lettere a) o g), e non siano in vigore misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato».

L'applicazione della disposizione descritta si deve dunque al verificarsi di tre fattori: a) una decisione; b) basata unicamente sul trattamento automatizzato; c) che produca effetti giuridici o che incida in modo analogo. Nell'esempio del *credit scoring* è possibile ravvisare una decisione in quanto

[882] «Il quantified self illustra anche quante informazioni possano essere tratte da sensori di movimento attraverso l'aggregazione e l'analisi avanzata. Questi dispositivi utilizzano spesso sensori elementari per acquisire dati grezzi (ad esempio i movimenti dell'interessato), si basano su algoritmi sofisticati per estrarre informazioni sensibili (ad esempio il numero dei passi) e deducono informazioni potenzialmente sensibili che saranno poi mostrate agli utenti finali (ad esempio le sue condizioni fisiche). Tale tendenza pone problemi specifici: l'utente accettava di condividere le informazioni originarie per uno scopo specifico, ma potrebbe non voler condividere tali informazioni secondarie, che potrebbero essere utilizzate per scopi completamente differenti», parere numero 8 del 16 Settembre 2014 sui recenti sviluppi nel campo dell'Internet degli oggetti, 2014, pag. 9.

l'algoritmo influisce sulla sfera soggettiva di Tizio, influenzandola[883]. Essa è inoltre basata unicamente sul trattamento automatizzato in quanto non si ha un ruolo umano, ma come già chiarito, la decisione si intenderebbe tale in tutti i casi in cui non vi è un significativo effetto umano[884]. L'*output* consistente nell'assegnare un certo *score* e quindi un determinato tasso di interesse non può essere definito una decisione che produce effetti giuridici in quanto non produce un mutamento sui diritti o sugli obblighi[885]; tuttavia tale fattispecie, secondo chi scrive, è riconducibile alla fattispecie espressamente prevista come esempio dal considerando numero 71 tra quelle che incidono in modo analogo significativamente sulla sua persona, ossia al «rifiuto automatico di una domanda di credito online»[886]. Inoltre, sempre le summenzionate linee guida sul trattamento automatizzato, nell'esemplificare casi di decisioni che possono portare a conseguenze «significative» si riferiscono a «decisioni che influenzano le circostanze finanziarie di una persona, come la sua ammissibilità al credito». Per questi motivi, Tizio ha diritto alla tutela prevista nei casi di trattamenti perpetrati attraverso procedimenti decisionali automatizzati.

Questa, si concreta innanzitutto in un generale divieto di prendere decisioni basate soltanto su trattamenti automatizzati. Nel caso si verifichino le eccezioni previste dal secondo paragrafo invece, la protezione si realizza attraverso il ricevimento delle informazioni previste dagli articoli 13, 14 e 15 GDPR e in forza di quanto previsto dall'articolo 22 GDPR[887].

Gli articoli 13 paragrafo 2, lettera f), e 14 paragrafo 3, lettera g), statuiscono in modo identico che all'interessato vada data comunicazione in merito alla «esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato». Di egual tenore

---

[883] Edwards L., Veale M., *Enslaving the algorithm: from a "right to explanation" to a "right to better decision"?*, IEEE Security & Privacy, volume 16, numero 3, 2018, pag. 3. Disponibile online al seguente link: https://arxiv.org/pdf/1803.07540.pdf

[884] Linee guida del 6 Febbraio 2018 sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679, (WP 251), pag. 23.

[885] Ibidem.

[886] Considerando numero 71: «l'interessato dovrebbe avere il diritto di non essere sottoposto a una decisione, che possa includere una misura, che valuti aspetti personali che lo riguardano, che sia basata unicamente su un trattamento automatizzato e che produca effetti giuridici che lo riguardano o incida in modo analogo significativamente sulla sua persona, quali il rifiuto automatico di una domanda di credito online o pratiche di assunzione elettronica senza interventi umani…».

[887] «In sintesi, l'articolo 22 stabilisce che: i) di norma, esiste un divieto generale all'adozione di decisioni completamente automatizzate relative alle persone fisiche, compresa la profilazione, che hanno un effetto giuridico o che incidono in modo analogo significativamente; ii) esistono eccezioni alla regola; iii) laddove si applichi una di tali eccezioni, devono essere adottate misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato», Linee guida del 6 Febbraio 2018 sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679, (WP 251), pag. 22.

letterale anche la previsione *ex* articolo 15 GDPR, secondo cui l'interessato ha il diritto di ottenere l'accesso ai dati personali in relazione alla «esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato».

Gli articoli 13 e 14 GDPR instaurano un diritto ad essere informati, mentre il contenuto dell'obbligo *ex* articolo 15 GDPR non si limita ad un semplice dovere informativo. Tali norme sono convergenti: il titolare deve portare avanti il trattamento in modo trasparente. Con ciò, l'interessato deve avere a disposizione le informazioni che gli permettono di comprendere come vengono trattati i suoi dati: le norme fanno esplicito riferimento alla «esistenza di un processo decisionale automatizzato», ad «informazioni significative sulla logica utilizzata» e alla «importanza e le conseguenze previste di tale trattamento per l'interessato», ed in virtù di quanto affermato nel considerando numero 39, è necessario che tali informazioni «siano facilmente accessibili e comprensibili e che sia utilizzato un linguaggio semplice e chiaro».

Tali norme vengono fortemente messe alla prova nella *black-box society*, in cui gli algoritmi presentano diversi elementi di opacità, sia per gli interessati che per i titolari stessi. A proposito di ciò, si sono formati due orientamenti contrapposti: l'uno secondo cui, alla luce della lettura combinata degli articoli 13, 14, 15 e 22 GDPR non esisterebbe un diritto alla spiegazione *ex post* della decisione algoritmica, e l'altro secondo cui esisterebbe[888] (il diritto in questione è stato definito in diversi modi: *right to legibility*[889]; *right to explanation*[890] ecc.).

Il primo orientamento, secondo cui non esisterebbe un diritto ad aprire la *black box* algoritmica, si fonda sull'assunto secondo cui i doveri informativi *ex* articoli 13 e 14 GDPR precedono rispetto al trattamento: il tenore letterale delle norme fa riferimento alle «conseguenze previste», e in virtù di tale fattore temporale (*timeline problem*) si ritiene non possa essere accolta la ricostruzione di un diritto alla spiegazione successiva della decisione[891]. L'unico riferimento ad un *right to explanation* si ritroverebbe al

[888] Le opere principali cui puòo essere ricondotti tali orientamenti sono: Wachter S., Mittelstadt B., Floridi L., *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, International Data Privacy Law, volume 7, numero 2, 2017 e Malgieri G., Comandè G., *Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation*, International Data Privacy Law, volume 7, numero 3, 2017. Disponibile online al seguente link:
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3088976

[889] In questi termini Mortier R., Haddadi H., Henderson T., McAuley D., Crowcroft J. *Human-Data Interaction: The Human Face of the Data-Driven Society*, 2014.

[890] In questi termini Wachter S., Mittelstadt B., Floridi L., *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, 2017.

[891] Ibidem, pag. 82.

considerando numero 71, che non è però vincolante[892]. Per quanto concerne invece l'articolo 15 GDPR, pur ammettendosi che questo si presti maggiormente all'avallo di una spiegazione della decisione *ex post*, si nota come anch'esso faccia riferimento alle «conseguenze previste», permarrebbe dunque il *timeline problem*.

Quanto detto verrebbe anche suffragato dai lavori preparatori del testo del Regolamento: si sottolinea infatti come nelle bozze precedenti l'approvazione si scorga la volontà del Parlamento europeo di inserire uno specifico diritto alla spiegazione postuma; Il Consiglio europeo invece denotava una volontà meno netta, preferendo il *right to legibility* in un considerando. A questi si contrapponeva il volere della Commissione, che si oppose a tali orientamenti escludendo *in toto* tale diritto[893].

Conseguenza di queste premesse è che il contenuto informativo delle comunicazioni *ex* articoli 13, 14 e 15 GDPR verterebbe soltanto in merito all'esistenza del trattamento decisionale automatizzato, al suo generico funzionamento, alle finalità dello stesso e alle conseguenze previste in una prospettiva *ex ante* (si parla a proposito di un *right to be informed*)[894]. Dunque, nessuna notizia in merito al come e perché la successiva decisione è stata formulata, e in questo senso sembrerebbe deporre anche un passo delle linee guida summenzionate: «il regolamento impone al titolare del trattamento di fornire informazioni significative sulla logica utilizzata, ma non necessariamente una spiegazione complessa degli algoritmi utilizzati o la divulgazione dell'algoritmo completo»[895].

L'orientamento invece più estensivo, che ammette il diritto ad una spiegazione *ex post*, si fonda non tanto sugli articoli 13 e 14, ma sugli articoli 15 e 22 paragrafo 3 GDPR. Quest'ultimo, tra le altre, prevede che il titolare del trattamento attui misure volte a garantire *almeno* «il diritto di ottenere l'intervento umano da parte del Titolare del trattamento, di esprimere la propria opinione di contestare la decisione», e se la trasparenza è il mezzo attraverso cui rendere effettivo l'esercizio dei diritti, allora il titolare del trattamento dovrà fornire all'interessato le informazioni utili a comprendere la decisione subìta, di modo da poterla financo contestare; difatti, l'assenza di un'adeguata informazione in merito alla decisione rischia di svuotare il diritto alla contestazione[896]. Inoltre, si sottolinea che qualora il diritto

[892] Ibidem.

[893] Ibidem, pag. 96.

[894] Ibidem.

[895] Linee guida del 6 Febbraio 2018 sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679, (WP 251), pag. 28.

[896] «Il titolare del trattamento dovrebbe fornire all'interessato informazioni di carattere generale (in particolare, sui fattori presi in considerazione per il processo decisionale e sul rispettivo "peso" a livello aggregato) che sono utili all'interessato anche per contestare la decisione», linee guida del 6 Febbraio 2018 sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679, (WP 251); nello stesso senso Mendoza I., Bygrave L. A., *The Right not to be Subject to Automated Decisions based on Profiling*, Research Paper Series, Oslo, numero 20, 2017, pag. 23. Disponibile online al seguente link:

d'accesso fosse esercitato dopo aver ricevuto la decisione derivante dal trattamento automatizzato, quindi in un momento successivo rispetto alla ricezione delle informazioni *ex* articoli 13 e 14 GDPR, il contenuto informativo non potrebbe essere identico a quello apprestato da tali ultime due norme[897]. Fornire *ex post* le medesime informazioni già offerte prima dell'avvio del trattamento sarebbe del tutto inutile: se ai sensi degli articoli 13 e 14 GDPR va edotto l'interessato in merito alla logica utilizzata dall'algoritmo, al termine del trattamento andrebbe detto qualcosa in più.

Attraverso questi argomenti si arriva alla formulazione di un diritto alla spiegazione della decisione *de quo*[898], che dovrà tenere conto dei passaggi inferenziali che hanno portato a quel determinato *output*[899]. In altre parole, andrà spiegato in modo chiaro e semplice all'interessato come *ragiona* l'algoritmo: sulla base di quali dati ha deciso, da quali fonti ha ottenuto i dati, il peso che questi hanno avuto nel processo che ha condotto a quella decisione ecc.; quali misure ha adottato per evitare malfunzionamenti o distorsioni dell'algoritmo[900].

Chi scrive ritiene preferibile l'orientamento espansivo appena descritto[901]. In tal senso deporrebbe anche un'interpretazione delle norme analizzate alla luce dell'approccio *risk-based* tipico del principio di *accountability*. Nei paragrafi precedenti si è fatto riferimento ai *bias* degli algoritmi e dei rischi che questi comportano. Si ritiene che la tutela apprestata dal combinato disposto degli articoli 15 e 22 GDPR possa essere utile a prevenire la realizzazione di tali rischi solo se la persona fisica interessata sia adeguatamente informata sulla specifica decisione patita. Questa, infatti, notando un *output*[902] non coerente con la sua persona sarebbe nella posizione di segnalare il problema al titolare del trattamento, e questo potrebbe operare dei controlli per verificare la correttezza del funzionamento dell'algoritmo. Un trattamento automatizzato non corretto potrebbe violare il principio di esattezza previsto dall'articolo 5 del

---

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2964855

[897] Troisi E., *Decisione algoritmica. Black-box e AI etica: Il diritto di accesso come diritto a ottenere una spiegazione*, 2022, pag. 965.

[898] «*In sum, according to Article 15(1)(h), data controllers are obliged to disclose information about the logic actually employed, and not only about the general system functionality of an algorithmic decision-making*», Malgieri G., Comandè G., *Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation*, 2017, pag. 21.

[899] Troisi E., *Decisione algoritmica. Black-box e AI etica: Il diritto di accesso come diritto a ottenere una spiegazione*, 2022, pag. 964.

[900] Ibidem, pag. 962.

[901] Per un orientamento misto, secondo cui si potrebbe arrivare alla spiegazione della decisione *de quo* attraverso un corretto dovere informativo *ex ante*, vedasi Selbst A. D., Powles J., *Meaningful Information ant the Right to Explanation*, International Data Privacy Law, volume 7, numero 4, Novembre 2017.

[902] Troisi E., *Decisione algoritmica. Black-box e AI etica: Il diritto di accesso come diritto a ottenere una spiegazione*, 2022, pag. 964 precisa la natura di dato personale del punteggio ottenuto.

Regolamento, in quanto un *output* errato potrebbe ben essere frutto di dati personali non esatti valutati nelle inferenze dell'algoritmo[903]. Una corretta gestione del rischio impone al titolare del trattamento di fare quanto possibile per evitare che si verifichino danni all'interessato. Da una mancata spiegazione sulla decisione *de quo* potrebbero causarsi danni alla persona interessata, che invece ben potrebbero essere evitati con l'intervento informato di questa, posta nella posizione di indicare errori del trattamento, o addirittura discriminazioni, di richiedere la rettifica *ex* articolo 16 GDPR.

Rifacendosi al caso di Tizio che chiede un finanziamento in banca e ottiene uno *score* che gli impone di pagare importanti tassi d'interesse. Mettere Tizio nella posizione di contestare il punteggio e di indicare dove l'algoritmo avrebbe sbagliato condurrebbe ad una nuova valutazione dello *score* da parte del dirigente di banca. Potrebbe infatti darsi che Tizio non appartenga a quel gruppo in cui è stato incluso, magari perché astemio, perché non avvezzo alla vita mondana, oppure potrebbe essere un soggetto che in virtù di un lavoro particolare (ad esempio il tassista) sia costretto a lavorare di notte. Solo sapendo come l'algoritmo abbia valutato la sua età e la sua provenienza potrebbe contestare di non appartenere quel determinato gruppo, evitando così la realizzazione del pregiudizio.

Il combinato disposto degli articoli 15 e 22 GDPR sembra dunque offrire al titolare del trattamento uno strumento di *accountability*. Nello specifico, l'istituto di credito titolare del trattamento dovrebbe indicare a Tizio il punteggio assegnatogli; su quali informazioni si è basato per ottenere lo *score*: quindi i dati da questi immessi nel modulo di domanda; eventuali insolvenze pregresse, informazioni derivanti da registri pubblici ufficiali, quali i registri di frodi e i registri d'insolvenza; dati provenienti da banche dati private; il peso attribuito ad ogni fattore e quindi i criteri per i quali la valutazione complessiva di questi dati ha condotto a quel determinato punteggio. Ancora, andranno indicate le misure preposte per garantire i diritti, le libertà e gli interessi dell'interessato (si pensi agli *audits*, di cui si dirà a breve).

Un altro elemento volto a rendere trasparente il trattamento potrebbe ravvisarsi nel disposto dell'articolo 35 paragrafo 9 del Regolamento, secondo cui «se del caso, il titolare del trattamento raccoglie le opinioni degli interessati e dei loro rappresentanti sul trattamento previsto, fatta salva la tutela degli interessi commerciali o pubblici o la sicurezza dei trattamenti». Una volta conferite le informazioni relative alla logica utilizzata dall'algoritmo, richiedere tali opinioni potrebbe essere un forte elemento di *accountability*: l'interessato o i suoi rappresentanti potrebbero esprimere perplessità, o indicare dati riguardanti l'interessato da immettere nel processo decisionale automatizzato di modo da non creare un profilo

[903] «Dunque, la qualita` dei dati diviene essenziale. Da dati qualitativamente non corretti, non possono che scaturire elaborazioni non corrette, secondo il noto principio ''garbage in, garbage out''», Finocchiaro G., *Intelligenza Artificiale e protezione dei dati personali*, Giurisprudenza Italiana, 2019, pag. 1674.

distorto[904]. In un'ottica di prevenzione del rischio una politica di tal fatta potrebbe rivelarsi molto utile in sede di dimostrazione del proprio essere *accountable*.

Volgendo per un attimo lo sguardo al prossimo futuro, può esaminarsi quanto sancito nella proposta di regolamento per l'IA[905]. L'articolo 13 paragrafo 1 stabilisce che i «sistemi di IA ad alto rischio sono progettati e sviluppati in modo tale da garantire che il loro funzionamento sia sufficientemente trasparente da consentire agli utenti di interpretare l'output del sistema e utilizzarlo adeguatamente». Da ciò potrebbe scorgersi un obbligo a fornire informazioni sulla decisione algoritmica e specularmente un riconoscimento del diritto ad essere informati sullo specifico *output*; tuttavia, il medesimo paragrafo prevede anche che «sono garantiti un tipo e un livello di trasparenza adeguati, che consentano di conseguire il rispetto dei pertinenti obblighi dell'utente e del fornitore di cui al capo 3 del presente titolo», ed il capo III non prevede un simile obbligo». La questione non potrà dunque dirsi risolta neppure con una regolamentazione sull'IA[906].

L'*accountability* del titolare del trattamento potrebbe però essere messa in discussione qualora la causa di un *output* discriminatorio sia riconducibile al *core* dell'algoritmo tutelato dal segreto industriale. Tale problematica si pone in minor misura quando il titolare del trattamento sia anche proprietario dell'algoritmo, ma come già visto, spesso nell'*IoT* si assiste ad una condivisione di spazi, capacità computazionali e mezzi di ogni tipo.

Nel caso descritto, l'istituto di credito non è proprietario dell'algoritmo utilizzato, e in caso di intervento dell'interessato (Tizio) che chieda «informazioni significative sulla logica utilizzata» per la decisione ai sensi dell'articolo 15 GDPR, potrebbero verificarsi delle frizioni tra la disciplina della protezione dei dati personali e quella della tutela dei segreti industriali. Di ciò si occupa il considerando numero 61, che riferendosi al diritto di accesso afferma: «tale diritto non dovrebbe ledere i diritti e le libertà altrui, compreso il segreto industriale e aziendale e la proprietà intellettuale, segnatamente i diritti d'autore che tutelano il software», e allo stesso tempo

---

[904] «Il diritto all'identità, di riflesso, assume nuove connotazioni, in quanto implica non più soltanto la «corretta rappresentazione in ciascun contesto», ma presuppone una «rappresentazione integrale della persona» e per di più «rappresentazione non affidata solo agli strumenti automatizzati», Resta G., *Identità personale e identità* digitale, 2007, pag. 522.

[905] Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale del 21 Aprile 2021. Disponibile online al seguente link:

https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A52021PC0206

[906] «Quindi, sebbene la Proposta di Regolamento sull'intelligenza artificiale dimostri che l'obiettivo perseguito a livello europeo sia di garantire una normativa equilibrata, che incentivi l'utilizzo dell'IA assicurando il rispetto dei diritti fondamentali, essa non contiene riferimenti specifici alla *conoscibilità* dell'algoritmo», Sandulli S., *Algoritmi, trasparenza ed effettività del consenso*, 2021, pag. 1536.

«tali considerazioni non dovrebbero condurre a un diniego a fornire all'interessato tutte le informazioni». Sembra dunque rinvenirsi una tensione all'interno del Regolamento, relativa alla possibilità o meno di disvelare i segreti commerciali in nome della trasparenza. Per tale ragione, al fine di fare chiarezza sul punto la dottrina ha fatto riferimento a quanto espresso in altre discipline.

Prendendo innanzitutto in esame la direttiva sui segreti commerciali[907], il considerando numero 35 prevede che «la presente direttiva non dovrebbe pertanto pregiudicare i diritti e gli obblighi stabiliti dalla direttiva 95/46/CE, in particolare i diritti della persona interessata di accedere ai suoi dati personali che sono oggetto di trattamento e di ottenere la rettifica, la cancellazione o il congelamento dei dati incompleti o inesatti e, se del caso, l'obbligo di trattare i dati sensibili conformemente all'articolo 8, paragrafo 5, della direttiva 95/46/CE». Sembra dunque ammettersi la rivelazione del segreto; nello stesso senso si muove il Gruppo di lavoro nelle linee guida sui processi decisionali automatizzati, in cui si afferma che «il titolare del trattamento non può fare affidamento sulla protezione dei segreti aziendali come scusa per negare l'accesso o rifiutarsi di fornire informazioni all'interessato»[908]. Di recente, il Consiglio d'Europa, in una raccomandazione sull'impatto dei sistemi algoritmici sui diritti umani, ha stabilito che le normative sulla proprietà intellettuale o industriale non dovrebbero precludere la trasparenza e non dovrebbero essere sfruttati a tal fine[909]. Pertanto, la *quaestio* viene risolta alla luce di quanto espresso in altre sedi nel senso della prevalenza del principio di trasparenza rispetto al segreto industriale.

Tuttavia, è stato sottolineato come ammettendo l'accesso agli elementi tutelati, non è detto che si raggiunga quel grado di trasparenza necessario per il corretto esperimento dei diritti.

---

[907] Direttiva (UE) 2016/943 del Parlamento europeo e del Consiglio, dell'8 giugno 2016, sulla protezione del know-how riservato e delle informazioni commerciali riservate (segreti commerciali) contro l'acquisizione, l'utilizzo e la divulgazione illeciti, recepita in Italia dal d.lgs. 11 maggio 2018, numero 63. La direttiva è disponibile online al seguente link: https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX%3A32016L0943

[908] Linee guida del 6 Febbraio 2018 sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679, (WP 251), pag. 19.

[909] «*States should establish appropriate levels of transparency with regard to the public procurement, use, design and basic processing criteria and methods of algorithmic systems implemented by and for them, or by private sector actors. The legislative frameworks for intellectual property or trade secrets should not preclude such transparency, nor should States or private parties seek to exploit them for this purpose. Transparency levels should be as high as possible and proportionate to the severity of adverse human rights impacts, including ethics labels or seals for algorithmic systems to enable users to navigate between systems. The use of algorithmic systems in decision-making processes that carry high risks to human rights should be subject to particularly high standards as regards the explainability of processes and outputs*», articolo 4 paragrafo 1 («*levels of transparency***»)**, raccomandazione CM/Rec (2020) 1 del Comitato dei ministri agli Stati membri sull'impatto dei sistemi algoritmici sui diritti umani.

Ad esempio, la *disclosure* del codice sorgente potrebbe rivelarsi totalmente infruttuosa nell'ottica di una trasparenza strumentale all'esercizio del controllo sui propri dati[910]. Si evidenzia come le istruzioni che compongono il codice siano espresse in un linguaggio di programmazione non intellegibile ai più[911]. La trasparenza reca con sé i requisiti della chiarezza e della comprensibilità come indicato dal considerando numero 39, e una divulgazione di segreti commerciali quali il codice sorgente potrebbe risultare non utile all'obiettivo del rispetto del principio di trasparenza[912]. L'opacità caratterizzante tali sistemi, infatti, non è dovuta solamente all'applicabilità della disciplina sulla proprietà industriale. La consegna dei documenti riportanti il linguaggio di programmazione potrebbe non essere sufficiente per essere considerati *accountable*. Questa dovrà essere accompagnata anche da informazioni chiare e semplici utili a comprendere i documenti dettagliati relativi al codice. Si ritorna dunque al problema dell'intellegibilità dei meccanismi sottostanti il funzionamento di tali macchine, che potrà essere risolto solamente attraverso una spiegazione leggibile offerta dal titolare del trattamento, pena la violazione del principio di trasparenza nella sua specifica declinazione del contenuto del diritto di accesso[913]. Tali obblighi risultano particolarmente gravosi da rispettare, soprattutto in relazione ai meccanismi di IA, difficilmente comprensibili anche ai proprietari[914].

---

[910] Bravo F., *Trasparenza del codice sorgente e decisioni automatizzate*, Il diritto dell'informazione e dell'informatica, 2020, pag. 714.

[911] De Rosa P., in merito al problema della complessità parla di *technoapartheid* e tecnoconsapevolezza in *Diritti e libertà in Internet: un mondo digitale è davvero sinonimo di libertà?*, Data Protection Law, numero 1, 2022.

[912] «Le istruzioni (in linguaggio di programmazione) con cui vengono scritti i programmi utilizzati per l'adozione di decisioni automatizzate non seguono una "logica lineare", ma modelli "euristici" basati su "sistemi esperti" o su reti "neurali": dovendo gestire quella che viene definita "un'esplosione combinatoria", forniscono "meta-regole" o altre strategie di funzionamento che consentono al software di decision-making, unitamente ad una base di conoscenze prede- terminate ed incrementali (anche mediante sistemi di machine learning capaci di autoapprendimento), di raggiungere soluzioni non predeterminabili sulla base delle sole istruzioni contenute nel codice sorgente», Bravo F., *Trasparenza del codice sorgente e decisioni automatizzate*, 2020, pag. 715.

[913] «L'inadeguatezza del GDPR rispetto all'intelligenza artificiale e all'impiego degli algoritmi dimostra così che l'obiettivo di trasparenza non si adatta realmente al contesto digitale, contraddistinto da caratteristiche tecniche estremamente complesse e da un'opacità che difficilmente sembra limitabile, imponendo di ripensare gli strumenti di funzione della privacy. Ciò considerando, peraltro, che anche qualora il soggetto interessato fosse portato a conoscenza del c.d. codice sorgente, il processo decisionale rimarrebbe comunque ignoto e incomprensibile - e di conseguenza anche inutile - in virtù dei tecnicismi che contraddistinguono l'algoritmo e, dunque, più che al diritto all'informazione sarebbe opportuno riferirsi ad un diritto alla spiegazione quale ricerca di equilibrio fra le esigenze di trasparenza del processo decisionale automatizzato il progresso digitale», Sandulli S., *Algoritmi, trasparenza ed effettività del consenso*, 2021, pag. 1538.

[914] «Il paradigma della trasparenza sarebbe stato impropriamente trasposto in un contesto – l'ambiente digitale – connotato da caratteristiche strutturali che condannano il paradigma medesimo alla fallacia e a generare nuove opacita», Messinetti R., *La tutela della*

5.3.4 I principi di *data protection by design*, *data protection by default* e *security by design*

I principi di *data protection by design* (di seguito anche Dpbd) e *data protection by default* sono oggi previsti principalmente dall'articolo 25 del GDPR, ma come si vedrà a breve essi costituiscono un principio ampio, che ingloba all'interno diverse altre disposizioni.

Il *core* della Dpbd è rappresentato dall'obbligo per il titolare del trattamento di progettare l'intera catena del trattamento in modo conforme al Regolamento (*latu sensu*), così da assicurare la conformità richiesta dal principio di *accountability* già da un momento precedente rispetto a quello dell'effettivo trattamento («al momento di determinare i mezzi del trattamento»). Il motivo per cui si è scelto di prestare un paragrafo alla Dpbd nell'*IoT* è presto detto: il nesso tra responsabilizzazione e Dpbd è fondamentale. Nell'*IoT*, vista la complessità della catena del trattamento, sarebbe difficile, se non impossibile, assicurare la tutela dei dati personali se questa non fosse stata prevista sin dalla fase di sviluppo dei *softwares* e degli *hardwares*. Un esplicito riferimento si ha al considerando numero 78, che rimanda all'opportunità di far rispettare le norme sulla protezione dei dati personali financo agli sviluppatori. In ciò, si rivede quella dottrina ormai consolidata che vede già nel codice il primo punto da cui iniziare ad implementare le misure utili alla protezione dei dati personali e delle libertà fondamentali[915].

Tra gli aspetti fondamentali legati alla Dpbd vi è quello della sicurezza. Come a breve si vedrà, essa è un aspetto fondamentale per tutelare la protezione dei dati personali e delle libertà fondamentali, specialmente nell'*IoT*. Tali contesti sono infatti caratterizzati dalla complessità, intesa nel suo significato più antico di *complexus*, ossia tessuto insieme. Le varie fasi del trattamento, i diversi luoghi in cui questo avviene e i diversi soggetti agli ordini dei quali si sviluppa, costituiscono momenti diversi di un medesimo trattamento. Pertanto, affinchè questo possa essere idoneo a garantire le libertà degli individui, sarà necessario che sia posto al sicuro da agenti endogeni ed esogeni. Il primo passo da compiere per raggiungere tale risultato è una corretta pianificazione delle misure volte a proteggere i sistemi, quindi i dati, dunque gli individui.

La scelta di parlare di *security by design* (nel titolo del paragrafo) si deve in virtù di questa intima relazione tra Dpbd e sicurezza, indagata in diverse sedi. Già la Federal Trade Commission si esprimeva in tal senso nel

---

persona umana versus l'intelligenza artificiale. Potere decisionale dell'apparato tecnologico e diritto alla spiegazione della decisione automatizzata, 2019, pag. 869.

[915] Si fa riferimento all'opera pioneristica di Lessig L., *Code and Other Laws of Cyberspace*, Basic Books, New York, 1999.

suo report sull'*IoT*, in cui scriveva che «*first, companies should implement "security by design" by building security into their devices at the outset, rather than as an afterthought. One participant stated that security should be designed into every IoT product, at every stage of development, including "early on in the design cycle of a technology*»[916]. Si nota dunque come per i sistemi di IoT si scelga di perseguire la conformità al Regolamento richiesta dal principio di *accountability* mediante un approccio ingegneristico, volto ad affrontare i problemi derivanti dalle nuove tecnologie con altrettanti strumenti tecnologici. In tal senso si muove anche l'Enisa nel documento relati alla privacy by design nell'epoca delle *big data analytics «so, with respect to the underlying legal framework, technology (for big data) should be addressed by technology (for privacy). We cannot deal with new processing operations using old solutions. Therefore, measures for the protection of personal data need to grow together with big data advances*»[917].

Va dunque immaginato un sistema composito di misure tecniche ed organizzative volto a rendere *accountable* ogni fase e luogo del trattamento. Ciò rende quantomai necessaria la collaborazione di tutti i soggetti coinvolti nel trattamento. A tal proposito il Gruppo di lavoro raccomandava affinché tutti gli attori coinvolti nel trattamento applicassero i principi della Dpbd e *by default*[918]. Tuttavia, quanto appena detto stride con la serrata ripartizione delle responsabilità prevista in capo a titolare e responsabile del trattamento ai sensi dell'articolo 82 GDPR. I programmatori, infatti, non risponderebbero ai sensi della predetta norma, essendo al massimo definibili come soggetti autorizzati al trattamento ai sensi dell'articolo 28 paragrafo 3 del Regolamento, che rimangono sotto la responsabilità del titolare del trattamento ai sensi dell'articolo 29 GDPR. Ciò pone seri problemi in ordine alla loro responsabilizzazione.

Inoltre, la sicurezza è uno dei principi generali del trattamento previsti dall'articolo 5 GDPR, e le relative misure sono richieste dal principio di *accountability* nelle sue norme principali: gli articoli 24, 25 e 32, dedicato esclusivamente alla *data security*. La differenza tra l'articolo 24 GDPR e l'articolo 32 GDPR è il fine cui le disposizioni sono dirette: se l'articolo 24 GDPR indirizza alla conformità al Regolamento, l'articolo 32 GDPR richiede che sia realizzata la sicurezza del trattamento. L'articolo 32 offre un elenco non esaustivo di misure applicabili (in base alla valutazione del contesto, dei rischi ecc.) di cui i primi esempi sono la pseudonimizzazione e la cifratura.

[916] Federal Trade Commission, *Privacy & Security in a Internet of Things: Privacy & Security in a Connected World World*, ftc staff report, Gennaio 2015, pag. 44.

[917] Enisa, *Privacy by design in big data. An overview of privacy enhancing technologies in the era of big data analytics*, Dicembre 2015, pag. 20.

[918] Parere numero 8 del 16 Settembre 2014 sui recenti sviluppi nel campo dell'Internet degli oggetti, 2014 pag. 24.

Non serve rammentare come, nel contesto dell'*IoT*, il rischio elevato richiederà misure di sicurezza altrettanto importanti[919].

Proseguendo, nell'ottica di un'adeguata sicurezza dei sistemi, appaiono particolarmente significative le c.d. *privacy enhancing technologies* (*PETs*), definite come l'applicazione di tecnologie di informazione e comunicazione volte a garantire il rispetto della privacy[920]. Queste vengono considerate strumenti operativi fondamentali nella messa in sicurezza dell'Internet delle cose (alcuni esempi di PET verranno forniti più avanti nella trattazione)[921].

I rischi inerenti alla sicurezza vanno dai meri problemi tecnici (ad esempio *black out*), alla naturale obsolescenza delle misure applicate, fino ad arrivare agli attacchi mirati ad opera dei c.d. *hackers*. Quest'ultima ipotesi ha rappresentato fonte di grande preoccupazione soprattutto nell'opinione pubblica, comprensibilmente preoccupata in merito all'intrusione non autorizzata di soggetti malintenzionati. I tipi di attacchi sono molto vari, dall'introduzione di *softwares* e *hardwares* malevoli (*trojan*, corruzione dei nodi ecc.), ad attacchi che inficiano i servizi forniti dai *devices* (ad esempio la privazione della carica della batteria), al c.d. *sniffing* (l'intercettazione di comunicazioni tra i *devices*) ecc.[922]. Tra gli attacchi più significativi ai dispositivi *IoT* vanno menzionati i c.d. *salami attacks*: questi consistono in minime violazioni protratte in larga scala. Spesso hanno riguardato la sottrazione di piccolissime somme di denaro (inferiori al centesimo)[923]. Ad oggi, sono parecchio diffuse le app di *e-banking*, o altre applicazioni comunque idonee a muovere denaro; un attacco su larga scala

---

[919] Nel *Handbook on Security of Personal Data Processing* dell'Enisa (Dicembre 2017) si offrono modalità per la valutazione dei rischi e la consequenziale scelta delle misure di sicurezza. Il documento è disponibile online al seguente link:

https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing

[920] «*The application of information and communications technologies (ICT) for the sake of privacy protection has become widely known under the name of Privacy Enhancing Technologies (PETs*)», Borking J. J., Raab C. D., *Laws, PETs and other Technologies for Privacy Protection*, Journal of Information, Law & Technology (JILT), volume 1, 2001. Tale definizione è accolta dall'Enisa nel suo documento sulle PETs, *Readiness Analysis for the Adoption and Evolution of Privacy Enhancing Technologies*, Dicembre 2015, pag. 2.

[921] «*Without clear limitations on privacy infringements through appropriate PET measures the IoT will be inhibited in its expansion as various laws such as the EU data protection framework and other sector-specific laws (i.e. U.S. HIPAA) restrict the collection of personal data, unless strict requirements as to the data subject's consent or other legal justification are present as well as appropriate security measures are taken*», Weber R. H., *Internet of Things: Privacy issues revisited*, Computer law & security review, volume 31, 2015, pag. 622.

[922] Per una visione sinottica delle famiglie di attacchi più comuni si rimanda a Alwarafi A., Al-Thelaya K. A., Abdallah M., Schneider J., Hamdi M., *A Survey on Security and Privacy Issues in Edge-Computing-Assisted Internet of Things*, IEEE Internet of Things Journal, volume 8, Marzo 2021 pag. 4008 e ss.

[923] D'Acquisto G., Naldi M., *Big data e privacy by design: anonimizzazione pseudonimizzazione sicurezza*, 2017, pag. 197.

consentirebbe agli *hackers* di sottrarre minime somme ad una elevatissima quantità di soggetti. Violare i sistemi di sicurezza dei *devices* per sottrarre denaro significa anche accedere ad una moltitudine di altre informazioni. Ad esempio, è possibile conoscere quasi perfettamente la situazione finanziaria del soggetto (anche la presenza di debiti), oppure notare spese ripetute presso farmacie, o per medicina settoriale (ad esempio oncologia), e quindi entrare in possesso di informazioni molto sensibili. Le misure volte ad impedire la realizzazione di tali rischi sono molte.

Tra le indicazioni volte a rendere *accountable* un trattamento nell'*IoT* si deve fare innanzitutto riferimento all'architettura delle varie fasi del trattamento. Si propone di archiviare ed analizzare i dati secondo modelli distribuiti, sì da tenere separate informazioni che altrimenti, se tenute insieme, porterebbero a generare nuovi dati[924]. Non serve nemmeno precisare come tale approccio risulti quanto mai antitetico rispetto alle odierne prassi sullo *storage* e sull'analisi dei dati, rivolte all'estrazione di nuove informazioni. Allo stesso modo, l'Enisa suggerisce lo sviluppo di *analytics* distribuite nei diversi *databases* in cui vengono raccolti i dati, di modo da estrarre valore senza però permettere la fusione dei *datasets*[925]. A questo punto, nell'ideale modello distribuito, bisognerebbe assicurare il rispetto dei principi generali del trattamento previsti all'articolo 5 GDPR. Nel momento in cui un'applicazione o un *device* viene immesso nel mercato, esso deve essere già conforme al Regolamento. Un esempio per garantire il rispetto del principio di minimizzazione attraverso la progettazione è costituito dal c.d. *edge computing*. Dotare il *device* di autonome capacità computazionali significa renderlo maggiormente indipendente dai servizi di *storage* e analisi di terzi. Ad esempio, il *device* sarà in grado di eliminare tutte le informazioni non specificatamente inerenti alle finalità del trattamento per cui sono state raccolte, di modo da inviare (ad esempio) nel *cloud* di un soggetto terzo solo i dati strettamente necessari.

Nel paragrafo 5.1 si è spiegato come alcuni problemi principali riguardanti la sicurezza siano derivati da insufficienze dell'*hardware*: batterie non capaci di sostenere le importanti misure di sicurezza e i relativi sistemi di aggiornamento richieste dai rischi realizzabili[926] (in particolare

[924] Perera C., McCormick C., Bandara A. K., Price B., A., Nuseibeh B., *Privacy-by-Design Framework for Assessing Internet of Things Applications and Platforms*, 2016, pag. 86; Giovanella F., *Le persone e le cose: la tutela dei dati personali nell'ambito dell'Internet of Things,* 2019, pag. 1237.

[925] «*Privacy preserving analytics in distributed systems are also important for the protection of personal data as they provide for computations across different databases without the need for central warehouses*», Enisa, *Privacy by design in big data An overview of privacy enhancing technologies in the era of big data analytics*, Dicembre 2015, pag. 24.

[926] Peppet S. R., 2014, *Regulating the internet of things: first steps toward managing discrimination, privacy, security and consent*, 135; più recentemente Alwarafi A., Al-Thelaya K. A., Abdallah M., Schneider J., Hamdi M., *A Survey on Security and Privacy Issues in Edge-Computing-Assisted Internet of Things*, 2021, pag. 4015.

sembra essere ancora poco implementabile la misura della cifratura[927]). Talvolta però è stato notato come le insufficienze di sicurezza fossero dovute ad un'errata implementazione delle misure di sicurezza[928]. Chiaramente, visto l'equilibrio fissato dall'articolo 1 e l'approccio *risk-based* del Regolamento, non risulta rispondente al principio di *accountability* (nello specifico aspetto della Dpbd) una simile progettazione dell'*hardware*. Un *device* che nasce inidoneo alla protezione dei dati non può sicuramente soddisfare i requisiti di sicurezza del Regolamento, neppure in caso di costi elevatissimi. Il limite dei costi può rinvenirsi allorquando la misura tecnica o organizzativa si prospetti almeno *ex ante* idonea prevenire i rischi del trattamento, e un dispositivo intelligente che sacrifichi idonee misure di sicurezza in virtù di una logica esclusivamente economica non può dirsi *GDPR-compliant*.

L'articolo 32 GDPR prevede particolari indicazioni in merito alle specifiche tutele da applicare. Ad esempio, attacchi come quelli evidenziati pac'anzi minano l'integrità e la riservatezza dei sistemi, da tutelare ai sensi dell'articolo 32 paragrafo 1, lettera b del Regolamento, secondo cui le misure di sicurezza devono avere «la capacità di assicurare su base permanente la riservatezza l'integrità la disponibilità e la resilienza dei sistemi dei servizi di trattamento». Per quanto concerne la resilienza dei sistemi, si fa riferimento a quegli incidenti temporanei che possano minare la fruizione dei servizi e il controllo dei propri dati personali.

La lettera c) del primo paragrafo prevede invece che le misure di sicurezza siano in grado di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico». Qui viene espressamente menzionato il diritto di accesso dell'interessato, che non può essere compromesso da questo o quel problema tecnico. A riguardo, risulta particolarmente problematica la questione relativa alle misure di sicurezza apposte dai responsabili del trattamento. Si pensi ai prestatori di servizi di *cloud storage*: il titolare del trattamento dovrà scegliere soltanto quelli che presentino garanzie sufficienti al rispetto del diritto di accesso dell'interessato, ed in tale valutazione saranno fondamentali le misure di sicurezza[929]. Nell'Internet delle cose il diritto di accesso rileva in particolar modo se connesso al diritto alla portabilità dei dati previsto dall'articolo 20

[927] Parere numero 8 del 16 Settembre 2014 sui recenti sviluppi nel campo dell'Internet degli oggetti (WP 223), pag.11; Giovanella F., *Le persone e le cose: la tutela dei dati personali nell'ambito dell'Internet of Things,* 2019, pag. 1224. La cifratura viene comunque ritenuta un valido strumento per garantire il principio di anonimizzazione, vedasi Weber R. H., *Internet of things: Privacy issued revisited*, Computer law & Security review, volume 31, 2015, pag. 622; Perera C., McCormick C., Bandara A. K., Price B., A., Nuseibeh B., *Privacy-by-Design Framework for Assessing Internet of Things Applications and Platforms*, 2016, pag. 86.

[928] Ci si riferiva alla vulnerabilità di alcuni tracciatori Fitbit in Peppet S. R., *Regulating the internet of things: first steps toward managing discrimination, privacy, security and consent*, 2014, pag. 134.

[929] Pizzetti F., *Intelligenza artificiale, protezione dei dati personali e regolazione* 2018, pag. 133.

GDPR. Innanzitutto, il diritto di accesso sarà utile per avere il controllo non solo sui dati forniti volontariamente al titolare del trattamento, ma anche su quelli eventualmente prodotti dalle *analytics* utilizzate. La portabilità invece risulta quanto mai rilevante per evitare il meccanismo del c.d. *lock-in*, consistente nella difficoltà di abbandonare un servizio e passare ad un altro in forza della non trasferibilità dei dati dal vecchio al nuovo titolare[930].

Proseguendo, l'articolo 25 riporta come misure atte a garantire la *data protection by design* la pseudonimizzazione e la minimizzazione (elenco non esaustivo). La norma stabilisce anche che le misure tecniche e organizzative da adottare vanno valutate in base al contesto, ai rischi del trattamento, ecc.; visto il contesto esaminato al paragrafo 5.1 andranno utilizzate tutte le misure di *data protection by design* maggiormente rigorose.

Il principio di minimizzazione è al centro del dibattito relativo alla protezione dei dati personali nell'*IoT*. Si è detto infatti come quest'ultimo si basi sul fondamentale fenomeno dei *Big Data*; il principio di minimizzazione invece richiede che siano raccolti solamente i dati strettamente necessari ai fini per cui sono stati raccolti e che siano immediatamente eliminati al termine del trattamento[931]. Tale tensione potrebbe essere parzialmente risolta mettendo in luce gli aspetti positivi di una corretta applicazione del principio in esame. In particolare, *datasets* particolarmente grandi costituiscono obiettivi più attrattivi per chi voglia condurre attacchi, mentre una raccolta minimale dei dati scoraggia tali comportamenti. Ancora, qualora l'impresa volesse mantenere i dati anche dopo il termine del trattamento, dovrebbe anonimizzarli immediatamente: questo consentirebbe un adeguato livello di protezione dei dati e non ostacolerebbe in modo eccessivo la circolazione dei dati. Nell'ordinamento europeo un simile approccio è comunque possibile alla luce dell'equilibrio fissato dall'articolo 1 del Regolamento tra circolazione e protezione dei dati; occorre dunque indagare i metodi attraverso i quali il principio di minimizzazione possa essere adottato senza recidere in modo eccessivo la circolazione dei dati.

In tal senso, autorevole dottrina ha elaborato alcune linee guida relative alla minimizzazione nell'*IoT*[932]; in particolare si consiglia di scomporre la minimizzazione in: minimizzazione delle risorse da cui si

---

[930] Giovanella F., *Le persone e le cose: la tutela dei dati personali nell'ambito dell'Internet of Things,* 2019, pag. 1232.

[931] «*…it can be argued that data minimization contravenes big data where large volumes of data are collected and stored before being used. Indeed, some of the most successful examples of big data come from digital breadcrumbs left behind by individual's use of technologies and later repurposed for analysis. It is, thus, a major challenge in big data to minimize data collection, allowing at the same time for a useful rich content that can be used for analytics*», Enisa, *Privacy by design in big data An overview of privacy enhancing technologies in the era of big data analytics*, del Dicembre 2015, pag. 22.

[932] Perera C., McCormick C., Bandara A. K., Price B., A., Nuseibeh B., *Privacy-by-Design Framework for Assessing Internet of Things Applications and Platforms*, 2016, pag. 85.

attinge per la raccolta dei dati; minimizzazione dei dati grezzi, mantenendo soltanto dati di contesto[933]; minimizzare le informazioni estratte dai dati alle sole necessarie al perseguimento degli scopi per cui sono stati raccolti i dati; minimizzare il periodo di conservazione dei dati.

Per quanto riguarda invece la pseudonimizzazione, innanzitutto, questa è da considerarsi sia come misura di sicurezza sia come misura utile ad innalzare il livello di protezione dai rischi[934]. Sebbene la misura risulti molto utile a diminuire il livello di rischio, si ritiene preferibile, anche in relazione ai rischi che il contesto dell'*Internet of Things* presenta, procedere attraverso lo strumento della anonimizzazione, che presenta un maggior livello di tutela[935]. Se al paragrafo 5.1 si è detto che ad oggi l'anonimizzazione possa considerarsi uno strumento non perfettamente efficace, va da sé che la mera misura della pseudonimizzazione non deporrà nel senso della *accountability* del titolare del trattamento[936]. Visti i rischi massimi dell'*Internet of Things* si richiederanno misure altrettanto drastiche. Dunque, secondo chi scrive, nel caso in cui si verifichi un danno ascrivibile ad una carenza della pseudonimizzazione, il titolare del trattamento potrà difficilmente dirsi *accountable*, e rischierà di essere condannato ai sensi dell'articolo 82 GDPR, per violazione dell'articolo 25 GDPR[937]. Ancora, la pseudonimizzazione sembra essere poco adatta a quelle catene di trattamenti non protratte all'interno della medesima organizzazione, volte dunque a fuoriuscire dall'impresa che ha raccolto i dati per essere condotte

[933] «*Wherever possible, IoT applications should reduce the amount of raw data acquired by the system. Raw data could lead to secondary usage and privacy violation. Therefore, IoT platforms should consider converting raw data into secondary context data. For example, IoT applications can generate orientation (e.g., sitting, standing, walking) by processing accelerometer data, storing only the results (i.e. secondary context) and discarding the raw accelerometer values*», ibidem, pag. 85.

[934] Pizzetti F., *Intelligenza artificiale, protezione dei dati personali e regolazione*, 2018, pag. 116.

[935] «In altri termini, l'associazione biunivoca tra dato e persona non è modificata in alcun modo dalla pseudonimizzazione e il dato pseudonimo, una volta impiegato in combinazione con tutti i mezzi necessari per effettuare la sostituzione di attributi a ritroso, è inequivocamente riferibile alla persona. Ciò non accade con un processo di anonimizzazione ben congegnato: sia con l'applicazione delle tecniche di distorsione, sia di generalizzazione, infatti, la riferibilità del dato anonimizzato alla persona diventa, lo si ribadisce, verosimile quanto un'attribuzione casuale», D'Acquisto G., Naldi M., *Big data e privacy by design: anonimizzazione pseudonimizzazione sicurezza*, 2017, pag. 39.

[936] «Pur scontando il fatto che, come è noto, qualunque processo di anonimizzazione non può mai dare assoluta garanzia che i dati non possano essere più ricondotti alla persona alla quale si riferiscono, non vi è dubbio che un procedimento di anonimizzazione offra una garanzia assai più elevata ai fini del rischio che il trattamento può comportare per le persone fisiche», Pizzetti F., *Intelligenza artificiale, protezione dei dati personali e regolazione*, 2018, pag. 116.

[937] Il titolare del trattamento potrebbe comunque provare a dimostrare che anche in caso di anonimizzazione adeguatamente operata, in quel caso, il danno si sarebbe prodotto ugualmente.

anche in seno ad altre organizzazioni, con ulteriori, diversi, titolari del trattamento[938].

Sebbene l'esclusione della pseudonimizzazione dalle tecniche utili a garantire la sicurezza nell'*IoT* possa sembrare una scelta estrema, incompatibile con i legittimi interessi economici sottostanti le *big data analytics*, si deve evidenziare come la anonimizzazione presenti delle sfumature utili a ricavare valore dai dati, pur comunque garantendo la sicurezza dei *datasets* più della pseudonimizzazione. Si parla in tali casi di *controlled linkability*[939], resa possibile da tecniche come la *k-anonymity* o *l-anonymity*[940], o la *differential privacy*[941].

L'anonimizzazione sarà tanto più efficace quanto più sarà anticipata: secondo l'Enisa spesso non è necessario raccogliere i dati personali, ben potendo limitarsi a raccogliere solamente dati aggregati mediante un'anomizzazione alla fonte (*local anonymization*)[942].

Proseguendo, vi sono diverse misure organizzative rilevanti da progettare in ossequio al principio di Dpbd. In particolare, si raccomanda una corretta istruzione mirata di tutti i soggetti coinvolti nel trattamento. Ad esempio, essere capaci di scrivere codici non significa necessariamente conoscere le funzioni principali della sicurezza. Motivo per cui tutti dovranno essere edotti dei principali protocolli di sicurezza scelti opportunamente dal titolare del trattamento. Ancora, il Gruppo di lavoro raccomandava che i gestori dei sensori inviassero periodiche notifiche all'interessato relative alla

---

[938] Pizzetti F., *Intelligenza artificiale, protezione dei dati personali e regolazione*, 2018, pag. 119.

[939] A proposito vedasi il documento dell'Enisa, *Privacy by design in big data An overview of privacy enhancing technologies in the era of big data analytics*, del Dicembre 2015, pag. 27: «*even if preventing linking records is one usual goal of anonymization, methods that fulfil the other two goals (preventing re-identification and attribute disclosure) while allowing some linkability are of interest in the case of big data. Indeed, big data anonymization should be compatible with linking data from several (anonymized) sources*». Disponibile online al seguente link: https://www.enisa.europa.eu/news/enisa-news/privacy-by-design-in-big-data-an-overview-of-privacy-enhancing-technologies-in-the-era-of-big-data-analytics

Sul punto anche Torra V. Navarro-Arribas G., *Big Data Privacy and Anonymization*, Springer, book series: IFIP Advances in Information and Communication Technology, 2017, pag. 20: «*if databases are anonymized in origin, we need ways to ensure that these databases can still be somehow linked in order to fulfill big data requirements. k-anonymity allows linkability at group level. Algorithms for controlled linkability are needed, as well as methods that can exploit e.g. linkability at group level*».

[940] Weber R. H., *Internet of things: Privacy issued revisited*, 2015, pag. 622.

[941] «*One of the most prominent techniques in the context of big data analysis is that of anonymization. Different privacy models and anonymization methods are in place to preserve data inference, for instance in statistical disclosure control and privacy preserving data mining techniques, including association rule mining, classification and clustering. K-anonymity and differential privacy are the two main families of privacy models with different types of implementations*», Enisa, *Privacy by design in big data An overview of privacy enhancing technologies in the era of big data analytics*, Dicembre 2015, pag. 24.

[942] Enisa, *Privacy by design in big data An overview of privacy enhancing technologies in the era of big data analytics*, Dicembre 2015, pag. 24.

raccolta dei dati, per scongiurare che questa continuasse all'oscuro del soggetto[943]. Ancora, si suggerisce la pubblicazione del codice sorgente, di modo che questo possa essere migliorato anche da soggetti terzi[944]. Nei trattamenti compositi, in cui rilevano diverse fasi del trattamento protratte in seno a diverse organizzazioni, rileveranno anche le misure di sicurezza apprestate al trasferimento dei dati da una fase all'altra del trattamento[945]. Importante sarà anche un'accurata redazione del registro dei trattamenti previsto ai sensi dell'articolo 30 GDPR[946]. Le misure ipotizzabili sono tantissime, e si è tentato fin qui di saggiare l'importanza di alcune di esse in merito ai sistemi di *IoT*.

La complessità dei trattamenti tipici dell'*IoT*, (dovuta alla presenza di sistemi di intelligenza artificiale, alla compresenza di diversi attori per diverse fasi del trattamento e alla grande capacità delle *analytics* di reidentificare dati anonimi o pseudonimi partendo da grandi *datests*), ricade su una corretta previsione dei rischi. Accede infatti che persino per i programmatori sia difficile predire come si comporteranno le macchine e a quali decisioni possano giungere. Ciò rende particolarmente complesso per il titolare del trattamento operare un'accurata definizione dei rischi derivanti dal trattamento.

Da un contesto come quello descritto al paragrafo 5.1 risulta addirittura difficile immaginare uno spazio per i rischi non prevedibili, proprio per l'ormai nota opacità dei sistemi volontariamente utilizzati. Ad esempio, si immagini il comportamento della società Alfa nel caso proposto relativo allo *smartwatch*. Alfa, conformemente al Regolamento, prima di cedere i dati raccolti si assicura di anonimizzarli. Se però risulta acclarata l'impossibilità di assicurare una perfetta anonimizzazione (per non parlare della pseudonimizzazione), ci si deve chiedere se non si debba addossare ad Alfa la responsabilità in caso di reidentificazione dei dati seguita da un danno ai relativi interessati. Va infatti ricordato come la Dpbd richieda al titolare del trattamento di adoperare misure tecniche ed organizzative valutando i rischi e il contesto in cui avviene il trattamento. In un contesto tecnologico in cui ci si spinge ad affermare la morte della protezione dei dati, o la fine del mito dell'anonimizzazione, ci si chiede se i danni derivanti dall'insufficienza di tali pratiche non vadano ricondotti all'alveo dei rischi prevedibili, con conseguente responsabilità ai sensi dell'articolo 82 GDPR del titolare del trattamento. Un'impostazione simile, tuttavia, rischierebbe di svilire il principio di *accountability*, che non richiede di *non fare*, ma di fare

[943] Parere numero 8 del 16 Settembre 2014 sui recenti sviluppi nel campo dell'Internet degli oggetti (WP 223), pag. 25.

[944] Perera C., McCormick C., Bandara A. K., Price B., A., Nuseibeh B., *Privacy-by-Design Framework for Assessing Internet of Things Applications and Platforms*, 2016, pag. 88.

[945] Pizzetti F., *Intelligenza artificiale, protezione dei dati personali e regolazione*, 2018, pag. 131.

[946] Ibidem, pag. 108.

in modo responsabile[947]. Se dunque non appare rispondente al Regolamento poter venire meno ai principi generali del trattamento in virtù della logica dei costi e dei profitti, allo stesso modo non sembra potersi ammettere di addossare qualsiasi rischio, sebbene astrattamente prevedibile, in capo al titolare del trattamento, con indubbie conseguenze sulla circolazione dei dati, espressamente protetta dall'articolo 1 del Regolamento relativo agli obiettivi dello stesso. A tal proposito risultano fondamentali gli strumenti del *data protection impact assesment* e del continuo monitoraggio delle misure applicate, di cui si dirà a breve.

Per offrire un esempio virtuoso di Dpbd e *default* nell'Internet delle cose può farsi menzione dei *personal data services* (PDS)[948]. Questi sono servizi che vengono offerti agli interessati al precipuo scopo di consentire a questi di controllare il proprio flusso di dati trai i vari *smart objects*. La IoT Databox model, ad esempio, consiste in un *device* in cui vengono installate delle applicazioni volte a rendere facilmente controllabili i dati personali prodotti all'interno di una *smart home*[949]. I pregi di tale modello sono molteplici. Innanzitutto, si tratta di un dispositivo dotato di capacità computazionali considerevoli, che gli permettono di svolgere parte del trattamento già all'interno del dispositivo[950], così da far fuoriuscire dal dispositivo solamente i dati necessari al trattamento, eliminando quelli inutili rispetto alle finalità[951], esattamente come richiedeva il Gruppo di

[947] In merito all'anonimizzazione: «un processo di anonimizzazione che si basi su tecniche (di dispersione o generalizzazione dei dati) riconosciute dalla comunità scientifica internazionale e che tenga conto degli aspetti contestuali idonei a valutare l'irragionevolezza dei mezzi è dunque, a tutti gli effetti, strumento di tutela integrato nel trattamento, così come richiesto dal principio di privacy by design introdotto dal nuovo Regolamento. Inoltre, considerata la finalità ulteriore perseguita dal processo di anonimizzazione, di impedire la re-identificazione della persona mediante l'uso di ogni mezzo ragionevole, tale finalità diventa non-incompatibile con qualsiasi finalità iniziale originalmente legittimamente perseguita dal titolare, prestandosi a promuovere un riuso dei dati ampio e trasversale, come è nella ratio del modello Big Data», D'Acquisto G., Naldi M., *Big data e privacy by design: anonimizzazione pseudonimizzazione sicurezza*, 2017, pag. 37.

[948] Queste possono essere ricondotte alle *Privacy Enhancing Technologies*.

[949] Crabtree A., Lodge T., Colley J., Greenhalgh C., Glover K., Haddadi H., Amar Y., Mortier R., Li Q., Moore J., Wang L., Yadav P., Zhao J., Brown A., Urquhart L., McAuley D., *Building accountability into the Internet of Things: the IoT Databox model*, Journal of Reliable Intelligent Environments, 2018.

[950] Dell'*edge computing* si è discusso al paragrafo 1.4.3.

[951] «*Situated at the edge of the network, the IoT Databox enables local control, which is seen as key to user empowerment. Taking computing to the data, rather than data to the computing, provides individuals with strong privacy management mechanisms. It also has potential computational advantages, decreasing latency, enhancing resilience insofar as devices only need to talk to a local box rather than a remote server, and decreasing network traffic insofar as this approach is adopted at scale, not to mention greater availability and access to data*», Crabtree A., Lodge T., Colley J., Greenhalgh C., Glover K., Haddadi H., Amar Y., Mortier R., Li Q., Moore J., Wang L., Yadav P., Zhao J., Brown A., Urquhart L., McAuley D., *Building accountability into the Internet of Things: the IoT Databox model*, 2018, pag. 51.

lavoro[952]. Le applicazioni utili al controllo dei dati personali rendono possibile in ogni momento l'accesso, la rettifica, la cancellazione, l'invio di richieste al titolare del trattamento ecc. Anche la trasparenza giova di supporto: l'informativa che viene mostrata non è infatti un mero passaggio prima di accedere ad un qualche servizio. Il servizio è la gestione dei propri dati personali: ciò fa sì che nel momento in cui si utilizza la Databox, tutta l'attenzione è rivolta alla cura dei propri dati personali, cosa rara quando invece l'informativa è vista solo come un adempimento[953].

Ancora, le applicazioni installate all'interno del dispositivo informano l'interessato su ogni aspetto della sua privacy che richieda il consenso mediante notifiche *push*, che vengono inviate per ogni nuovo trattamento. Questo consente un controllo sui propri dati che va oltre la mera accettazione di una informativa fornita *una tantum*. Si rispetta così la richiesta del Gruppo di lavoro di un consenso granulare, da fornire per ogni trattamento diverso[954]. Oltre la Databox model esistono diverse altri PDS[955]. Nel momento in cui diverranno diffuse, dovranno ritenersi essenziali ai fini della valutazione dell'*accountability* del titolare del trattamento: nel momento in cui il mercato offrirà un adeguato livello di scelta tra i vari PDS, l'aver fornito o meno un sistema di controllo dei propri dati di tal fatta potrà essere dirimente nel chiarire se il titolare del trattamento ha effettivamente consentito il controllo dei dati personali all'interessato o meno.

La citata problematica relativa all'opportunità di imporre i principi di Dpbd e *default* agli sviluppatori risulta particolarmente rilevante allorquando si faccia riferimento agli strumenti di analisi dei dati basati

[952] «Molti portatori di interessi dell'IoT hanno bisogno solo di dati aggregati e non hanno alcun bisogno dei dati grezzi raccolti dai dispositivi IoT. I portatori di interessi devono cancellare i dati grezzi non appena hanno estratto i dati necessari per il loro trattamento. In linea di principio, la cancellazione deve avere luogo nel punto di raccolta dei dati grezzi più vicino (ad esempio sullo stesso dispositivo, dopo il trattamento)», parere numero 8 del 16 Settembre 2014 sui recenti sviluppi nel campo dell'Internet degli oggetti (WP 223), pag. 24

[953] Si è già fatto riferimento al fatto che quando il consenso è richiesto per accedere ad un servizio, esso viene prestato per via di euristiche ed altre scorciatoie cognitive. Si rimanda a Caggiano I. A., *Il consenso al trattamento dei dati personali nel nuovo Regolamento europeo. Analisi giuridica e studi comportamentali*, 2018.

[954] «I fabbricanti di dispositivi devono fornire un consenso granulare nel concedere l'accesso alle applicazioni. La granularità non deve riguardare solo la categoria dei dati raccolti, ma anche il momento e la frequenza con la quale i dati vengono rilevati. Analogamente alla funzione "non disturbare" degli smartphone, i dispositivi per l'IoT dovrebbero prevedere un'opzione "non raccogliere" ("do not collect") per programmare o disattivare velocemente i sensori», parere numero 8 del 16 Settembre 2014 sui recenti sviluppi nel campo dell'Internet degli oggetti (WP 223), pag. 24.

[955] Si veda ad esempio la applicazione MyData. Visionabile al seguente link: https://www.mydata.org/

Oppure la piattaforma DISPEL. Visionabile al seguente link: https://legal.dispel.io/

Su quest'ultima, si rimanda a Stach C., Gritti C., Mitschang B., *Bringing Privacy Control Back to Citizens*, Proceedings of the 35th Annual ACM Symposium on Applied Computing, Marzo 2020.

sull'IA[956]. Applicare i suddetti principi agli algoritmi è fondamentale, proprio per evitare che si concretizzino i rischi derivanti dai *software* intelligenti di cui si è discusso, discriminazioni *in primis*. Anche qui, però, si rinviene la problematica relativa alla *black-box*. Quand'anche un titolare del trattamento volesse valutare se i sistemi di IA forniti dal responsabile del trattamento (si è detto della IAaaS) siano effettivamente *privacy-compliant*, questi non potrebbe superare la barriera legittimamente innalzabile del segreto industriale. In questo caso, infatti, non essendosi ancora verificata alcuna violazione della sfera privata di un qualche individuo, risulta improbabile che si opti per la prevalenza della protezione dei dati personali (in quel momento ancora intaccati) rispetto alla tutela degli interessi economici protetti dal segreto. Dunque, l'unico strumento utile al titolare del trattamento potrebbe essere una garanzia contrattuale di conformità, ma ciò non rileverebbe ai sensi della sua *accountability*: rimarrebbe dunque responsabile ai sensi dell'articolo 82 GDPR[957].

È da ricercare altrove dunque lo strumento attraverso cui il titolare può scegliere più coscientemente tali sistemi in modo da risultare *accountable*. Uno di questi potrebbe essere la certificazione, richiamata espressamente dall'articolo 25 GDPR[958]. Qualora infatti, in sede di condanna al risarcimento del danno del titolare del trattamento per *culpa in eligendo* di un responsabile che non abbia fornito un sistema di IA adeguato, si chieda al titolare del trattamento perché ha scelto un fornitore di servizi IA privo di certificazione a fronte di altri certificati, sarebbe difficile sostenere l'esistenza della diligenza adeguata (nella specie si violerebbe l'articolo 28 paragrafo 1 nella parte in cui statuisce che il titolare del trattamento «quest'ultimo ricorre 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»). Un altro elemento in grado di giovare al titolare del trattamento in termini di *accountability* sono i codici di condotta.

Nel caso in cui invece l'algoritmo di IA sia proprietario, l'Edpb raccomanda che vada progettato, in tutti i suoi *layers*, in modo conforme al

[956] «Si segnala, peraltro, come il sovrapporsi di ruoli e competenze di molteplici attori diversi, inseriti lungo la catena in cui si articolano i processi di ideazione e sviluppo e quelli successivi di diffusione e utilizzo delle complesse e variegate forme di IA, manifesti l'esigenza di incentivarli tutti a minimizzare i rischi prima che ad affrontare l'eventuale impatto negativo della loro attività», Gambini M., *Algoritmi e sicurezza,* Giurisprudenza italiana, Luglio 2019, pag. 1738.

[957] Bincoletto G., *Data Protection by Design in the E-Health Care Sector: theoretical and applied perspectives*, Nomos Verlagsgesellschaft, 2021, pag. 108.

[958] «*Certification will add trustworthiness to IoT applications*», Perera C., McCormick C., Bandara A. K., Price B., A., Nuseibeh B., *Privacy-by-Design Framework for Assessing Internet of Things Applications and Platforms*, 2016, pag. 88.

Regolamento[959]. A tal proposito, nella risoluzione del Parlamento europeo sulle norme civili relative alla robotica si è raccomandato che «il progettista dovrebbe introdurre funzionalità di "privacy by design" (tutela della vita privata fin dalla progettazione), in modo da garantire la sicurezza delle informazioni private e assicurare che queste ultime siano utilizzate soltanto in modo appropriato»[960].

Sempre in merito ai sistemi di IA, da segnalarsi la questione valoriale[961]. Si è detto in precedenza come i *bias*, e quindi le discriminazioni possano discendere da improvvide inclusioni valoriali specifiche da parte del progettatore (ad esempio, tutti gli uomini sono più indicati per i lavori fisici rispetto a tutte le donne)[962]. Dunque, si pone il tema di un corretto sviluppo valoriale dell'algoritmo. Sul tema sono stati diramati gli orientamenti etici posti alla base dei lavori dell'Unione sulla IA, ed in questi si è sottolineata la direzione antropocentrica che va impressa in tali sistemi[963]. Ciò nasce dalla presa di coscienza della fallibilità di tali macchine, che necessitano dunque di una guida umana, sempre pronta a correggere le storture del codice[964].

---

[959] Nelle linee guida 4/2019 sull'articolo 25 e la protezione dei dati fin dalla progettazione e per impostazione predefinita, l'Edpb prevede specifici indirizzi di implementazione in merito ai singoli principi del trattamento previsti dall'articolo 5 GDPR.

[960] Norme di diritto civile sulla robotica. Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica (2015/2103(INL). Disponibile online al seguente link:

https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_IT.html

[961] Il tema etico delle macchine ha radici profonde. D'obbligo menzionare gli scritti di Isaac Asimov. In particolare, nella raccolta *Robot visions* del 1990 si asseriva l'impossibilità di errore delle macchine nel caso in cui fossero state progettate adeguatamente. Oggi, le capacità delle machine hanno di gran lunga superato la prevedibilità in merito alle loro azioni, superando così gli assunti del celebre scrittore.

[962] «*Values are involved at various stages when training ML. First, the designer determines (with the controller's ADM purposes in mind) the data feed that is used to train the ML. They decide which data/what type of data is used, and which data is left out. A designer's decisions about the data feed inherently involve choices (and values). As these choices have to be made, there may be bias, and potentially unfairness and discrimination, in data input, output and decisions. The use of historical data is another potential source of human bias and discrimination.47 Equally important are values involved in the determination of the weightings of input data in the statistical model, to achieve the desired outcome. Potential failures should be identified and dealt with by the algorithm designer, through dry runs of the system in experimental, but secured settings, away from the public*», Jannsen H., *An approach for a fundamental rights impact assessment to automated decision-making*, International Data Privacy Law, volume 10, numero 1, 2020, pag. 13.

[963] Orientamenti etici sull'intelligenza artificiale: proseguono i lavori della Commissione. Comunicato stampa del 8 Aprile 2019. Disponibile online al seguente link:

https://ec.europa.eu/commission/presscorner/detail/it/IP_19_1893

[964] «Una strada da battere non solo per motivi giuridici ma anche per assicurare una tutela reale, anche fisica, delle persone, sarà quella di accompagnare l'uso di queste macchine con istruzioni e modalità che, come richiede nella sua, solo apparente ingenua semplicità, l'articolo 22 GDPR, consentano sempre l'intervento umano. Non vi è dubbio, infatti, che sarebbe assolutamente irresponsabile, prima di tutto sul piano etico e poi anche su quello della responsabilità civile, consentire e mettere in circolazione robot o forme di IoT che gli uomini non fossero in alcun modo in grado di controllare e, al limite, disattivare

In merito ai rischi di discriminazione si è fatta luce sui valori di tolleranza ed apertura fatti propri dalla Corte europea dei diritti dell'uomo[965]; gli algoritmi andranno intrisi di tali principi, e, al mutare degli stessi, dovrà intervenire la mano dell'uomo, pronto a rendere l'algoritmo al servizio dell'essere umano e non il contrario[966].

Sul punto, la proposta di regolamento sull'IA, all'articolo 10 paragrafo 3, non sembra però essere particolarmente innovativa, stabilendo semplicemente che «i set di dati di addestramento, convalida e prova devono essere pertinenti, rappresentativi, esenti da errori e completi. Essi possiedono le proprietà statistiche appropriate, anche, ove applicabile, per quanto riguarda le persone o gruppi di persone sui quali il sistema di IA ad alto rischio è destinato a essere usato»[967].

La questione dei valori algoritmici non sembra dunque aver fatto ancora breccia.

Quanto detto finora sulla Dpbd va rapportato agli obblighi descritti nei precedenti paragrafi. Tutti quei sistemi, ad esempio le notifiche *push*, o la dotazione di monitor che permettano quanto meno la lettura dell'informativa, oppure ancora una preventiva informazione (accessibile in ogni momento dallo *smart object*) sulla logica utilizzata dall'algoritmo, devono essere previste già in un momento anteriore all'effettivo trattamento. Tra i principi maestri della privacy by designva infatti sempre rammentato il «*proactive not reactive; preventative not remedial*»[968]. Nello stesso senso si pone la proposta di regolamento sull'IA, quando all'articolo 13 stabilisce che «i sistemi di IA ad alto rischio sono progettati e sviluppati in modo tale da garantire che il loro funzionamento sia sufficientemente trasparente da consentire agli utenti di interpretare l'output del sistema e utilizzarlo adeguatamente».

Visioni futuristiche relative al rapporto tra macchine intelligenti e Dpbd, pongono l'accento sulla questione relativa alla possibilità di

anche contro la volontà della macchina e superando ogni sua possibile resistenza», Pizzetti F., *Intelligenza artificiale, protezione dei dati personali e regolazione*, 2018, pag. 126.

[965] Si fa riferimento al principio di precauzione in Pizzetti F., *Intelligenza artificiale, protezione dei dati personali e regolazione*, 2018, pag. 127.

[966] In diverse opere è stato affrontato il tema della prevalenza nel rapporto uomo-macchina. A proposito vedasi Cave S., Dihal K., Dillon S., *AI Narratives: A History of Imaginative Thinking about Intelligent Machines*, Oxford University Press, 5 Marzo 2020; Kim T.W., Maimone F., Pattit K., Sison A. J., Teehankee B., *Master and Slave: the Dialectic of Human-Artificial Intelligence Engagement*, Humanist Management Journal, 3 Dicembre 2021; Edwards L., Veale M., *Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking for*, Duke Law & Technology Review, 2017.

[967] Sul punto Contaldi G., *Intelligenza artificiale e dati personali*, 2021, pag. 1208-1209.

[968] Si fa riferimento all'opera maestra sulla *privacy by design*: Cavoukian A., *Privacy by Design*, Information & Privacy Commissioner, 2009.

addestrare tali macchine ad applicare autonomamente i principi di Dpbd e *default*[969].

Della minimizzazione si è già detto al paragrafo 5.3.2, e questa risulta particolarmente importante se rapportata alla progettazione degli algoritmi. Ad oggi questi vengono elaborati al precipuo scopo di ottenere «dati dai dati»[970], e il che non risulterebbe in linea con il principio di minimizzazione. Altrettanto deve dirsi per le fasi di addestramento degli algoritmi: maggiori dati (qualitativamente corretti) questi algoritmi avranno, e meglio funzioneranno. Anche qualora venissero utilizzati solo dati anonimi, bisognerà tenere a mente che le capacità inferenziali odierne renderebbero presumibile un'identificazione degli interessati. Anche da questo punto di vista, dunque, il principio di minimizzazione si pone in contrasto rispetto alle *business practices* più diffuse e andrà modulato secondo le più moderne *best practices*.

Quanto fin qui detto viene concluso con il principio di *data protection by default*, per mezzo del quale tutte le regole sin qui esposte vanno impostate come regole di *default* del dispositivo *smart*. Tale paradigma risulta particolarmente importante nei sistemi di *IoT*, in cui la particolare complessità renderebbe ardua l'autodeterminazione informativa dell'interessato[971].

A. Il *data protection impact assessment*

Ai sensi dell'articolo 35 del Regolamento, obbligo fondamentale del titolare del trattamento è la redazione di una valutazione d'impatto sulla protezione dei dati personali (DPIA). Questa rappresenta uno degli obblighi in cui è più evidente l'approccio *risk-based* del Regolamento e un cardine del principio di *accountability*[972]. Requisito ed elemento vincolante per una DPIA è l'elevato rischio per i diritti e le libertà delle persone fisiche. Il terzo paragrafo dell'articolo 35 GDPR esemplifica tre casi in cui si rende necessaria una DPIA:

> «a) 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; b) 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; o c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico».

---

[969] Pizzetti F., *Intelligenza artificiale, protezione dei dati personali e regolazione*, 2018, pag. 124.

[970] Ibidem.

[971] Giovanella F., *Le persone e le cose: la tutela dei dati personali nell'ambito dell'Internet of Things,* 2019, pag. 1237.

[972] Se ne è discusso al paragrafo 3.4.

Tali scenari sono facilmente ascrivibili (anche) all'ambito dell'*Internet of Things*; non a caso, nel relativo parere, il Gruppo di lavoro invitava ad effettuare DPIA per ogni lancio di nuove applicazioni per *smart objects*[973]. In merito alla prima ipotesi indicata dal citato articolo 35 paragrafo 3 GDPR si pensi alla profilazione operata su Tizio al momento della richiesta di accesso al finanziamento. Il secondo e il terzo caso potrebbero invece essere entrambi ricondotti nell'esempio del caso R. (Bridges)[974].

Della questione si è occupato il Gruppo di lavoro nelle apposite linee guida, in cui si specifica che tale elenco non è certo esaustivo, e che possono ravvisarvi diverse fattispecie risultanti in rischi elevati per i diritti e le libertà delle persone fisiche[975]. A tal proposito, di modo da riconoscere casi di rischio elevato, il Gruppo di lavoro ha elencato alcuni criteri utili: si fa riferimento alla valutazione o assegnazione di un punteggio; ad un processo decisionale automatizzato; ad un monitoraggio sistematico; al trattamento di dati particolari; a trattamenti su larga scala; creazioni di corrispondenze o combinazione di insiemi di dati; dati relativi ad interessati vulnerabili (minori, infermi di mente, richiedenti asilo ecc.); uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative; quando il trattamento in sé impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto. In questi casi è probabile che si abbia un rischio elevato ed è caldamente consigliata la predisposizione della valutazione d'impatto.

Ragionando su quanto detto sull'*Internet of Things* e sulla sua deriva nel capitalismo della sorveglianza, è possibile ricondurre ad esso diversi riferimenti tra quelli elencati dal Gruppo di lavoro: il monitoraggio sistematico, i trattamenti su larga scala, la combinazione di diversi dati, soluzioni tecnologiche innovative ecc.[976].

---

[973] Parere numero 8 del 16 Settembre 2014 sui recenti sviluppi nel campo dell'Internet degli oggetti (WP 223), pag. 24.

[974] Se ne è parlato al paragrafo 2.5: in questo caso la polizia del Galles aveva installato sulle sue vetture dei sistemi di riconoscimento facciale automatico, volti a riconoscere tra i passanti di strade accessibili al pubblico i lineamenti del viso dei soggetti ricercati. Dunque, è possibile ravvisare sia il trattamento su larga scala di dati particolari, sia il trattamento di informazioni relative a condanne penali e reati. A ciò si aggiunge il fattore della sorveglianza sistematica su larga scala di zone accessibili al pubblico.

[975] Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" del 7 Aprile 2017 e modificate in data 4 Ottobre 2017 (WP 248), pag. 9. Disponibili online al seguente link:

https://www.garanteprivacy.it/Regolamentoue/DPIA

[976] «Ad esempio, alcune applicazioni di "Internet delle cose" potrebbero avere un impatto significativo sulla vita quotidiana e sulla vita privata delle persone e, di conseguenza, richiedono la realizzazione di una valutazione d'impatto sulla protezione dei dati», linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" del 7 Aprile 2017 e modificate in data 4 Ottobre 2017 (WP 248).

Da ciò, chi scrive ritiene che la DPIA, nell'ambito dell'Internet delle cose, debba essere considerato un adempimento sistematico, sia al momento della predisposizione dei mezzi e delle finalità, sia durante tutto il ciclo del trattamento. Così come il titolare del trattamento deve informare gli interessati ai sensi dell'articolo 13 e 14 GDPR, dovrà fornire loro la valutazione d'impatto *ex* articolo 35, senza indugio. Essa è anche strumento utile a garantire la trasparenza all'interno del trattamento, in quanto rende edotto l'interessato su uno degli elementi fondamentali del trattamento: i rischi. In merito alla descrizione di essi il Gruppo di lavoro si limita a fornire degli schemi esemplificativi, ma il modello e le modalità rimangono libere.

Nell'ambito dei procedimenti automatizzati la DPIA assolve alla duplice funzione mezzo utile a garantire la trasparenza e strumento di esplicazione dei rischi previsti.

Il caso del *credit scoring* sin qui analizzato rientra tra i trattamenti ad alto rischio[977], che dunque, ai sensi dell'articolo 35 GDPR, richiedono la redazione di una valutazione d'impatto.

Commentatori hanno specificato che in relazione ai trattamenti automatizzati la valutazione dovrebbe indicare sia i rischi che derivanti dall'algoritmo così come progettato, sia quelli derivanti dal suo funzionamento effettivo (si sono già menzionati i *bias* emergenti in momenti successivi alla programmazione); andrebbe indicato anche che tipo di controllo gli interessati riescono a mantenere durante il procedimento e quindi nel lasso di tempo in cui tali dati vengono elaborati ed incrociati con altri[978].

Nella valutazione, il titolare di un trattamento operato nell'*IoT* dovrà indicare anche i rischi di discriminazione potenzialmente derivabili, un'influenza sull'autodeterminazione commerciale, rischi alla salute ecc.; una valutazione dell'impatto di questi rischi sui diritti e le libertà, così come la logica utilizzata dall'algoritmo e le relative misure adottate per mitigarne i rischi[979].

Quanto detto finora riguarda il *design* della valutazione d'impatto al momento iniziale del trattamento[980]. Tuttavia, un aspetto molto importante

---

[977] Un esplicito riferimento si ritrova nelle linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" del Edpb. Disponibili online al seguente link:
https://www.garanteprivacy.it/Regolamentoue/DPIA

[978] Jannsen H., *An approach for a fundamental rights impact assessment to automated decision-making*, 2020, pag. 11.

[979] Hamon R., Junklewitz H., Sanchez I., Malgieri G., De Hert P., *Bridginh the Gap Between AI and Explainability in the GDPR: Towards Trustworthiness-by-Design in Automated Decision-Making*, IEEE computational intelligence magazine, Febbraio 2022, pag.83.

[980] «La valutazione d'impatto sulla protezione dei dati va effettuata "prima del trattamento" (articolo 35, paragrafi 1 e 10, considerando 90 e 93). Ciò è coerente con i principi di protezione dei dati fin dalla progettazione e di protezione per impostazione predefinita (articolo 25 e considerando 78)», linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa

dell'*accountability* è il continuo monitoraggio delle misure preposte a salvaguardia dei diritti e delle libertà dell'interessato, così come anche degli strumenti automatizzati utilizzati nel trattamento. A seguito di *audit* (di cui nel prossimo paragrafo) potrebbero rinvenirsi fattori che rendano doverosa una correzione della DPIA; si pensi ai già menzionati *bias* emergenti, o magari a recenti botnet diffuse in quel momento che possano intaccare i sistemi di sicurezza[981].

Nella DPIA andrebbero indicate anche le argomentazioni relative alle opinioni eventualmente espresse dagli interessati e dai loro rappresentanti ai sensi dell'articolo 35 paragrafo 9 GDPR.

Tra le *best practices*, si indica anche la consultazione di esperti informatici, di sicurezza, sociologi, di etica ecc.[982], a conferma dei diversi tipi di impatto che trattamenti ad alto rischio possono causare.

B. Il monitoraggio

Sebbene un adeguato rispetto dei principi di *data protection by design* e *by default* costituisca un ottimo punto di partenza, esso non potrebbe considerarsi punto di arrivo. È infatti richiesto il continuo monitoraggio delle misure preposte alla salvaguardia dei diritti e delle libertà dell'interessato, in quanto il mutare del contesto tecnologico o normativo potrebbe far venire meno l'adeguato *standard* di protezione fissato al momento della raccolta dei dati. Ad esempio, qualora anche un titolare del trattamento avesse predisposto un'architettura ed un sistema di monitoraggio soddisfacente, l'avvento del (futuro) regolamento sulla IA potrebbe cambiare le regole del gioco, e ciò richiederebbe una nuova analisi *by design*.

Quanto detto risulta particolarmente importante nell'ambito dei trattamenti protratti con l'ausilio di procedimenti automatizzati, specialmente se assistiti da algoritmi di *machine learning*. Al momento della progettazione delle formule e dei criteri che il *software* di calcolo deve seguire per arrivare alla decisione potrebbe verificarsi l'assenza di *bias* suscettibili di cagionare trattamenti discriminatori; tuttavia, visto l'elevato grado di autonomia di tali macchine, e il relativo livello di comprensibilità dei loro meccanismi (ancor di più qualora non siano di proprietà del titolare del trattamento), si raccomanda fortemente l'implementazione di un sistema di

presentare un rischio elevato" del 7 Aprile 2017 e modificate in data 4 Ottobre 2017 (WP 248).

[981] «L'aggiornamento della valutazione d'impatto sulla protezione dei dati nel corso dell'intero ciclo di vita del progetto garantirà che la protezione dei dati e della vita privata sia presa in considerazione e favorisca la creazione di soluzioni che promuovono la conformità. Può essere altresì necessario ripetere singole fasi della valutazione man mano che il processo di sviluppo evolve, dato che la selezione di determinate misure tecniche od organizzative può influenzare la gravità o la probabilità dei rischi posti dal trattamento», Ibidem, pag. 17.

[982] Ibidem, pag. 18.

attività di ispezioni regolari volte a verificare che l'algoritmo non abbia sviluppato nuovi *bias*[983]*.* Questi, infatti, possono ben svilupparsi anche dopo lassi di tempo relativamente elevati, visto che le inferenze mutano man mano che il sistema analizza più dati. Nello stesso senso sembrerebbe essere orientato il considerando numero 71, nella parte in cui stabilisce che

> «è opportuno che il titolare del trattamento utilizzi procedure matematiche o statistiche appropriate per la profilazione, metta in atto misure tecniche e organizzative adeguate al fine di garantire, in particolare, che siano rettificati i fattori che comportano inesattezze dei dati e sia minimizzato il rischio di errori e al fine di garantire la sicurezza dei dati personali secondo una modalità che tenga conto dei potenziali rischi esistenti per gli interessi e i diritti dell'interessato e impedisca, tra l'altro, effetti discriminatori nei confronti di persone fisiche sulla base della razza o dell'origine etnica, delle opinioni politiche, della religione o delle convinzioni personali, dell'appartenenza sindacale, dello status genetico, dello stato di salute o dell'orientamento sessuale, ovvero un trattamento che comporti misure aventi tali effetti..»

Allo stesso modo dovrebbero verificarsi i sistemi di sicurezza apprestati nell'ottica di difendere l'integrità dei dati da attacchi esterni.

Tali controlli dovrebbero costituire un dovere da estendersi in tutti gli anelli che compongono la catena dei trattamenti nell'*Internet of Things*, rivolto al programmatore, al soggetto che offre il servizio di analisi e a chi ne beneficia[984]. Un modello di controllo siffatto è già consolidato in settori diversi da quello del trattamento dei dati personali, in particolare in quello della prestazione di servizi della società dell'informazione[985].

Concordi in tale orientamento anche le linee guida del Gruppo di lavoro relative ai procedimenti automatizzati, che nell'esemplificare significative *best practices* fanno riferimento a controlli regolari relativi alla qualità dei sistemi, alla verifica degli algoritmi; si suggerisce anche di sfruttare verifiche da parte di terzi[986]. Nei paragrafi precedenti si sono espresse perplessità relative alla possibilità di essere davvero *accountable* quando il *software* di cui si beneficia non è proprietario. Le succitate linee guida, a tal proposito, compiono un significato passo, consigliando al titolare del trattamento di farsi rilasciare garanzie contrattuali relative all'espletamento di ispezioni concernenti gli algoritmi e i sistemi. Si è detto nel paragrafo 4.2.1 come il soggetto generalmente responsabile ai sensi dell'articolo 82 del GDPR sia però soltanto il titolare del trattamento; dunque, a nulla varrebbe un contratto con cui si *muove* la responsabilità di questi a chi mette a disposizione il proprio *software* (nella maggior parte dei

[983] Malgieri G., Comandè G., *Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation*, 2017, pag. 10.

[984] Gambini M., *Algoritmi e sicurezza,* 2019, pag. 1738.

[985] Ibidem, pag. 1737.

[986] Sul punto Wachter S., Mittlestadt B., Floridi L., *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, 2017, pag. 98.

casi questi sarà classificabile come responsabile del trattamento). Per ovviare a tale problema le linee guida individuano lo strumento delle garanzie contrattuali, volte dunque non a sollevare il titolare del trattamento dalle sue responsabilità, ma a garantirlo rispetto alle conseguenze nefaste di un trattamento illecito.

Nello stesso senso anche la relazione alla proposta di regolamento dell'IA, secondo cui «una valutazione completa della conformità ex ante attraverso controlli interni, combinata con una forte applicazione ex post, potrebbe costituire una soluzione efficace e ragionevole per tali sistemi, considerato che l'intervento normativo è in fase iniziale e che il settore dell'IA è molto innovativo e soltanto ora si stanno maturando le competenze di audit»[987].

5.4 Conseguenze dell'*Internet of Things* sul rapporto tra il principio di *Accountability* e il regime di responsabilità

Alla luce di quanto detto nei paragrafi precedenti, appare chiara la difficoltà nell'applicare pienamente il sistema di diligenza costruito attraverso il principio di *accountability* nel contesto dell'*IoT*. I problemi riconducibili a tali ambienti sono da attribuire alla molteplicità di attori del trattamento e al fatto che i vari processi, seppur singolarmente leciti, se concatenati, sono in grado di cagionare nocumento altri individui. Il principio di *accountability* impone al titolare del trattamento di valutare i rischi del suo trattamento: il problema risiede nel fatto che sebbene il suo trattamento possa essere lecito e non particolarmente rischioso, esso potrebbe costituire la base di un ulteriore trattamento operato da altri soggetti, meno lecito e più rischioso, e così via.

I modelli di attività che fanno dei dati personali prodotti attraverso l'*Internet of Things* la propria linfa si basano essenzialmente sulla possibilità di trattare e scambiare quei dati. Sebbene sia riconosciuto che il Regolamento nasca dalla presa di coscienza di una circolazione dei dati non più bidirezionale (interessato – titolare del trattamento) si può affermare che risulti particolarmente complesso applicare pienamente gli istituti posti a presidio della tutela dei dati personali in questo ambito.

Talvolta, i danni sono prodotti da macchinari talmente complessi da sfuggire al controllo del titolare del trattamento, oppure derivano da trattamenti perfettamente leciti operati da titolari precedenti.

In questi casi, risulta difficile da immaginare una responsabilità per fatto altrui, in quanto non c'è neppure un legame tra i vari attori: si immagini che Tizio produca e venda braccialetti per il *fitness* e che una volta generati, i dati vengono immagazzinati sul *cloud* di Caio, che dopo averli anonimizzati,

[987] Relazione introduttiva alla proposta, pagina 15.

li rende disponibili a Sempronio. Non c'è alcuna relazione tra Tizio e Sempronio, né di natura commerciale né di altro tipo, ed è probabile che il primo non sappia neppure che i dati da lui generati siano adesso trattati (seppur in forma anonima) da Sempronio. L'eventuale danno cagionato da Sempronio non può certo ascriversi a Tizio, eppure senza il trattamento di questi non sarebbe stato possibile. Le problematicità derivano dal fatto che quanto appena detto non costituisce una eccezione rispetto alla regola, ma la regola stessa. I dati circolano (in modo più o meno lecito) e sono destinati ad essere elaborati, scambiati, e rielaborati e scambiati nuovamente da molti soggetti diversi.

Se dopo la rivoluzione industriale un problema era costituito dal frazionamento della colpa, oggi è il contrario. Si sente la necessità di attribuire la responsabilità e gli obblighi di responsabilizzazione ad una moltitudine di soggetti diversi, che proprio in virtù dell'accentramento della responsabilità, non rispondono ai sensi dell'articolo 82 GDPR e non sono tenuti a tutti gli obblighi imposti al titolare del trattamento; possono tuttavia rispondere in altro modo, ma sul punto c'è molta incertezza vista l'assenza di norme specifiche sulla responsabilità civile delle macchine intelligenti. Oggi la discussione sulla colpa e sulla oggettività mantiene certamente una sua rilevanza[988], tuttavia non è qui che si ricercano risposte.

Se negli anni sessanta del secolo scorso le mancanze di tutela erano state individuate nel criterio d'imputazione della colpa, a nulla varrebbe riproporre oggi le medesime perplessità. La responsabilità oggettiva, infatti, si basa sempre su una relazione tra il soggetto responsabile e la cosa o l'essere vivente che ha cagionato il danno, relazione che spesso, negli ambienti tipici dell'*IoT*, non sussiste. La mancanza di una relazione tra Tizio e Sempronio renderebbe inapplicabile il principio di causalità pura. Se dopo la rivoluzione industriale si pensava di poter porre rimedio attraverso la responsabilità oggettiva, oggi si ricerca nuovi istituti di protezione, capaci di esaltare la complessità dei trattamenti e la dimensione collettiva della privacy

Ancora, alcune norme, come quella sulla profilazione solo individuale, non permettono un'adeguata tutela di interessi diffusi nei gruppi sociali, e ciò costituisce un serio problema di *accountability*, in quanto i titolari del trattamento ben potrebbero impattare sulla vita degli interessati senza poter essere chiamati a rispondere.

La tutela civile e la previsione dei rischi non possono dirsi efficaci in questi *smart environments* se non si prende in considerazione cosa accadrà una volta inseriti i dati all'interno di un circuito globale. Il principio di *accountability* invece richiede che vengano presi in considerazione solo i rischi derivanti dal proprio trattamento; finché dunque questo rimane lecito, il titolare del trattamento sarà sollevato da qualsiasi altra conseguenza.

[988] Si pensi a quell'orientamento giurisprudenziale secondo cui se le misure fossero state idonee allora il danno non si sarebbe verificato.

Il principio di *accountability* doveva costituire la chiave di volta della protezione dei dati personali nell'odierno modello di circolazione dei dati. Tuttavia, sebbene possa essere considerato soddisfacente dal punto di vista della responsabilizzazione, in quanto importa una serie di obblighi puntuali e procedure volte ad impegnare il titolare del trattamento a mitigare i rischi derivanti dal trattamento, rischia di divenire inefficace sotto il profilo della protezione. Come detto infatti, essere *accountable* risulta già particolarmente complesso nell'ambito dell'*Internet of Things*, e anche qualora lo si fosse, da una concatenazione di trattamenti *accountable* ben potrebbero derivare pregiudizi molto rilevanti, non tutelabili mediante l'articolo 82 del GDPR.

Conclusioni

Nel corso della presente tesi sono stati indagati i temi dell'*Internet of Things*, del principio di *accountability* e della responsabilità da trattamento illecito di dati personali. L'analisi è stata svolta considerando singolarmente gli specifici argomenti, per poi valutarli congiuntamente nell'ultimo capitolo.

Si è scelto di discutere il fenomeno dell'*Internet of Things* in quanto questo, secondo chi scrive, presenta problematiche inerenti alla privacy ancora non pienamente esplorate. Ad oggi, la comunità degli utenti dell'Internet si dimostra maggiormente prona ai rischi alla privacy derivanti dai *social networks* e dai motori di ricerca. L'*Internet o Things* si presenta però sotto una nuova veste: un orologio, una suola delle scarpe, una telecamera apprestata per sorvegliare l'ingresso della proprietà, gli occhiali da sole. Questi sono tutti oggetti molto conosciuti, diffusi, e capaci di ingenerare un senso di familiarità nella comunità. Nel momento in cui però anche questi oggetti diventano *smart*, quindi in grado di trarre informazioni anche molto importanti sugli individui, ecco che potrebbero generarsi nuove violazioni alla privacy. La familiarità che questi oggetti diffusissimi riescono a veicolare potrebbe essere il grande problema rappresentato da tali *devices*. Mentre gli *smartphones* e i computer nascono con il riconosciuto l'obiettivo di connettere la persona ad Internet, un orologio o un occhiale da sole, sebbene *smart*, potrebbero non ingenerare la stessa sensazione. Se ci si è accorti di come i microfoni degli smartphones siano attivi anche quando non azionati dalle persone, non altrimenti potrebbe dirsi dei microfoni già presenti negli *smartwatches*. Da tale senso di familiarità potrebbe derivarsi una minor cautela nell'utilizzo di tali apparecchi. Gli *smart objects* stanno divenendo sempre più diffusi, così come stanno aumentando anche i fornitori di tali *devices*. Tuttavia, questi mercati sono caratterizzati da un grande accentramento, dovuto ai consistenti costi fissi da sostenere per le infrastrutture *software* e *hardware* utili allo storage e all'analisi dei dati. Questo porterà in nuovi players ad affidarsi sempre più alle celebri *big-tech companies*, come Google, Facebook, Amazon ecc. Tali compagnie sono state messe sotto la lente d'ingrandimento di illuminante letteratura sociologica, conosciuta mediante l'espressione "capitalismo della sorveglianza", che ha dimostrato come tali compagnie si siano spesso rese attrici di profonde e persistente violazioni della privacy. Questi elementi hanno condotto chi scrive a concentrarsi sul tema del trattamento dei dati personali generati attraverso gli *smart objects*.

Il primo capitolo è stato dedicato all'evoluzione delle tecnologie che supportano l'*Internet of Things*. Oggigiorno spiccano il *cloud computing* e le modernissime tecniche di *edge* e *fog computing*, che hanno ampliato il novero dei luoghi ove può avvenire il trattamento, e di conseguenza il

numero degli attori dello stesso. La tecnologia di *edge computing* è quella che conferisce all'individuo il maggiore controllo sui dati in quanto il trattamento, in tutto o in parte, avviene all'interno del dispositivo o nel nodo più vicino allo stesso, limitando così l'intervento di terzi. Il *cloud computing* invece fa sì che i dati generati dai *devices* finiscano per essere immagazzinati in *spazi* di proprietà di terzi, ed analizzati anche da ulteriori altri soggetti. Il *fog computing* rappresenta invece una posizione intermedia, in quanto i nodi in cui avviene parte del trattamento potrebbero essere di proprietà dell'interessato, come di soggetti terzi, quali i proprietari degli *hotspot*. L'aumento dei *luoghi* in cui avviene il trattamento dei dati personali ha fatto si che si moltiplicassero anche gli attori coinvolti nello stesso. Un'altra conseguenza è anche l'aumento degli *spazi* attaccabili da possibili *hackers*. Sebbene l'*edge computing* si presenti come l'opzione più rispondente ad esigenze di tutela dei dati personali, è stato segnalato come i *devices*, in virtù delle ridotte dimensioni, non siano in grado di installare batterie e processori in grado di supportare le importanti misure di sicurezza richieste per un'idonea tutela dei dati personali. Le capacità necessarie per la giustapposizione delle più corrette misure di sicurezza sono invece rinvenibili nel *cloud* e nel *fog computing*, che però, come detto, sono tecnologie connaturate da altre problematicità. Tali innovazioni vanno sono foriere di nuove opportunità dal punto di vista economico, ma anche di rischi per i diritti della personalità legati alla protezione dei dati personali.

I rischi di cui si è trattato nella tesi sono la discriminazione e l'indebita influenza sull'autodeterminazione della persona. La discriminazione può essere operata dall'uomo, e sono stati forniti alcuni esempi; tuttavia, quella che preoccupa di più avviene ad opera degli algoritmi, specialmente quelli di *machine learning*, in grado di operare attraverso regole inferte autonomamente, i quali sono in grado di operare diversi tipi di discriminazione. Il tipo di discriminazione cui si è prestata più attenzione è quella economica, riconducibile al *credit scoring*. La discriminazione degli algoritmi è causata dai *biases* di cui questi sono intrisi; è ormai riconosciuta la non neutralità degli algoritmi. Attenta letteratura ha evidenziato come possano essere distinti tre tipi di *biases*: preesistenti, tecnici ed emergenti. I primi sono riconducibili ai valori impressi dai progettatori dell'algoritmo: ad esempio, è ancora in parte diffusa l'idea che i lavoratori di sesso maschile siano maggiormente affidabili. Una discriminazione del genere si ha avuta nel caso del *software* di *machine learning* di assunzione di Amazon, che scartava i *curricula* femminili. Un altro tipo di *bias* è quello c.d. tecnico, riferibile a limiti nel *software* o nell'*hardware*. Può anche derivare dalla decontestualizzazione del *software*: un algoritmo progettato in un determinato luogo potrebbe essere intriso di valori che se trasportati in un'altra comunità possono essere considerati discriminanti. Esistono poi i *biases* emergenti, ad avviso dello scrivente i più preoccupanti in una società come quella odierna caratterizzata dalla fluidità, dalla nuova valutazione dei valori tradizionali. Questi, infatti, sono quelli che nascono in un momento

successivo rispetto alla progettazione. Emergono poiché sono cambiati i valori sociali mentre l'algoritmo non si è evoluto adeguatamente, o poiché, attraverso il *machine learning* ed il suo potere inferenziale, si è evoluto in modo discriminatorio.

I pericoli derivanti dalla discriminazione algoritmica sono mitigabili solo attraverso una grande responsabilizzazione, da aversi sin dal momento della progettazione dei codici, e che continui durante tutto il corso del trattamento. I soggetti coinvolti, dunque *in primis* i programmatori, non sono tuttavia soggetti agli obblighi imposti dal Regolamento, fintantoché non vengano qualificati come titolari del trattamento o responsabili del trattamento. Questo potrebbe costituire un problema, in quanto non si avrebbe un'attuazione compiuta del principio di *data protection by design* e *by default*. Inoltre, il titolare del trattamento potrebbe avere delle difficoltà a scegliere adeguatamente il responsabile del trattamento, ben potendo questo mantenere segreti alcuni elementi dei servizi offerti grazie al legittimo strumento del segreto industriale. L'*accountability* del titolare del trattamento, in ogni caso, non si risolve solo nell'adeguata scelta del responsabile del trattamento. Tutte le operazioni relative a dati vanno infatti costantemente monitorate. La discriminazione algoritmica, se risultante da un processo decisionale automatizzato, può però essere corretta grazie ad un duplice intervento: quello dell'interessato e del titolare del trattamento. Ai sensi dell'articolo 22 GDPR, infatti, l'interessato ha il diritto di essere informato e di esercitare i suoi diritti in merito alla decisione algoritmica. In particolare, potrebbe accedere ai suoi dati personali posti alla base della decisione, ottenendo una spiegazione relativa al come e perché l'algoritmo abbia deciso in quel determinato modo. La spiegazione del titolare del trattamento potrebbe a quel punto concorrere a realizzare la trasparenza necessaria al fine di consentire all'interessato un pieno controllo sui suoi dati personali.

Il principio di trasparenza, quando è in gioco la possibile lesione degli interessi legati al diritto alla protezione dei dati personali, dovrebbe prevalere anche sugli interessi economici tutelati attraverso l'istituto del segreto commerciale, cosa che però, di sovente, non avviene. Tuttavia, anche qualora fosse riconosciuta tale prevalenza, essa potrebbe non essere sufficiente per raggiungere il grado di trasparenza richiesto per un effettivo controllo dei propri dati personali. Il contesto dell'*Internet of Things* è infatti caratterizzato da una grande opacità, dovuta principalmente alla difficile intellegibilità dei sistemi, e questa potrebbe rendere poco utile anche una *disclosure* degli elementi dell'algoritmo coperti dal segreto industriale.

A prescindere dai processi decisionali automatizzati, le difficoltà nel rendere effettivo il controllo dei dati per l'interessato viene in parte mitigato grazie all'ausilio della tecnologia. Le *privacy enhancing technologies* (PETs) sono ormai riconosciute come strumento fondamentale per il controllo dei dati personali. In queste rientrano anche i *personal data services* (PDS), di

cui si è parlato in merito al modello Databox, virtuoso esempio di *data protection by design* e *by default*.

Infine, sono state evidenziate alcune problematiche ancora aperte riconducibili al rapporto tra *accountability*, responsabilità ed *Internet of Things.* Si è manifestata innanzitutto la necessità di espandere a tutti gli attori del trattamento, e non solo ai titolari ed a responsabili, i principi di *data protection by design*, resa particolarmente difficile dalla mancanza di relazione tra gli sviluppatori e i soggetti gravati dai nocumenti cagionati dai *software* in questione.

Inoltre, il pieno rispetto del principio di *accountability* da parte del titolare del trattamento potrebbe non essere sufficiente per garantire il rispetto della protezione dei dati personali e delle libertà fondamentali, in quanto il suo trattamento potrebbe rimanere *slegato* rispetto ad altri trattamenti dannosi operati assumendo il suo trattamento come base.

Nell'ultimo paragrafo si è difatti ragionato sulle possibili catene di trattamenti leciti. In questi casi, il titolare del trattamento potrà dirsi *accountable* avendo rispettato tutti i principi e gli obblighi imposti dal Regolamento. Purtroppo, però, il suo trattamento potrebbe costituire la base per altri trattamenti, più o meno leciti, altrimenti impossibili, e per questi non sarebbe chiamato a rispondere ai sensi dell'articolo 82 GDPR. A nulla servirebbe qualificare la natura della responsabilità derivante dall'articolo 82 GDPR in termini oggettivi puri, mancando la relazione tra alcuni titolari del trattamento ed altri titolari del trattamento successivi, e anche tra il titolare del trattamento e l'interessato.

Il principio di *accountability, dunque*, sebbene possa essere considerato soddisfacente dal punto di vista della responsabilizzazione, in quanto importa una serie di obblighi puntuali e procedure volte ad impegnare il titolare del trattamento a mitigare i rischi derivanti dal trattamento, rischia di divenire inefficace sotto il profilo della protezione. Come detto infatti, essere *accountable* risulta già particolarmente complesso nell'ambito dell'*Internet of Things*, e anche qualora lo si fosse, da una concatenazione di trattamenti *accountable* ben potrebbero derivare pregiudizi molto rilevanti, non tutelabili mediante l'articolo 82 del GDPR.

Alla luce di quanto espresso nell'elaborato, la ricerca di strumenti idonei alla protezione dei dati personali nell'ambito dell'*Internet of Things* sembra doversi concentrare al di fuori del GDPR. Si spera dunque in una forte presa di posizione dell'Unione Europea nei futuri regolamenti sulle comunicazioni elettroniche e sull'intelligenza artificiale, che alla luce di alcuni punti esaminati sembrano dedicare maggiore attenzione alla complessità dei trattamenti che caratterizzano l'era digitale.

Bibliografia

Abba B., Sulaiman M. N., Mustapha N., Perumal T., *HMM-Based Decision Model for Smart Home Environment*, International Journal of Smart Home, volume 8, numero 1, Gennaio 2014, pag. 129

Acciai R., *Il diritto alla protezione dei dati personali*, Maggioli Editore, Santarcangelo di Romagna, 2004

Agenzia dell'Unione europea per i diritti fondamentali e Consiglio d'Europa, *Privacy and data protection in mobile applications*, Novembre 2017

Agenzia dell'Unione europea per i diritti fondamentali, *#BigData: Discrimination in data-supported decision making*, 30 Maggio 2018

Agenzia dell'Unione europea per i diritti fondamentali e Consiglio d'Europa, *Manuale sul diritto europeo in materia di protezione dei dati*, 2018

Agrifoglio G., *Risarcimento e quantificazione del danno da lesione della privacy: dal danno alla persona al danno alla personalità*, Europa e Diritto privato, fascicolo 4, 2017, pag. 1265

Alpa G., Conte G., (a cura di), *La responsabilità d'impresa*, Giuffrè Editore, Milano, 2015

Alpa G., Resta G., *Le persone fisiche e i diritti della personalità*, in Sacco R., *Trattato di Diritto Civile*, Utet giuridica, Milano, 2019

Alpa G., Manuale di diritto privato, Wolters Kluwer Italia, Milano, 2020

Alpa G., *Diritto e intelligenza artificiale*, Pacini giuridica, Pisa, 2020

Altman I., *Privacy Regulation: Culturally Universal or Culturally Specific?*, Journal of Social Issues, volume 33, questione 3, 1977

Alwarafi A., Al-Thelaya K. A., Abdallah M., Schneider J., Hamdi M., *A Survey on Security and Privacy Issues in Edge-Computing-Assisted Internet of Things*, IEEE Internet of Things Journal, volume 8, Marzo 2021, pag. 4004

Amore G., *Fairness, Transparency e Accountability nella protezione dei dati personali*, Studium Iuris, volume 4, 2020

Angelakis V., Tragos E., Pöhls H. C., Kapovits A., Bassi A., *Designing, Developing, and Facilitating Smart Cities*, Springer, 2017

Arena F., Pau G., Severino A., *An Overview on the Current Status and Future Perspectives of Smart Cars*, Giugno 2020

Arora J. B., *IoT and Machine Learning- A Technological Combination for Smart Application*, International Conference on Innovative Advancement in Engineering and Technology, 21 Febbraio 2020

Ashton K., *That "Internet of things" thing*, RFID Journal, 22 Giugno 2009

Bale C., Fischer J. L., Schneider M. J., Weber S., Chang, S., *Legally Anonymizing Location Data Under the GDPR*, Giugno 2022

Basedow J., Hopt K. J., Zimmermann R. (edito da), con Stier A., *The Max Planck Encyclopedia of European Private Law*, Oxford University Press, 2012

Barbierato D., *Trattamento dei dati personali e «nuova» responsabilità civile*, Responsabilità Civile e Previdenza, fascicolo 6, 1 Giugno 2019, pag. 2151

Barcellona M., *Trattato della responsabilità civile*, Wolters Kluwer Italia, Milano, 2011

Berners-Lee T., Hendler J., Lassila O., *The Semantic Web*, Scientific American,17 Maggio, 2001

Bianca C. M., *La protezione dei dati personali*, Cedam, Padova, 2007

Bianca C. M., *Diritto civile. La responsabilità*, in Diritto Civile, Giuffrè, Milano, 1994

Bianca C. M., *Diritto civile. La responsabilità*, Giuffrè Francis Lefebvre, 2012

Bianca C. M., *Diritto civile. La responsabilità*, Giuffrè Francis Lefebvre, Milano, 2021

Bieker F., *The Right to Data Protection*, T.M.C. Asser press, Springer-Verlag GmbH, L'Aia, 2022

Bigliazzi Geri L., Breccia U., Busnelli F.D., Natoli U., *Diritto civile*, Utet, Torino, 1991

Bincoletto G., *Data Protection by Design in the E-Health Care Sector: theoretical and applied perspectives*, Nomos Verlagsgesellschaft, 2021

Boehme-Neβler V., *Privacy: a matter of democracy. Why democracy needs privacy and data protection*, International Data Privacy Law, volume 6, numero 3, 2016, pag. 222

Blumberg A., Eckersley P., *On locational privacy and how to avoid losing it forever*, Electronic Frontier Foundation, 2009

Bolognini L., Pelino E., Bistolfi C., *Il Regolamento privacy europeo*. Commentario alla nuova disciplina sulla protezione dei dati personali, Giuffrè Editore, Milano, 2016.

Bolognini L., Bistolfi C., *Pseudonymization and impacts of Big (personal/anonymous) Data processing in the transition from the Directive 95/46/EC to the new EU General Data Protection Regulation*, Computer Law & Security Review, volume 33, questione 2, Aprile 2017, pag. 171

Bolognini L., Pelino E., *Codice della disciplina privacy*, Giuffrè, Milano, 2019

Boncinelli V., *Modelli tecnici e disciplina giuridica del c.d. cloud computing*, Rivista italiana di informatica e diritto, fascicolo 1, 2021, pag. 27

Bonomi F., Milito R., Zhu J., Addepalli S., *Fog Computing and Its Role in the Internet of things*, Cisco Systems Inc, Agosto 2012

Borking J. J., Raab C. D., *Laws, PETs and other Technologies for Privacy Protection*, Journal of Information, Law & Technology (JILT), volume 1, 2001

Borrillo B., *La tutela della privacy e le nuove tecnologie: il principio di accountability e le sanzioni inflitte dalle Autorità di controllo dell'Unione europea dopo l'entrata in vigore del GDPR*, Dirittifondamentali.it, fascicolo 2, 2020, pag. 326

Bouhai N., Saleh I., *Internet of Things: Evolutions and Innovations*, John Wiley & Sons Inc., 29 Novembre 2017

Brasher E., *Addressing the Failure of Anonymization*: Guidance from the European Union's General Data Protection Regulation, Columbia Business Law Review, 2018, pag. 209

Bravo F., *Il «diritto» a trattare dati personali nello svolgimento dell'attività economica*, Cedam, 2018

Bravo F., *Trasparenza del codice sorgente e decisioni automatizzate*, Il diritto dell'informazione e dell'informatica, 2020, pag. 694

Brooks R., *Machine Learning Explained*, MIT Rethink, 28 Agosto 2017

Bygrave L. A., Tosoni L., *Article 4 (1). Personal data*, in Kuner C., Bygrave L. A., Docksey C., Drechsler L., *The EU General Data Protection Regulation (GDPR): A Commentary,* Oxford press, 13 Febbraio 2020

Caggiano I. A., *Il consenso al trattamento dei dati personali nel nuovo Regolamento europeo. Analisi giuridica e studi comportamentali*, Osservatorio del diritto civile e commerciale, fascicolo 1, Gennaio 2018, pag. 67

Calabrese G., *La responsabilità civile da illecito trattamento dei dati personali*, 2022

Calabresi G., *Concerning Cause and the Law of Torts: An Essay for Harry Kalven Jr.*, University of Chicago Law Review, volume 43, questione 1, articolo 8, 1975, pag. 69

Camardi C., *Note critiche in tema di danno da illecito trattamento dei dati personali*, Jus civile, volume 3, 2020, 786

Carrer L., *Il Comune di Como ha scoperto che il suo sistema di riconoscimento facciale non è quello che aveva comprato*, Wired, Settembre 2020

Caso R., *La società della mercificazione e della sorveglianza*: *dalla persona ai dati*. *Casi e problemi di diritto civile*, Ledizioni, Febbraio 2021

Cassano G., Fadda S., *Codice in materia di protezione dei dati personali*, Wolters Kluwer Italia, Ipsoa, 2004

Castellaneta M., D'Orazio R., Finocchiaro G., Pollicino O., Resta G., *Codice della privacy e data protection*, Giuffrè, Milano, 2021

Castronovo C., *Situazioni soggettive e tutela nella legge su il trattamento dei dati personali*, in Europa e Diritto privato, fascicolo 3, 1998, pag. 653

Castronovo C., Mazzamuto S., *Manuale di diritto* privato, Giuffrè Editore, Milano, 2007

Cataleta M., S., *Diritti umani e algoritmi*, Nuova Editrice Universitaria, Roma, 2021

Caterina R., Thobani S, *Il diritto al risarcimento dei* danni, Giurisprudenza italiana, Dicembre 2019, 2805

Cave S., Dihal K., Dillon S., *AI Narratives: A History of Imaginative Thinking about Intelligent Machines*, Oxford University Press, 5 Marzo 2020

Cavoukian A., *Privacy by Design*, Information & Privacy Commissioner, 2009

Celeste E., De Gregorio G., *Digital Humanism: The Constitutional Message of the GDPR*, Global Privacy Law Review, volume 3, questione 1, 2022, pag. 4

Chauvenet R., in D'Orazio R., Finocchiaro G., Pollicino O., Resta G., *Codice della privacy e data protection*, Giuffrè, Milano, 2021

Chen D., Kalra S., Irwin D., Shenoy P., Albrecht J., *Preventing Occupancy Detection From Smart Meters*, IEEE Transactions on Smart Grids, volume 6, numero 5, Settembre 2015

Chen D., Irwin D., *Weatherman: Exposing Weather-based Privacy Threats in Big Energy Data*, IEEE International Conference on Big Data, 11-14 Dicembre 2017

Chen D., Bovornkeeratiroj P., Irwin D., Shenoy P., *Private Memoirs of IoT Devices: Safeguarding User Privacy in the IoT Era*, IEEE 38th International Conference on Distributed Computing Systems (ICDCS), 2018

Chen N., Chen Y., Ye X., Ling H., Song, S., Huang C.-T., *Advances in Mobile Cloud Computing and Big Data in the 5G Era*, Springer, Studies in Big Data, volume 22, 2017

Cherciu N., *Non-personal data processing – why should we take it personally?*, European Journal of Privacy Law & Technologies, volume 2, 2020, pag. 183

Cirani S., Ferrari G., Picone M., Veltri L., *Internet of Things: Architectures, Protocols and Standards*, John Wiley & Sons, Inc, 12 Novembre 2018

Cisco, *Annual Internet Report*, 2018

Citron K., Solove D. J., *Privacy harms*, Boston University Law Review, 2022

Confessore N., *Cambridge Analytica and Facebook: The Scandal and the Fallout So* Far, New York Times, 4 Aprile 2018

Consiglio d'Europa e Corte Europea dei diritti dell'uomo, *Guide on Article 8 of the European Convention on Human Rights*, 31 Agosto 2022

Contaldi G., *Intelligenza artificiale e dati personali*, Ordine internazionale e diritti umani, 2021

Conti M., Dehghantanha A., Franke F., Watson S., *Internet of Things security and forensics: Challenges and opportunities*, Future Generation Computer Systems volume 78, parte 2, Gennaio 2018

Cordeiro M., *A Civil Liability for Processing of Personal Data in the GDPR*, European Data Protection Law Review, volume 5, questione 4, 2019, pag. 492

Crabtree A., Lodge T., Colley J., Greenhalgh C., Glover K., Haddadi H., Amar Y., Mortier R., Li Q., Moore J., Wang L., Yadav P., Zhao J., Brown A., Urquhart L., McAuley D., *Building accountability into the Internet of Things: the IoT Databox model*, Journal of Reliable Intelligent Environments, 2018, pag. 39

Cuffaro V., D'Orazio R., Ricciuto V., *Il codice del trattamento dei dati personali*, G. Giappichelli Editore, Torino, 2006

Cuffaro V., D'Orazio R., Ricciuto V., *I dati personali nel diritto europeo,* Giappichelli, Torino, 2019

D'Acquisto G., Naldi M., *Big data e privacy by design: anonimizzazione pseudonimizzazione sicurezza*, Giappichelli, Torino, 22 Febbraio 2017

D'Orazio R., Finocchiaro G., Pollicino O., Resta G., *Codice della privacy e data protection*, Giuffrè, Milano, 2021

Dahal K., Giri D., Neogy S., Dutta S., Kumar S. (edito da), *Internet of Things and Its Applications*, Springer, 2020

De Franceschi A., in Cuffaro V., D'Orazio R., Ricciuto V., *I dati personali nel diritto europeo,* Giappichelli, Torino, 2019

De Hert P., Papakonstantinouac V., *The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals*, Computer Law & Security Review, volume 28, questione 2, Aprile 2012, pag. 130

De Rada D., *La responsabilità civile in caso di mancato rispetto del GDPR. Privacy by default, privacy by design e accountability nell'ottica del Diritto Privato*, Federalismi.it, 18 Dicembre 2019

De Rosa P., *Diritti e libertà in Internet: un mondo digitale è davvero sinonimo di libertà?*, Data Protection Law, numero 1, 2022, pag. 3

De Terwangne C., *Council of Europe convention 108 +: A modernised international treaty for the protection of personal data*, Computer Law & Security Review, volume 40, Aprile 2021

Del Federico C., Popoli A. R., *Le definizioni*, in Finocchiaro G., *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Zanichelli, Torino, 2019

Del Ninno A., *La tutela dei dati personali*, Cedam, Padova, 2006

Delmastro M., Nicita A., *Big data. Come stanno cambiando il nostro mondo*, Il Mulino, Bologna, 2019

Di Landro A. C., *Big Data. Rischi e tutele nel trattamento di dati personali*, Edizioni Scientifiche Italiane, Napoli, 2020

Docherty I., Marsden G., Anable J., *The governance of smart mobility, transportation research part A*, volume 115, 2008, pag. 114

Docksey C., *Article 24. Responsability of the controller*, in Kuner C., Bygrave L. A., Docksey C., Drechsler L., *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford press, 13 Febbraio 2020

Domingos P., *The master algorithm: how the quest for the ultimate learning machine will remake our world*, Basic Books, New York, 2015

Ducato R., *La crisi della definizione di dato personale del dato personale nell'era del web 3.0*, in *Le definizioni nel diritto*, Atti delle giornate di studio 30-31 ottobre 2015, Fulvio

C., Tomasi M., Università degli studi di Trento, quaderni della facoltà di giurisprudenza, numero 26, Dicembre 2016, pag. 143

Edpb, parere numero 6 del 2017 sulla proposta di regolamento sulla privacy e le comunicazioni elettroniche (regolamento e-privacy)

Edps, parere del 7 Marzo 2012 sul progetto di riforma relativo alla protezione dei dati personali varato dalla Commissione

Edps, *Technology report* numero 1 (*smart glasses and data protection*), 18 Gennaio 2019

Edu J. S., Such J. M., Suarez-Tangil G., *Smart Home Personal Assistants: A Security and Privacy Review*, ACM Computing Surveys, volume 53, articolo 116, Dicembre 2020

Edwards L., Veale M., *Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking for*, Duke Law & Technology Review, 2017, pag. 15

Edwards L., Veale M., *Enslaving the algorithm: from a "right to explanation" to a "right to better decision"?*, IEEE Security & Privacy, volume 16, numero 3, 2018, pag. 46

Enisa, *Handbook on Security of Personal Data Processing*, Dicembre 2017

Enisa, *Privacy by design in big data. An overview of privacy enhancing technologies in the era of big data analytics*, Dicembre 2015

Enisa, *Readiness Analysis for the Adoption and Evolution of Privacy Enhancing Technologies*, Dicembre 2015

Enisa, *Privacy and data protection in mobile applications*, del Novembre 2017

Evans D., Cisco, *The Internet of things How the Next Evolution of the Internet Is Changing Everything*, Aprile 2011

Federal Trade Commission, *Privacy & Security in a Internet of Things: Privacy & Security in a Connected World World*, ftc staff report, Gennaio 2015

Fernández-Ares A., Mora A.M., Arenas M.G., García-Sanchez P., Romero G., Rivas V, Castillo P.A., Merelo J.J., *Studying real traffic and mobility scenarios for a Smart City using a new monitoring and tracking system*, Future Generation Computer Systems, volume 76, Novembre 2017, pag. 163

Ferrari G. F. (a cura di), *La prossima città*, Milano, 2017
Finck M., Pallas F., *They who must not be identified—distinguishing personal from non-personal data under the GDPR*, International Data Privacy Law, 1 Ottobre 2019, pag. 11

Finocchiaro G., *Privacy e protezione dei dati personali*, Zanichelli editore, Torino, 2012

Finocchiaro G., Delfini F., (a cura di), *Diritto dell'informatica*, Wolters Kluwer Italia, Milano, 2014

Finocchiaro G., *Introduzione al Regolamento europeo sulla protezione dei dati*, Nuove leggi civili commentate, volume 1, 2017, pag. 1

Finocchiaro G., *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Zanichelli, Torino, 2019

Finocchiaro G., *Il Principio di Accountability*, Giurisprudenza Italiana, Dicembre 2019

Finocchiaro G., *Intelligenza Artificiale e protezione dei dati personali*, Giurisprudenza Italiana, 2019, pag. 1670

Firouzi F., Chakrabarty K., Nassif S. (edito da), *Intelligent Internet of Things*, Springer, Svizzera, 2020

Floridi L., *The Fourth Revolution: How the Infosphere is Reshaping Human Reality*, Oxford University Press, 2014

Foglia C., *Il dilemma (ancora aperto) dell'anonimizzazione e il ruolo della pseudonimizzazione*, in Panetta R. (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, Giuffrè, Milano, 15 Giugno 2019

Franzoni M., *L'illecito*, Giuffrè editore, Milano, 2004

Friedman B., Nissenbaum H., *Bias in Computer Systems*, ACM Transactions on Information Systems, volume 14, questione 3, Luglio 1996, 330

Fuster G., *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Springer, Dordrecht, 2014

Gaetano G., *La mancata nomina del responsabile per la protezione dei dati personali per i soggetti privati*, Data Protection Law, Gennaio – Giugno 2021, pag. 43

Gatouillat A., Badr Y., Massot B., Sejdić E., *Internet of Medical Things: A Review of Recent Contributions Dealing With Cyber-Physical Systems in Medicine*, in IEEE Internet of things Journal, volume. 5, 2018, pag. 3810

Gambini M., *Algoritmi e sicurezza,* Giurisprudenza italiana, Luglio 2019, pag. 1726

Gazzoni F., *Manuale di diritto privato*, Edizioni Scientifiche Italiane s.p.a., Napoli, 2013

Gazzoni F., *Manuale di diritto privato*, Edizioni Scientifiche Italiane s.p.a., Napoli, 2021

Gellert R., *Personal data's ever-expanding scope in smart environments and possible path(s) for regulating emerging digital technologies*, International Data Privacy Law, volume 11, numero 2, 2021, pag. 196

Geng H., *The internet of things and data analytics handbook*, John Wiley & Sons, Inc.,, New Jersey (Hoboken) e Canada, 2017

Giampiccolo G., *La tutela giuridica della persona umana e il c.d. diritto alla riservatezza*, Rivista trimestrale di diritto e procedura civile, 1958, pag. 458

Giovanella F., *Le persone e le cose: la tutela dei dati personali nell'ambito dell'Internet of Things,* in Cuffaro V., D'Orazio R., Ricciuto V., *I dati personali nel diritto europeo,* Giappichelli, Torino, 2019

González G., Van Brakel R., De Hert P. (edito da), *Research Handbook on Privacy and Data Protection Law*, Edward Elgar Publishing Limited, Northampton, 15 Marzo 2022

Greco L., *L'organigramma privacy: i soggetti del trattamento*, in Finocchiaro G., *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Zanichelli, Torino, 2019

Guarda P., *Data Protection, Information Privacy, and Security Measures: an essay on the European and the italian legal frameworks*, Ciberspazio e diritto, Dicembre 2008

Guarda P., *Il regime giuridico dei dati della ricerca*, Università degli Studi di Trento, 2020

Grabenwarter C., *European Convention on Human* Rights, Verlag C. H. Beck oHG, Monaco di Baviera, 2014

Greanleaf G., *How far can Convention 108+ 'globalise'? Prospects for Asian accessions*, Computer Law & Security Review, volume 40, Maggio 2021, pag. 1

Greenleaf G., *'Modernised' Data Protection Convention 108 and the GDPR,* Privacy Laws & Business International Report, 13 Novembre 2018

Greguric M., Vujic M., Alexopoulos C., Miletic M., *Application of Deep Reinforcement Learning in Traffic Signal Control: An Overview and Impact of Open Traffic Data*, 2020

Gruppo di lavoro *ex* articolo 29. Parere numero 4 del 20 Giugno 2007 (WP136)

Gruppo di lavoro *ex* articolo 29. Parere numero 3 del 13 Luglio 2010 sul principio di responsabilità

Gruppo di lavoro *ex* articolo 29. Parere numero 1 del 16 Febbraio 2010 sui concetti di responsabile del trattamento e incaricato del trattamento

Gruppo di lavoro *ex* articolo 29. Parere numero 13 del 16 Maggio 2011 sui servizi di geolocalizzazione su dispositivi mobili intelligenti

Gruppo di lavoro *ex* articolo 29. Parere numero 2 del 2013 sulle applicazioni per dispositivi intelligenti (WP 202)

Gruppo di lavoro *ex* articolo 29. Parere numero 8 del 16 Settembre 2014 sui recenti sviluppi nel campo dell'Internet degli oggetti (WP 223)

Gruppo di lavoro *ex* articolo 29. Parere numero 5 del 10 Aprile 2014 sulle tecniche di anonimizzazione

Gruppo di lavoro *ex* articolo 29. Parerene del 30 Maggio 2014 sull'approccio al rischio

Gruppo di lavoro *ex* articolo 29. Parere numero 6 del 9 Aprile 2014 sulla nozione del legittimo interesse e del titolare del trattamento ai sensi dell'articolo 7 della Direttiva 95/46/CE

Gruppo di lavoro *ex* articolo 29. Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679 del 3 Ottobre 2017, aggiornati il 6 Febbraio 2018 (WP 251)

Gruppo di lavoro *ex* articolo 29. Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679, 4 Ottobre 2017

Gruppo di lavoro *ex* articolo 29. Linee guida del 6 Febbraio 2018 sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679, (WP 251)

Gruppo di lavoro *ex* articolo 29. Linee guida sulla trasparenza ai sensi del regolamento 2016/679 adottate il 29 novembre 2017 ed emendate l'11 aprile 2018 (WP 260)

Gruppo di lavoro *ex* articolo 29. Linee guida 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR

Hadzovic S., Mrdovic S., Radonjic M., *Identification of IoT Actors*, Sensors, volume 21, 2021, pag. 1

Hamon R., Junklewitz H., Sanchez I., Malgieri G., De Hert P., *Bridginh the Gap Between AI and Explainability in the GDPR: Towards Trustworthiness-by-Design in Automated Decision-Making*, IEEE computational intelligence magazine, Febbraio 2022

Hancke G. P., De Carvalho B., Hancke G. P. Jr., *The Role of Advanced Sensing in Smart Cities*, Dicembre 2012

Haskel J., Westlake S., *Capitalism without capital*, Princeton University Press, 2018

Hijmans H., *The European Union as Guardian of Internet Privacy*, Springer, 2016

Hildebrandt M., *Law as Information in the Era of Data-Driven Agency*, The Modern Law Review, volume 74, Gennaio 2016, pag. 1

Hildebrandt M., O'Hara K., *Life and the Law in the Era of Data-Driven Agency*, Edward Elgar, 2020

Hintze M., *Viewing the GDPR through a de-identification lens: a tool for compliance, clarification and consistency*, Oxford University Press, volume 8, questione 1, Febbraio 2018, pag. 86

Holmes M., Nieto M.P., Song H., *Modelling Patient Behaviour Using IoT Sensor Data: a Case Study to Evaluate Techniques for Modelling Domestic Behaviour in Recovery from Total Hip Replacement Surgery*, Journal of Healthcare Informatics Research 4, 2020, pag. 238

Hu R., Yu B., Big Data Analytics for Cyber-Physical Systems, Springer, Cham, 2020

IEEE, *Towards a definition of the Internet of things (IoT)*, Maggio 2015

Imperiali R., Imperiali R., *Codice della privacy*, Il Sole 24 Ore, Milano, 2004

Inacio I., Silveira e Silva V., *The liability of data controllers/of data processors*, 2020

Italia V., *Codice della privacy*, Giuffrè editore, Milano, 2004

Imperiali R., Imperiali R., *Codice della privacy*, Il Sole 24 Ore, Milano, 2004

Inacio I., Silveira e Silva V., *The liability of data controllers/of data processors*, 2020

ITU Internet Reports, *The Internet of things*, Novembre 2005

ITU-T Raccomandazione Y.2060, *Overview of the Internet of things*, Giugno 2012

Jafarian B., Yazdani N., Haghighi M. S., *Discrimination-aware trust management for social internet of things*, Computer Networks, volume 178, 2020, pag. 1

Jalal L., Anedda M., Popescu V., Murroni M., *QoE Assessment for IoT-Based Multi Sensorial Media Broadcasting*, in IEEE Transactions on Broadcasting, volume 64, numero 2, Giugno 2018, pag. 552

Jannsen H., *An approach for a fundamental rights impact assessment to automated decision-making*, International Data Privacy Law, volume 10, numero 1, 2020, pag. 76

Rouillard J. *The Pervasive Fridge. A smart computer system against uneaten food loss*, Seventh International Conference on Systems (ICONS2012), Febbraio 2012

Kaminski M. E., *The right to explanation, explained*, Berkeley Technology Law Journal, volume 34, numero 1, 2019, pag. 189

Karadogan B., *Modernized Convention 108 And GDPR*, Ottobre 2019

Kashef M., Visvizi A., Troisi O., *Smart city as a smart service system: Human-computer interaction and smart city surveillance systems*, computers in Human Behavior, volume 124, Novembre 2021, pag. 1

Kedzior M., *GDPR and beyond—a year of changes in the data protection landscape of the European Union*, Europäische Rechtsakademie (ERA), 14 Febbraio 2019

Kim T.W., Maimone F., Pattit K., Sison A. J., Teehankee B., *Master and Slave: The Dialectic of Human-Artificial Intelligence Engagement*, Humanist Management Journal, 3 Dicembre 2021, pag. 355

Kolain M., Grafenauer C., Ebers M., *Anonymity Assessment – A Universal Tool for Measuring Anonymity of Data Sets under the GDPR with a Special Focus on Smart Robotics*, Rutgers University Computer & Technology Law Journal, volume 48, numero 2, 2022

Kosmides T., *The legal nature of the controller's civil liability according to art. 23 of Directive 95/46 EC (Data Protection Directive)*, Atene, 2013

Kovachev D., Cao Y., Klamma R., *Mobile Cloud Computing: A Comparison of Application Models*, Information Systems & Database Technologies, 2011

Kuner C., Bygrave L. A., Docksey C., Drechsler L., *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford press, 13 Febbraio 2020

Lachaud E., *Accountability and Certification in the GDPR*, 22 Ottobre 2021

Lessig L., *Code and Other Laws of Cyberspace*, Basic Books, New York, 1999

Linee guida numero 4 del 13 Novembre 2019 del European Data Protection Board sull'articolo 25 e il principio di *Data Protection by Design and by Default*

Lorenza, *Internet of Medical Things (IoMT): cos'è, come si fa e quali vantaggi porta alla sanità e ai cittadini*, Internet 4 things. Gennaio 2021

Lynskey O., *The Foundations of EU Data Protection Law*, Springer, Oxford University Press, Ney York, 2019

Macenaite M., *The "Riskification" of European Data Protection Law through a two-fold Shift*, Cambridge University Press, 10 Ottobre 2017

Maglio M., Polini M., Tilli N., *Manuale di diritto alla protezione dei dati personali*, Maggioli, Santarcangelo di Romagna, Giugno 2019

Malbakken O. K., *Towards Measuring Legal Compliance. A case study on EU Directive 95/46, Article 17: Security in Processing*, 2004

Malgieri G., Comandè G., *Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation*, International Data Privacy Law, volume 7, numero 3, 2017, pag. 243

Malgieri C., in Finocchiaro G., Pollicino O., Resta G., *Codice della privacy e data protection*, Giuffrè, Milano, 2021

Maldonado Y., Trujillo L., Schütze O., Riccardi A., Vasile M., *Results of the Numerical and Evolutionary Optimization Workshop NEO 2016 and the NEO Cities 2016 Workshop Held on September 20–24*, 2016, Tlalnepantla, Mexico, Studies in Computational Intelligence, Springer, volume 731, 2018

Mantelero A., *Processi di outsourcing informatico e cloud computing: la gestione dei dati personali ed aziendali*, Il diritto dell'informazione e dell'informatica, fascicolo 4-5, 2010, pag. 673

Mantelero A., *Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data* protection, Computer Law & Security Review, volume 32, 2016, pag. 238

Mantelero A., *Responsabilità e rischio nel Reg. UE 2016/679*, Le nuove leggi civili commentate, volume 1, Febbraio 2017, pag. 144

Mantelero A., *La gestione del rischio*, in Finocchiaro G., *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Zanichelli, Torino, 2019

Marr B., Forbes, *Big Data: 20 Mind-Boggling Facts Everyone Must Read*, Settembre 2015

Martelli S. (a cura di), *Internet of things (IoT) e Cloud Computing*, Settembre 2019

Margioti F., *Internet of things (IoT): applicazioni e problematiche*, Settembre 2019

Marighetto A., *La colpa e il rischio*, Revista da Faculdade de Direito, 18 Luglio 2018

Mastorakis G., Mavromoustakis C. X., Batalla J., M., Pallis E., (edito da), *Convergence of Artificial Intelligence and the Internet of things*, Springer, 2020

Mayer-Schönberger V., Cukier K. N., *Big data: A Revolution That Will Transform How We Live, Work, and Think*, Houghton Mifflin Harcourt, 5 Marzo 2013

Mazzamuto S., *Manuale di diritto privato*, G. Giappichelli Editore, Torino, 2019

Mazzamuto S., *Il contratto di diritto europeo*, G. Giappichelli Editore, Torino, 2020

McKinsey Global Institute, *Big Data: The next frontier for innovation, competition and productivity*, Maggio 2011

Mell P., Grance T., *The NIST Definition of Cloud Computing*, Recommendations of the National Institute of Standards and Technology, Settembre 2011

Mendoza I., Bygrave L. A., *The Right not to be Subject to Automated Decisions based on Profiling*, Research Paper Series, Oslo, numero 20, 2017

Mengoni L., *Obbligazioni di mezzi e obbligazioni di risultato*, Rivista di diritto commerciale, fascicolo 5-6, 1954, pag. 185

Mengozzi P., Morviducci C. *Istituzioni di diritto dell'Unione Europea*, Wolters Kluwer, Milano, 2018

Messinetti R., *La tutela della persona umana versus l'intelligenza artificiale. Potere decisionale dell'apparato tecnologico e diritto alla spiegazione della decisione automatizzata*, Contratto e impresa, volume 3, 2019, pag. 861

Mittlestadt B. D., Allo P., Taddeo M., Wachter S., Floridi L., *The ethics of algorithms: Mapping the debate*, Big Data & Society, volume 3, questione 2, Luglio – Dicembre 2016, pag. 1

Mittelstadt B., *From Individual to Group Privacy in Big Data Analytics*, Philosophy & Technology, volume 30, 2017, pag. 475

Mohammeda Z., Ahmedb E., *Internet of things Applications*, Challenges and Related Future Technologies, Gennaio 2017

Mohammadi M., Al-Fuqaha A., *Enabling Cognitive Smart Cities Using Big Data and Machine Learning*: *Approaches and Challenges*, IEEE Communications magazine, volume 56, numero 2, 2018, pag. 94

Monducci J., Sartor G., *Il codice in materia di protezione dei dati personali*, Cedam, Padova, 2004

Mortier R., Haddadi H., Henderson T., McAuley D., Crowcroft J. *Human-Data Interaction: The Human Face of the Data-Driven Society*, 2014

Mourby M., Mackey E., Elliot M., Gowans H., Wallace S. E., Bell J., Smith H., Aidinlis S., Kaye J., *Are 'pseudonymised' data always personal data? Implications of the GDPR for administrative data research in the UK*, computer law & security review, volume 34, 2018, pag. 222

Musso M., *l software che sfrutta lo smartphone per evitare il traffico*, Wired, 2017.
Napolitano D., *Le orecchie della smart city. Riconoscimento vocale e ascolto operazionale nella "città senziente"*, rivista trimestrale di scienza dell'amministrazione, Aprile 2020

Nawaz M. S., Ur Rehman Khan S., Hussain S., Iqbal J., *A study on application programming interface recommendation: state-of-the-art techniques, challenges and future directions*, Library Hi Tech, Emerald Publishing Limited, 2021

Niroshinie F., Seng W. L., Wenny R., *Mobile cloud computing: A survey, Future Generation Computer Systems*, volume 29, 2013

Norval C., Cobbe J., Singh J., *Towards an accountable Internet of Things. A call for reviewability*, in Crabtree A., Haddadi H., Mortier R. (edito da), *Privacy by design for the Internet of Things; Building accountability and security*, Londra, 2021

Ohm P., *Broken Promises of Prifvacy: Responding to the Surprising Failure of Anonymization*, UCLA Law Review, volume 57, 2010, pag. 1701

Paiva S., Ahad M.A., Zafar S., Tripathi G., Khalique A., Hussain I., *Privacy and security challenges in smart and sustainable mobility*, SN Applied Science 2, articolo numero 1175, 2020

Paliotta A. P., *Le politiche innovative di sicurezza nelle città tra tecnologie di riconoscimento e smart cities*, SINAPPSI – Connessioni tra ricerca e politiche pubbliche, numero 2, 2020

Panetta R. (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, Giuffrè, Milano, 15 Giugno 2019

Panetta R., *Privacy is not dead: it's hiring!*, in Panetta R. (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, Giuffrè, Milano, 15 Giugno 2019

Panetta R., *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, Giuffrè, Milano, 2010

Pardolesi R., *Diritto alla riservatezza e circolazione dei dati personali*, Giuffrè, Milano, 2003

Pariser A., *The Filter Bubble: What the Internet Is Hiding from You*, Penguin, 1 Marzo 2012

Pascuzzi G., *Has comparative law in Italy lost its driving force?,* Trento Law and Technology Research Group Research, Paper numero 31, Marzo 2017

Pascuzzi G., *Il diritto dell'era digitale*, Il Mulino, Bologna, 2020

Pasquale F., *The Black Box Society: The Secret Algorithms That Control Money and Information*, Harvard University Press, 2015

Passaglia P., *Il Sistema delle fonti normative in materia di tutela dei dati personali*, in Cuffaro V., D'Orazio R., Ricciuto V*., I dati personali nel diritto europeo*, Giappichelli, Torino, 2019

Patel P., Patel K., Tyagi S., Kumar N., Obaidat M. S., *An advanced Internet of things based Security Alert System for Smart Home*, International Conference on Computer, Information and Telecommunication Systems (CITS), 2017

Pellecchia E., *La responsabilità civile per trattamento dei dati personali*, Responsabilità Civile e Previdenza, fascicolo 2, 2006, pag. 234

Peers S., Hervey T., Kenner J., Ward a. (edito da), *The EU Charter of Fundamental Rights*, Hart/Beck, Londra, 2021

Peppet S. R., *Regulating the internet of things: first steps toward managing discrimination, privacy, security and consent*, Texas Law Review, 1 Marzo 2014, pag. 85

Perera C., McCormick C., Bandara A. K., Price B., A., Nuseibeh B., *Privacy-by-Design Framework for Assessing Internet of Things Applications and Platforms*, The 6th International Conference on the Internet of Things, Stoccarda, Novembre 2016

Piraino F., *Il Regolamento Europeo generale sulla protezione dei dati personali e i diritti dell'interessato*, Nuove leggi civili commentate, volume 2, 2017, pag. 369

Pizzetti F., *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Giappichelli, Torino, 2016

Pizzetti F., *Privacy e il diritto europeo alla protezione dei dati personali*, Giappichelli, Torino, 2016

Pizzetti F., *Intelligenza artificiale, protezione dei dati personali e regolazione*, G. Giappichelli Editore, Torino, 2018

Polini M., *Privacy e protezione dei dati personali nell'ordinamento europeo e italiano*, in Maglio M., Polini M., Tilli N., *Manuale di diritto alla protezione dei dati personali*, Maggioli, Santarcangelo di Romagna, Giugno 2019

Purtova N., *The law of everything. Broad concept of personal data and future of EU data protection law*, Law, Innovation, and Technology, volume 10, questione 1, 2018, pag. 41

Quelle C., *The 'risk revolution' in EU data protection law: We can't have our cake and eat it, too*, Tilburg Law School Legal Studies Research Paper Series, numero 17, 2017, pag. 506

Raffiotta E. C., Baroni M., *Intelligenza artificiale, strumenti di identificazione e tutela dell'identità*, BioLaw Journal, numero 1, 12 Aprile 2022, pag. 1

Ragno F., *Il diritto fondamentale alla tutela dei dati personali e la dimensione transnazionale del private enforcement del GDPR*, Ordine internazionale e diritti umani, 2020

Ramón Saura J., Ribeiro-Soriano D., Palacios-Marqués D., *Setting Privacy "by Default" in Social IoT: Theorizing the Challenges and Directions in Big Data Research*, Big Data Research, volume 25, 2021, pag. 1

Raso F., Hilligoss H., Krishnamurthy V., Bavitz C., Levin K., *Artificial Intelligence & Human Rights: Opportunities & Risks*, Berkman Klein Center for Internet & Society Research Publication, 2018

Ratti M., *La responsabilità da illecito trattamento dei dati personali*, in Finocchiaro G., *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Zanichelli, Torino, 2019

Ratti M., in D'Orazio R., Finocchiaro G., Pollicino O., Resta G., *Codice della privacy e data protection*, Giuffrè, Milano, 2021

Redazione Osservatori Digital Innovation, *Alla scoperta del Deep Learning*: significato, esempi e applicazioni, Febbraio 2021

Resta G., *Identità personale e identità* digitale, Il diritto dell'informazione e dell'informatica, fascicolo 3, 2007, pag. 511

Ricci S., Vaciago G., *Gli adempimenti del dpo*, Giuffrè Francis Lefebvre, Milano, 2019

Riccio G. M., Scorza G., Belisario E. (a cura di), *GDPR e normativa privacy*, Wolters Kluwer, Milano, 2018

Riccio G. M., Scorza G., Belisario E. (a cura di), *GDPR e normativa privacy*, Ipsoa, Milano, 2022

Ricciuto V., *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, Cuffaro V., D'Orazio R., Ricciuto V.*, I dati personali nel diritto europeo*, Giappichelli, Torino, 2019

Richterich A., *How Data-Driven research fuelled the Cambridge Analytica controversy*, The Open Journal of Sociopolitical Studies, 2018

Rocher L, Hendrickx J. M., de Montjoye Y.-A., *Estimating the success of re-identifications in incomplete datasets using generative models*, Nature Communications, volume 10, articolo numero 3069, 2019, pag. 1

Rodotà S., *Tecnologie e diritti*, Il Mulino, Bologna, 1995

Rodotà S., *Il problema della responsabilità civile*, Giuffrè, Milano, 1967

Romeri A., Ruggieri S., *A multidisciplinary survey on discrimination analysis*, The Knowledge Engineering Review, 2012

Rouillard J., The Pervasive Fridge. *A smart computer system against uneaten food loss*, Seventh International Conference on Systems (ICONS2012), Febbraio 2012

Ruffolo U. (a cura di), *Intelligenza artificiale*, Giuffrè Francis Lefebvre, Milano, 2020

Sadhukhan P., *An IoT-based E-parking system for smart cities*, International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2017

Sajfert J., Quintel T., *Data protection Directive (Eu) 2016/680 for police and criminal justice authorities*, 1 Dicembre 2017

Sandulli S., *Algoritmi, trasparenza ed effettività del consenso*, Jus civile, volume 5, 2021, pag. 1528

Saxena S., Pradhan A., K., *Internet of Things. Security and Privacy in Cyberspace*, Transactions on Computer Systems and Networks, Springer, Singapore, 2022

Selbst A. D., Powles J., *Meaningful Information ant the Right to Explanation*, International Data Privacy Law, volume 7, numero 4, Novembre 2017, pag. 233

Selzer A., *The Appropriateness of Technical and Organisational Measures under Article 32 GDPR*, European Data Protection Law Review, 2021, pag. 120

Sentenza R. (Bridges) contro Chief Constable Of South Wales Police & Information Commissioner

Settimio R., *Obblighi e responsabilità dei soggetti del trattamento: titolare e responsabile a confronto*, GiustiziaCivile.com, 18 Marzo 2022; nota a: Cassazione civile, numero 21234, 23 luglio 2021

Schabas W. A., *The European Convention on Human Rights*, Oxford University Press, New York, 2015

Schwartz P. M., Solove D. J., *Reconciling Personal Information in the United States and European Union*, California Law Review, 2014

Scognamiglio C., *Buona fede e responsabilità civile*, in Europa e Diritto Privato, fascicolo 2, 2001, pag. 343

Shaikh Y. S., *Privacy preserving internet of things recommender systems for smart cities*, Networking and Internet Architecture [cs.NI], Marzo 2020

Sica S., Stanzione P., *La nuova disciplina della privacy*, Zanichelli Editore, Bologna, 2005

Sica S., in D'Orazio R., Finocchiaro G., Pollicino O., Resta G., *Codice della privacy e data protection*, Giuffrè, Milano, 2021

Singh J., Cobbe J., Norval C*., Decision Provenance: Harnessing Data Flow for Accountable Systems,* IEEE Access, volume 7, 16 Dicembre 2019

Smorto G., *Il criterio di imputazione della responsabilità civile. Colpa e responsabilità oggettiva in civil law e common law*, Europa e Diritto Privato, fascicolo 2, 2008, pag. 423

Smorto G., *Verso una disciplina giuridica della sharing mobility nell'Unione europea*, Diritto e Questioni pubbliche, numero 17, 2020, pag. 17

Sobolewski M., Mazur J., Paliński M., *The European Digital Single Market*, Volume 52, numero 4, Luglio/Agosto 2017, pag. 196

Solove D., J., *"I've Got Nothing to Hide and Other Misunderstandings of Privacy*, San Diego Law Review, volume 44, 2007, pag. 745

Solove D. J., Schwartz P., *Information Privacy Law*, Wolters Kluwer, New York, 2021

Stach C., Gritti C., Mitschang B., *Bringing Privacy Control Back to Citizens*, Proceedings of the 35th Annual ACM Symposium on Applied Computing, Marzo 2020

Stalla-Bourdillon S., Knight A., *Anonymous Data v. Personal Data — A False Debate: An EU Perspective on Anonymization, Pseudonymization and Personal Data*, Wisconsin International Law Journal, 6 Marzo 2017, pag. 284

Stanzione P., *I "poteri privati" delle piattaforme e le nuove frontiere della privacy*, Giappichelli, Torino, 2022

Strugala R., *Art. 82 GDPR: Strict Liability or Liability Based on Fault?* European Journal of Privacy Law & Technologies (EJPLT), 2020, pag. 71

Sweeney L., *Simple Demographics Often Identify People Uniquely*, Carnegie Mellon University, Data Privacy Working Paper numero 3. Pittsburgh, 2000

Tanwar S., Patel P., Patel K., Tyagi S., Kumar N., Obaidat M. S., *An advanced Internet of things based Security Alert System for Smart Home*, International Conference on Computer, Information and Telecommunication Systems (CITS), 2017

Tava N., *Smart City: i mille utilizzi della sensoristica IoT*, 17 Novembre 2020

Tene O., Polonetsky J., *Big Data for All: Privacy and User Control in the Age of Analytics*, Northwestern Journal of Technology and Intellectual Property, 2013

The European Commission's high-level expert group on artificial intelligence, *A definition of AI: main capabilities and scientific disciplines*, Dicembre 2018

Tordera E. M., Masip-Bruin X., García-Almiñana J., Jukan A., Ren G., Zhu J., Farré J., *What is a Fog Node? A Tutorial on Current Concepts towards a Common Definition*, Novembre 2016

Torra V. Navarro-Arribas G., *Big Data Privacy and Anonymization*, Springer, book series: IFIP Advances in Information and Communication Technology, 2017

Torrente A., Schlesinger P., *Manuale di diritto privato*, Giuffrè Francis Lefebvre, 2019

Tosi E., *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale*, Giuffrè, Milano, 2019

Tosi E., *Trattamento illecito dei dati personali, responsabilità oggettiva e danno non patrimoniale alla luce dell'art. 82 del GDPR UE*, in Danno e responsabilità, volume 4, 2020

Trimarchi P., *Rischio e responsabilità oggettiva*, Giuffrè, Milano, 1961

Trimarchi P., *La responsabilità civile: atti illeciti, rischio, danno*, Giuffrè, Milano, 2021

Troisi E., *Decisione algoritmica. Black-box e AI etica: Il diritto di accesso come diritto a ottenere una spiegazione*, Jus Civile, volume 4, 2022, pag. 953

Truli E., *The General Data protection Regulation and Civil Liability*, 22 Giugno 2018

Tschider C. A., *Regulating the Internet of Things: Discrimination, Privacy, And Cybersecurity in the Artificial Intelligence Age*, Denver Law Review, volume 96, questione 1, 2018, pag. 87

Ufficio dell'Alto Commissario per i Diritti Umani, *Universal Declaration of Human Rights at 70: 30 Articles on 30 Articles - Article 12*, 14 Novembre 2018

Valtteri S., *Work-based use of Smart Personal Assistants and their impact on technostress*, 2021

Van Alsenoy B., *Liability under EU Data Protection Law*, Jipitec, 2016, pag. 271

Varmarken, J., Le H., Shuba A., Markopoulou A., e Shafiq Z., *The TV is Smart and Full of Trackers: Measuring Smart TV Advertising and Tracking*, Proceedings on Privacy Enhancing Technologies, Aprile 2020

Varshini B., Yogesh H. R., Pasha S. D., Suhail M., Madhumitha V., Sasi A*., IoT-Enabled smart doors for monitoring body temperature and face mask detection*, Global Transitions Proceedings, volume 2, Novembre 2021, pag. 246

Venezian G., *Danno e risarcimento fuori dei contratti*, Opere giuridiche, volume 1, Roma, 1919

Vishnu S., Ramson S. R. J., Jegan R., *Internet of Medical Things (IoMT) - An overview*, 5th International Conference on Devices, Circuits and Systems (ICDCS), 2020

Vokinger K. N., Stekhoven D. J., Krauthammer M., *Lost in Anonymization — A Data Anonymization Reference Classification Merging Legal and Technical Considerations*, The Journal of Law Medicine & Ethics, volume 48, questione 1, Marzo 2020, pag. 228

Voigt P., Von Dem Bussche A., *The EU General Data Protection Regulation (GDPR)*, Springer, 11 Novembre 2017

Wachter S., Mittelstadt B., Floridi L., *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, International Data Privacy Law, volume 7, numero 2, 2017, pag. 76

Wachter S., *Privacy: Primus Inter Pares — Privacy as a Precondition for Self-Development, Personal Fulfilment and the Free Enjoyment of Fundamental Human Rights*, 22 Gennaio 2017

Wachter S., *Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR*, Computer Law & Security Review, volume 34, 2018, pag. 436

Wachter S., *Affinity profiling and discrimination by association in online behavioural advertising*, Berkeley Technology Law Journal, volume 35, 2019

Wachter S., *Data Protection in the Age of Big Data*, Nature Electronics, volume. 2, Gennaio 2019

Warren S.D., Brandeis L.D., *The Right to Privacy*, in Harvard Law Review, volume. 4, numero 5, Dicembre 1890

Weber M., Lučić D., Lovrek I., *Internet of things context of the smart city*, 2017 International Conference on Smart Systems and Technologies (SST), 2017

Weber R. H., *Internet of things – New security and privacy challenges, in "Computer Law & Security Review"*, volume 26, numero 1, 2015, pag. 23

Weber R. H., *Internet of Things: Privacy issues revisited*, Computer law & security review, volume 31, 2015, pag. 618

Westin A. F., *Privacy and freedom*, Atheneum, New York, 1966

Wolters P. T. J., *The security of personal data under the GDPR: a harmonized duty or a shared responsibility?*, International Data Privacy Law, volume 7, numero 3, 2017, pag. 165

Wong B., *Problems with controller-based responsability in EU data protection law*, International Data Privacy Law, volume 11, numero 4, 2021

Wu J., Ping L., Ge X., Wang Y., Fu J., *Cloud Storage as the Infrastructure of Cloud Computing*, International Conference on Intelligent Computing and Cognitive Informatics, 2010

Yang Y., Wu L., Yin G., Li L., Zhao H., *A Survey on Security and Privacy Issues in Internet-of-Things*, IEEE Internet of Things Journal, volume 4, numero 5, Ottobre 2017

Zambrano V., *Il Comitato europeo per la protezione dei dati*, in Cuffaro V., D'Orazio R., Ricciuto V*., I dati personali nel diritto europeo*, Giappichelli, Torino, 2019

Zanfir-Fortuna G., *Article 82. Right to compensation and liability*, in Kuner C., Bygrave L. A., Docksey C., Drechsler L., *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford press, 13 Febbraio 2020

Zibuschka J., Kurowski S., Roßnagel H., Schunck C., Zimmermann C., *Anonymization Is Dead – Long Live Privacy*, Open Identity Summit, Marzo 2019.
Ziccardi G., Perri P. (a cura di), *Dizionario Legal tech*, Milano, 2020

Ziegler S. (edito da), *Internet of Things Security and Data Protection*, Springer, Ginevra, 2019

Zitouni M., Pan Q., Brulin D., Campo E., *Design of a Smart Sole with Advanced Fall Detection Algorithm*, Journal of Sensor Technology, volume 9, 2019, pag. 71

Zuboff S., *The age of surveillance capitalism*, PublicAffairs,15 Gennaio 2019, traduzione ad opera di Paolo Bassotti, Luiss University Press, Roma, 2019.

The Student Paper Series of the Trento LawTech Research Group is published since 2010

https://lawtech.jus.unitn.it/main-menu/paper-series/student-paper-series-of-the-trento-lawtech-research-group/2/

Freely downloadable papers already published:

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'EVA, MARTINA; DELMARCO, MARTINA; DELLA MURA, MARCO; DI MASCIO, FRANCESCA; FIUTEM, LORENZO; GENNARA, GIULIA; INNOCENTI, ALBERTO; LORIERI, ANNA; MAFFEI, BEATRICE; MARCOLINI, ALESSIA; MANZO, ARIANNA; MINERVINI, MONICA MARIA; MURESAN, ANAMARIA ELENA; NARDIN, NICOLÒ; PAISSAN, FILIPPO; PAISSAN, INGMAR; PANERO, MARTINA; PAVALEANU, CRISTIAN; RIZ, FRANCESCA; SCARSELLA, ALESSIA; SCODANIBBIO, GIULIA; SORRENTINO, MARIAROSA; TUCCI, GIULIANA; VIGNOLI, MARTINA; ZACCARIN, STEPHANIE; ZUCAL, SARA; IZZO, UMBERTO (a cura di) (2021), Diritto del turismo e Covid-19: cosa è cambiato nella seconda estate pandemica, Trento Law and Technology Research Group, Student Paper Series; 69. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-954-3

STUDENT PAPER N. 68

La protezione dei dati relativi alla salute nell'era dei Big Data. Un'analisi sulla sanità digitale in dialogo tra diritto e tecnologia

LIEVORE ANNA (2021), La protezione dei dati relativi alla salute nell'era dei Big Data. Un'analisi sulla sanità digitale in dialogo tra diritto e tecnologia, Trento Law and Technology Research Group, Student Paper Series; 68. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-903-1

STUDENT PAPER N. 67

«Cuius commoda, eius et incommoda»: l'art. 2049 del codice civile nella gig economy

PILZER LARA (2021), «Cuius commoda, eius et incommoda»: l'art. 2049 del codice civile nella gig economy, Trento Law and Technology Research Group, Student Paper Series; 67. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-946-8

STUDENT PAPER N. 66

La responsabilità sanitaria nel post Covid-19: scenari e proposte per affrontare il Contenzioso

PRIMICERI GIORGIA (2021), La responsabilità sanitaria nel post Covid-19: scenari e proposte per affrontare il contenzioso, Trento Law and Technology Research Group, Student Paper Series; 66. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-945-1

STUDENT PAPER N. 65

Legal design e sanità digitale: un innovativo approccio per favorire la tutela dei dati Personali

FRANCESCO TRAVERSO (2021), Legal design e sanità digitale: un innovativo approccio per favorire la tutela dei dati personali, Trento Law and Technology Research Group, Student Paper Series; 65. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-943-7

STUDENT PAPER N. 64

Sistemi decisionali automatizzati e tutela dei diritti: tra carenza di trasparenza ed esigenze di bilanciamento

IRENE TERENGHI (2021), Sistemi decisionali automatizzati e tutela dei diritti: tra carenza di trasparenza ed esigenze di bilanciamento, Trento Law and Technology Research Group. Student Paper Series; 64. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-942-0

STUDENT PAPER N. 63

Il disegno industriale e la moda tra disciplina dei disegni e modelli e normativa sul diritto d'autore

RUDIAN, MARGHERITA (2021), Il disegno industriale e la moda tra disciplina dei disegni e modelli e normativa sul diritto d'autore, Trento Law and Technology Research Group. Student Paper Series; 63. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-941-3

STUDENT PAPER N. 62

L'appropriazionismo artistico nell'arte visual: una comparazione tra Italia e Stati Uniti

DI NICOLA, LAURA (2021), L'appropriazionismo artistico nell'arte visual: una comparazione tra Italia e Stati Uniti, Trento Law and Technology Research Group. Student Paper Series; 62. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-940-6

STUDENT PAPER N. 61

Unfair trading practices in the business-to-business food supply chain between public and private regulation

BORGHETTO, MARIA VITTORIA (2020), Unfair trading practices in the business-to business food supply chain between public and private regulation, Trento Law and Technology Research Group. Student Paper Series; 61. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-933-8

STUDENT PAPER N. 60

PFAS e inquinamento delle falde acquifere venete: la tutela civilistica fra danno ambientale e azioni risarcitorie collettive

RAISA, VERONICA (2020), PFAS e inquinamento delle falde acquifere venete: la tutela civilistica fra danno ambientale e azioni risarcitorie collettive, Trento Law and Technology Research Group. Student Paper Series; 60. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-927-7

STUDENT PAPER N. 59

Il turismo alla prova del covid-19: una ricerca interdisciplinare: da quali dati partire e quali risposte dare alla più grande crisi che il comparto turistico abbia mai affrontato

UMBERTO IZZO (a cura di), Autori: ANDREATTA, GIULIA; ANDREOLI, ELISA; ARDU, SIMONE; BORTOLOTTO, FABIO; BRUZZO, PIERLUIGI; CALZOLARI, GIULIA; CAMPOS SANTOS, DIEGO; CARLINO, PIETRO; CAVALLERA, LORENZO; CEPPAROTTI, GIACOMO; CIABRELLI, ANTONIA; DALLE PALLE, GIORGIA; DAPRÀ, VALENTINA; DE SANTIS, DIEGO; FAVARO, SILVIA; FAVERO, ELEONORA; FERRARI, LAURA; GATTI, VERONICA; GAZZI, CHRISTIAN; GISMONDO, MARIANNA; GIUDICEANDREA, ANNA; GUIDA, GIOVANNI; INCARNATO, ANDREA; MARANER, ROBERTA; MICHELI, MARTA; ELENA MORARASU, LAURA; CHIARA NARDELLI, MARIA; PALLOTTA, EMANUELE; PANICHI, NICCOLÒ; PELLIZZARI, LAURA; PLAKSII, ANDRII; RANIERO, SAMANTHA; REGNO SIMONCINI, EMANUELE; RUSSO, SARA; SCHIAVONE, SARA; SERAFINO, ANTONIO; SILENZI, LUCA; TIRONZELLI, ELENA; PEGGY TSAFACK, CYNTHIA; VIGLIOTTI, AYLA; ZINETTI, GIULIA, Il turismo alla prova del Covid-19: una ricerca interdisciplinare: da quali dati partire e quali risposte dare alla più grande crisi che il comparto turistico abbia mai affrontato, Trento Law and Technology Research Group, Student Paper Series; 59. Trento: Università degli
Studi di Trento. 978-88-8443-903-1

STUDENT PAPER N. 58

La responsabilità dell'internet service provider alla luce della nuova direttiva sul diritto d'autore nel mercato unico digitale

CAMARELLA, LAURA (2020), La responsabilità dell'Internet Service Provider alla luce della nuova direttiva sul diritto d'autore nel mercato unico digitale, Student Paper Series; 58. Trento: Università degli Studi di Trento. 978-88-8443-893-5

STUDENT PAPER N. 57

Rischio idrogeologico e responsabilità civile

ROBERTI, CATERINA (2020), Rischio idrogeologico e responsabilità civile, Trento Law and Technology Research Group. Student Paper Series; 57. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-891-1

STUDENT PAPER N. 56

Assistente vocale e dati sanitari. Le sfide dell'intelligenza artificiale alla luce del Regolamento (UE) n. 2016/679

PETRUCCI, LIVIA (2020), Assistente vocale e dati sanitari. Le sfide dell'intelligenza artificiale alla luce del regolamento (UE) N. 2016/679, Trento Law and Technology Research Group. Student Paper Series; 56. Trento: Università degli Studi di Trento. ISBN: 978 88 8443 888 1

STUDENT PAPER N. 55

The Legal Dimension of Energy Security in EU Law

SCHMIEDHOFER, ANDREAS (2020), The legal dimensions of energy security in EU law, Trento Law and Technology Research Group. Student Paper Series; 55. Trento: Università degli Studi di Trento. ISBN: 978 88 8443 888 1

STUDENT PAPER N. 54

Macchine intelligenti che creano ed inventano. Profili e rilievi critici del nuovo rapporto tra intelligenza artificiale e diritti di proprietà intellettuale

TREVISANELLO, LAURA (2020), Macchine intelligenti che creano ed inventano. Profili e rilievi critici del nuovo rapporto tra intelligenza artificiale e diritti di proprietà intellettuale, Trento Law and Technology Research Group. Student Paper Series; 54. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-887-4

STUDENT PAPER N. 53

La protezione delle indicazioni geografiche: il sistema europeo e il sistema cinese a Confronto

COGO, MARTA (2019), La protezione delle indicazioni geografiche: il sistema europeo e il sistema cinese a confront, Trento Law and Technology Research Group. Student Paper Series; 53. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-856-0

STUDENT PAPER N. 52

Responsabilità civile e prevenzione dell'abuso interpersonale, fra molestie sessuali e Bullismo

PERETTI, FRANCESCA (2019), Responsabilità civile e prevenzione dell'abuso interpersonale, fra molestie sessuali e bullismo, Trento Law and Technology Research Group. Student Paper Series; 52. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-856-0

STUDENT PAPER N. 51

Blockchain, Smart Contract e diritto d'autore nel campo della musica

FAGLIA, FRANCESCO (2019), Blockchain, Smart Contract e diritto d'autore nel campo della musica, Trento Law and Technology Research Group. Student Paper Series; 51. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-855-3

STUDENT PAPER N. 50

Regole per l'innovazione: responsabilità civile e assicurazione di fronte all'auto a guida (progressivamente) autonoma

ZEMIGNANI, FILIPPO (2019), Regole per l'innovazione: responsabilità civile e assicurazione di fronte all'auto a guida (progressivamente) autonoma, Trento Law and Technology Research Group. Student Paper Series; 50. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-850-8

STUDENT PAPER N. 49

Unravelling the nexus between food systems and climate change: a legal analysis. A Plea for smart agriculture, a "new" organic agriculture and a wiser use of biotechnologies in the name of human rights protection

TELCH, ALESSANDRA (2019), Unravelling the nexus between food systems and climate change: a legal analysis. A Plea for smart agriculture, a "new" organic agriculture and a wiser use of biotechnologies in the name of human rights protection, Trento Law and Technology Research Group. Student Paper Series; 49. Trento: Università degli Studi di

Trento. ISBN: 978-88-8443-842-3

STUDENT PAPER N. 48

Wireless community networks e responsabilità extracontrattuale

VIDORNI, CHIARA (2019), Wireless community networks e responsabilità extracontrattuale, Trento Law and Technology Research Group. Student Paper Series; 48. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-841-6

STUDENT PAPER N. 47

Proprietà intellettuale e scienza aperta: il caso studio del Montreal Neurological Institute

CASSIN, GIOVANNA (2019), Proprietà intellettuale e scienza aperta: il caso studio del Montreal Neurological Institute, Trento Law and Technology Research Group. Student Paper Series; 47. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-835-5

STUDENT PAPER N. 46

Il "ciclista previdente" che si scontrò due volte: con un'auto e col principio indennitario applicato all'assicurazione infortuni

CHRISTOPH SIMON THUN HOHENSTEIN WELSPERG (2019), Il "ciclista previdente" che si scontrò due volte: con un'auto e col principio indennitario applicato all'assicurazione infortuni, Trento Law and Technology Research Group. Student Paper Series; 46. Trento:
Università degli Studi di Trento. ISBN: 978-88-8443-834 8

STUDENT PAPER N. 45

«Errare humanum est». L'errore nel diritto tra intenzionalità, razionalità ed emozioni

BENSALAH, LEILA (2018), «Errare humanum est». L'errore nel diritto tra intenzionalità, razionalità ed emozioni, Trento Law and Technology Research Group. Student Paper Series; 45. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-829-4

STUDENT PAPER N. 44

La gestione del rischio fitosanitario nel diritto agroalimentare europeo ed italiano: il caso Xylella

DE NOBILI, MARINA (2018), La gestione del rischio fitosanitario nel diritto

agroalimentare europeo ed italiano: il caso Xylella, Trento Law and Technology Research Group. Student Paper Series; 44. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-828-7

STUDENT PAPER N. 43

Mercato agroalimentare e disintermediazione: la dimensione giuridica della filiera Corta

ORLANDI, RICCARDO (2018), Mercato agroalimentare e disintermediazione: la dimensione giuridica della filiera corta, Trento Law and Technology Research Group. Student Paper Series; 43. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-827-0

STUDENT PAPER N. 42

Causa, meritevolezza degli interessi ed equilibrio contrattuale

PULEJO, CARLO ALBERTO (2018), Causa, meritevolezza degli interessi ed equilibrio contrattuale, Trento Law and Technology Research Group. Student Paper Series; 42. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-810-2

STUDENT PAPER N. 41

Graffiti, street art e diritto d'autore: un'analisi comparata

GIORDANI, LORENZA (2018), Graffiti, street art e diritto d'autore: un'analisi comparata, Trento Law and Technology Research Group. Student Paper Series; 41. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-809-6

STUDENT PAPER N. 40

Volo da diporto o sportivo e responsabilità civile per l'esercizio di attività pericolose

MAESTRINI, MATTIA (2018), Volo da diporto o sportivo e responsabilità civile per l'esercizio di attività pericolose, Trento Law and Technology Research Group. Student Paper Series; 40. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-784-6

STUDENT PAPER N. 39

"Attorno al cibo". Profili giuridici e sfide tecnologiche dello Smart Packaging in campo alimentare

BORDETTO, MATTEO (2018), "Attorno al cibo". Profili giuridici e sfide tecnologiche dello Smart Packaging in campo alimentare, Trento Law and Technology Research

Group. Student Paper Series; 39. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-795-2

STUDENT PAPER N. 38

Kitesurf e responsabilità civile

RUGGIERO, MARIA (2018), Kitesurf e responsabilità civile, Trento Law and Technology Research Group. Student Paper Series; 38. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-793-8

STUDENT PAPER N. 37

Giudicare e rispondere. La responsabilità civile per l'esercizio della giurisdizione in Italia, Israele e Spagna

MENEGHETTI HISKENS, SARA (2017), Giudicare e rispondere. La responsabilità civile per l'esercizio della giurisdizione in Italia, Israele e Spagna, Trento Law and Technology Research Group. Student Paper Series; 37. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-778-5

STUDENT PAPER N. 36

Il diritto in immersione: regole di sicurezza e responsabilità civile nella subacquea

CAPUZZO, MARTINA (2017), Il diritto in immersione: regole di sicurezza e responsabilità civile nella subacquea, Trento Law and Technology Research Group. Student Paper Series; 36. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-775-4

STUDENT PAPER N. 35

La privacy by design: un'analisi comparata nell'era digitale

BINCOLETTO, GIORGIA (2017), La privacy by design: un'analisi comparata nell'era digitale, Trento Law and Technology Research Group. Student Paper Series; 35. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-733-4

STUDENT PAPER N. 34

La dimensione giuridica del Terroir

BERTINATO, MATTEO (2017), La dimensione giuridica del Terroir, Trento Law and Technology Research Group. Student Paper Series; 34. Trento: Università degli Studi di

Trento. ISBN: 978-88-8443-728-0

STUDENT PAPER N. 33

La gravità del fatto nella commisurazione del danno non patrimoniale: un'indagine (anche) nella giurisprudenza di merito

MARISELLI, DAVIDE (2017), La gravità del fatto nella commisurazione del danno non patrimoniale: un'indagine (anche) nella giurisprudenza di merito, Trento Law and Technology Research Group. Student Paper Series; 33. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-727-3

STUDENT PAPER N. 32

«Edible insects». L'Entomofagia nel quadro delle nuove regole europee sui novel foods

TASINI, FEDERICO (2016), «Edible insects». L'Entomofagia nel quadro delle nuove regole europee sui novel foods = «Edible Insects»: Entomophagy in light of the new European Legislation on novel Foods, Trento Law and Technology Research Group. Student Paper Series; 32. Trento: Università degli Studi di Trento. ISBN 978-88-8443-709-9

STUDENT PAPER N. 31

L'insegnamento dello sci: responsabilità civile e assicurazione per danni ad allievi o a Terzi

TAUFER FRANCESCO (2016), L'insegnamento dello sci: responsabilità civile e assicurazione per danni ad allievi o a terzi, Trento Law and Technology Research Group. Student Paper Series; 31. Trento: Università degli Studi di Trento. ISBN 978-88-8443-697-9

STUDENT PAPER N. 30

Incrocio tra Contratti e Proprietà Intellettuale nella Innovazione Scientifica e tecnologica: il Modello del Consortium Agreement europeo

MAGGIOLO ANNA (2016), Incrocio tra Contratti e Proprietà Intellettuale nella Innovazione Scientifica e tecnologica: il Modello del Consortium Agreement europeo, Trento Law and Technology Research Group. Student Paper Series; 30. Trento: Università degli Studi di Trento. ISBN 978-88-8443-696-2

STUDENT PAPER N. 29

La neutralità della rete

BIASIN, ELISABETTA (2016) La neutralità della rete, Trento Law and Technology Research Group. Student Paper Series; 29. Trento: Università degli Studi di Trento. ISBN 978-88-8443-693-1

STUDENT PAPER N. 28

Negotiation Bases and Application Perspectives of TTIP with Reference to Food Law

ACERBI, GIOVANNI (2016) Negotiation Bases and Application Perspectives of TTIP with Reference to Food Law. The Trento Law and Technology Research Group. Student Paper Series; 28. Trento: Università degli Studi di Trento. ISBN 978-88-8443-563-7

STUDENT PAPER N. 27

Privacy and Health Data: A Comparative analysis

FOGLIA, CAROLINA (2016) Privacy and Health Data: A Comparative analysis. The Trento Law and Technology Research Group. Student Paper Series; 27. Trento: Università degli Studi di Trento. ISBN 978-88-8443-546-0

STUDENT PAPER N. 26

Big Data: Privacy and Intellectual Property in a Comparative Perspective

SARTORE, FEDERICO (2016) Big Data: Privacy and Intellectual Property in a Comparative Perspective. The Trento Law and Technology Research Group. Student Paper Series; 26. Trento: Università degli Studi di Trento. ISBN 978-88-8443-534-7

STUDENT PAPER N. 25

Leggere (nel)la giurisprudenza: 53 sentenze inedite in tema di responsabilità civile nelle analisi di 53 annotatori in formazione = Reading (in) the caselaw: 53 unpublished judgemnts dealing with civil liability law analyzed with annotations and comments by 53 students during their civil law course

REMO ANDREOLLI, DALILA MACCIONI, ALBERTO MANTOVANI, CHIARA MARCHETTO, MARIASOLE MASCHIO, GIULIA MASSIMO, ALICE MATTEOTTI, MICHELE MAZZETTI, PIERA MIGNEMI, CHIARA MILANESE, GIACOMO MINGARDO, ANNA LAURA MOGETTA, AMEDEO MONTI, SARA MORANDI, BENEDETTA MUNARI, EDOARDO NADALINI, SERENA NANNI, VANIA ODORIZZI, ANTONIA PALOMBELLA, EMANUELE PASTORINO, JULIA PAU, TOMMASO PEDRAZZANI, PATRIZIA PEDRETTI, VERA PERRICONE, BEATRICE PEVARELLO, LARA PIASERE, MARTA PILOTTO, MARCO POLI, ANNA POLITO, CARLO ALBERTO PULEJO, SILVIA RICCAMBONI, ROBERTA RICCHIUTI, LORENZO RICCO, ELEONORA RIGHI,

FRANCESCA RIGO, CHIARA ROMANO, ANTONIO ROSSI, ELEONORA ROTOLA, ALESSANDRO RUFFINI, DENISE SACCO, GIULIA SAKEZI, CHIARA SALATI, MATTEO SANTOMAURO, SILVIA SARTORI, ANGELA SETTE, BIANCA STELZER, GIORGIA TRENTINI, SILVIA TROVATO, GIULIA URBANIS, MARIA CRISTINA URBANO, NICOL VECCARO, VERONICA VILLOTTI, GIULIA VISENTINI, LETIZIA ZAVATTI, ELENA ZUCCHI (2016) Leggere (nel)la giurisprudenza: 53 sentenze inedite in tema di responsabilità civile nelle analisi di 53 annotatori in formazione = Reading (in) the caselaw: 53 unpublished judgemnts dealing with civil liability law analyzed with annotations and comments by 53 students during their civil law course. The Trento Law and Technology Research Group. Student Paper Series; 25. Trento: Università degli Studi di Trento. ISBN 978-88-8443-626-9

STUDENT PAPER N. 24

La digitalizzazione del prodotto difettoso: stampa 3D e responsabilità civile= The Digital Defective Product: 3D Product and Civil Liability

CAERAN, MIRCO (2016) La digitalizzazione del prodotto difettoso: stampa 3D e responsabilità civile = The Digital Defective Product: 3D Product and Civil Liability. The Trento Law and Technology Research Group. Student Paper Series; 24. Trento: Università degli Studi di Trento. ISBN 978-88-8443-663-4

STUDENT PAPER N. 23

La gestione della proprietà intellettuale nelle università australiane = Intellectual Property Management in Australian Universities

CHIARUTTINI, MARIA OTTAVIA (2015) La gestione della proprietà intellettuale nelle università australiane = Intellectual Property Management in Australian Universities. The Trento Law and Technology Research Group. Student Paper Series; 23. Trento: Università degli Studi di Trento. ISBN 978-88-8443-626-9

STUDENT PAPER N. 22

Trasferimento tecnologico e realtà locale: vecchie problematiche e nuove prospettive per una collaborazione tra università, industria e territorio = Technology Transfer and Regional Context: Old Problems and New Perspectives for a Sustainable Co-operation among Universitiy, Entrepreneurship and Local Economy

CALGARO, GIOVANNI (2013) Trasferimento tecnologico e realtà locale: vecchie problematiche e nuove prospettive per una collaborazione tra università, industria e territorio. The Trento Law and Technology Research Group. Student Paper Series; 22. Trento: Università degli Studi di Trento. ISBN 978-88-8443-525-5

STUDENT PAPER N. 21

La responsabilità dell'Internet Service Provider per violazione del diritto d'autore: un'analisi comparata = Internet Service Provider liability and copyright infringement: a comparative analysis

IMPERADORI, ROSSELLA (2014) *La responsabilità dell'Internet Service Provider per violazione del diritto d'autore: un'analisi comparata.* Trento Law and Technology Research Group. Student Paper; 21. Trento: Università degli Studi di Trento. ISBN 978-88-8443-572-9

STUDENT PAPER N. 20

Open innovation e patent: un'analisi comparata = Open innovation and patent: a comparative analysis

PONTI, STEFANIA (2014) *Open innovation e patent: un'analisi comparata.* The Trento Law and Technology Research Group. Student Paper Series; 20. Trento: Università degli Studi di Trento. ISBN 978-88-8443-573-6

STUDENT PAPER N. 19

La responsabilità civile nell'attività sciistica

CAPPA, MARISA (2014) La responsabilità civile nell'attività sciistica = Ski accidents and civil liability. Trento Law and Technology Research Group. Student Paper Series, 19. Trento: Università degli Studi di Trento.

STUDENT PAPER N. 18

Biodiversità agricola e tutela degli agricoltori dall'Hold-Up brevettuale: il caso degli OGM

TEBANO, GIANLUIGI (2014) Biodiversità agricola e tutela degli agricoltori dall'Hold-Up brevettuale: il caso degli OGM = Agricultural Biodiversity and the Protection of Farmers from patent Hold-Up: the case of GMOs. Trento Law and Technology Research Group. Student Paper Series; 18. Trento: Università degli Studi di Trento.

STUDENT PAPER N. 17

Produrre e nutrirsi "bio": analisi comparata del diritto degli alimenti biologici

MAFFEI, STEPHANIE (2013) Produrre e nutrirsi "bio" : analisi comparata del diritto degli alimenti biologici = Producing and Eating "Bio": A Comparative Analisys of the Law of Organic Food. Trento Law and Technology Research Group. Student Paper Series; 17. Trento: Università degli Studi di Trento.

STUDENT PAPER N. 16

La tutela delle indicazioni geografiche nel settore vitivinicolo: un'analisi comparata = The Protection of Geographical Indications in the Wine Sector: A Comparative 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).