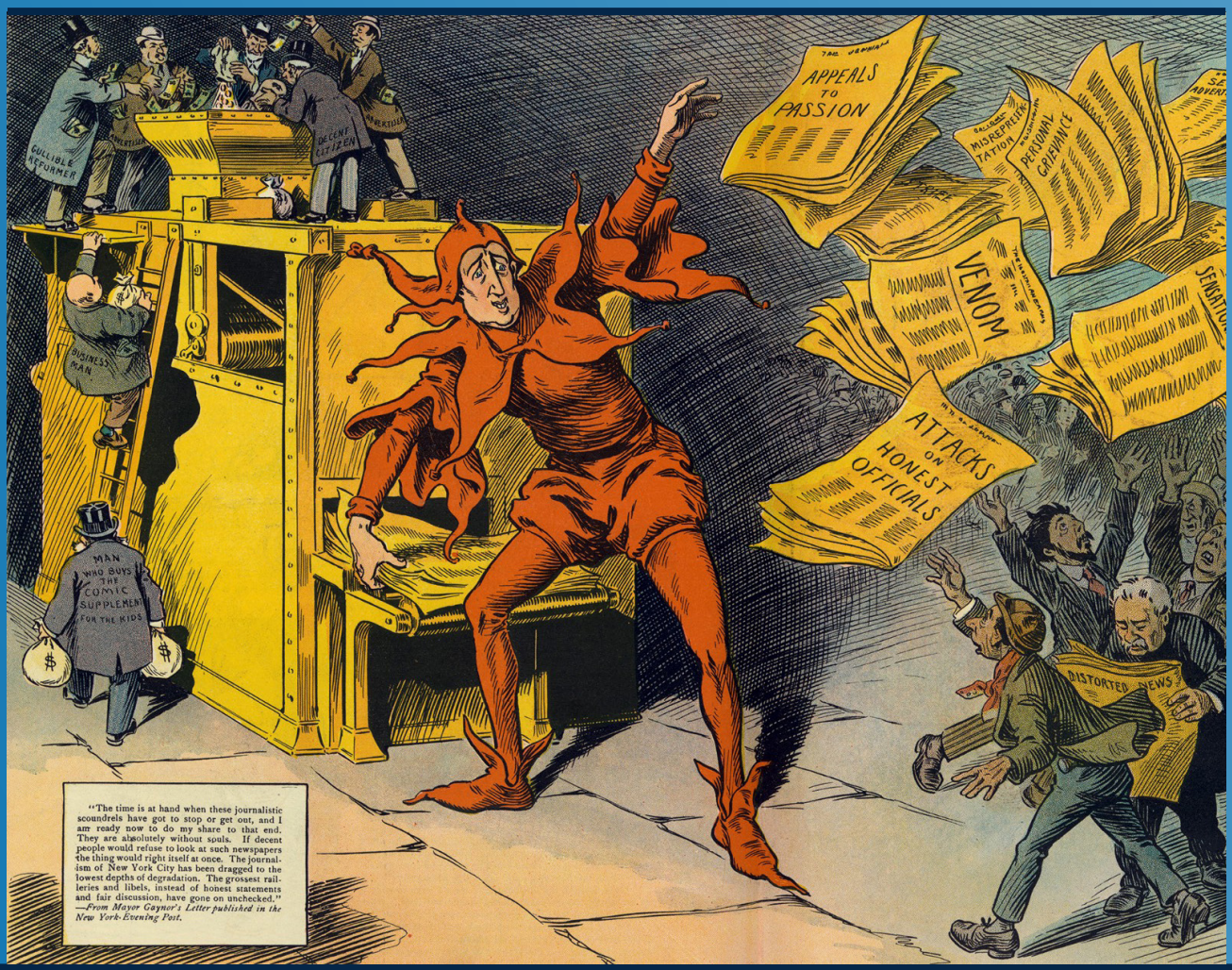
Paolo Guarda - Giorgia Bincoletto

Diritto comparato della privacy e della protezione dei dati personali



Ledizioni
The Innovative LEDIpublishing Company

Paolo Guarda - Giorgia Bincoletto

Diritto comparato della privacy e della protezione dei dati personali

Ledizioni

In copertina: The Yellow Press by L.M. Glackens (Library of Congress's Prints and Photographs division) - Pubblico dominio - Wikipedia

Paolo Guarda - Giorgia Bincoletto, *Diritto comparato della privacy e della protezione dei dati personali*
Ledizioni: marzo 2023.

ISBN cartaceo: 978-88-5526-886-8
ISBN versione ePub: 978-88-5526-887-5
ISBN PDF Open Access: 978-88-5526-888-2

Il volume è acquistabile nelle versioni ePub e cartacee sul sito Internet www.ledizioni.it, nelle librerie online o tradizionali.
Il PDF Open Access è scaricabile da DOAB (Directory Open Access Books) o dal sito www.ledizioni.it

Indice

Introduzione

«Da un grande potere derivano grandi responsabilità».

La celebre citazione tratta dalla saga di «Spiderman» può assurgere a frase paradigmatica per definire la disciplina apprestata dai vari ordinamenti giuridici al fine di regolare la tutela della privacy e dei dati personali.

La privacy nasce concettualmente alla fine del diciannovesimo secolo negli Stati Uniti allorquando Warren e Brandeis danno vita ad un sodalizio editoriale che cambierà il corso della storia (giuridica) e pubblicano il famoso articolo intitolato «The right to privacy» nell'ancor più celebre Harvard Law Review. Il motivo che spinge questi giuristi a scrivere sembra essere stato l'invasione da parte dei paparazzi della vita privata di Warren. Il contesto tecnologico nel contempo vede l'affermarsi di una nuova tecnologia, la «Kodak snap camera», che permette di scattare foto in modo «surrettizio». Un emergente modello di business trae da questa innovazione nuova linfa: ci si riferisce allo «yellow journalism», ovvero la stampa scandalistica. In questo contesto un nuovo interesse merita di assurgere al rango di diritto: *the right to be let alone*.

Il tempo corre, i casi giurisprudenziali si susseguono. Un'altra tecnologia fa la sua apparizione e il suo impatto cambierà completamente il mondo in cui ora viviamo. A partire dagli anni Settanta cominciano ad affermarsi e diffondersi i personal computer e con questi, dagli anni Novanta, il World Wide Web. La disponibilità di enormi basi di dati e di capacità computazionale sempre crescente spingono i legislatori nazionali a regolamentare il «trattamento» di dati che riguarda innegabilmente anche le vite delle persone. Inizia la storia della disciplina in materia di protezione dei dati personali.

Da un grande potere (tecnologico) derivano grandi responsabilità. È necessario che l'ordinamento giuridico codifichi ed imponga tali responsabilità ai soggetti che detengono il nuovo potere nell'era digitale.

Il diritto è obbligato a considerare l'uso e l'impatto delle tecnologie al fine di meglio governare i processi che caratterizzano la società. Le implicazioni della relazione tra diritto e tecnologia sono molteplici e la loro reciproca influenza biunivoca [Pascuzzi 2020, 17 ss. e Caso 2021,

61-72]. La tecnologia può modificare i contenuti degli interessi giuridici protetti. L'emersione di una nuova soluzione tecnica può trasformare uno scenario che in precedenza era ben definito. Nel momento in cui il progresso mette a disposizione dell'umanità nuove tecnologie è verosimile attendersi che queste ultime possano essere utilizzate dal diritto per perseguire obiettivi propri, con la conseguenza che ciò possa portare alla creazione di nuove regole o alla messa in discussione di quelle preesistenti. Le regole che derivano dalle tecnologie sono costruite attorno alle caratteristiche della tecnologia (vedi il diritto d'autore) e ciò determina la necessità di rimodulare i concetti che tradizionalmente vengono utilizzati.

Quest'opera si propone di esplorare le specificità della disciplina in materia di privacy e protezione dei dati personali, offrendo un approccio olistico che fa dell'interdisciplinarità il vero valore aggiunto e la necessaria chiave di lettura dei fenomeni in atto. Per realizzare questi obiettivi la comparazione rappresenta lo strumento metodologico principe. Il discorso sulla comparazione si caratterizza per diverse e peculiari letture ed interpretazioni volte a dar risposta alle tradizionali domande sul perché, sul come e sul cosa si compara [Resta, Somma, Zeno Zencovich 2020 e Sacco, Rossi 2019].

Per realizzare tale scopo occorre analizzare le risposte normative che i diversi ordinamenti giuridici hanno prospettato per fornire soluzioni affidanti a contesti simili. Oltre alle regole dell'ordinamento giuridico nazionale e dell'Unione europea, che ha svolto e svolge un ruolo chiave in materia di protezione dei dati personali, verranno perciò considerati altri sistemi, quali Canada, Francia, Regno Unito, Stati Uniti. La dimensione di protezione a livello nazionale è oggi alimentata dalle regole derivanti dal livello sovranazionale e dalla circolazione dei modelli in un contesto internazionale.

Ma questo non è sufficiente per comprendere appieno la complessità dei fenomeni. Altre scienze, altri saperi (informatico, biologico, economico, sociologico, ecc.) consegnano tanti piccoli tasselli dello stesso mosaico che il giurista è chiamato a ricomporre per riuscire a tracciare percorsi rivolti alla concretizzazione di obiettivi che realizzino gli interessi primari della società e, di conseguenza, degli individui che la compongono.

Se il diritto comparato propone una visione olistica dell'ordinamento giuridico, si è inevitabilmente portati a considerarlo immerso in un con-

testo sociale e intellettuale molto più ampio. Da questa prospettiva la comparazione può essere utilizzata per mettere in luce l'interazione fra contesti giuridici e non giuridici. Gli elementi «non giuridici» appunto divengono rilevanti anche per acquisire una più precisa comprensione del mondo giuridico. Eventuali differenze di carattere fattuale (tecnologico) possono essere utilizzate allo scopo di spiegare le differenze che sussistono nei problemi posti e nei risultati ottenuti [Dannemann 2019]. Il metodo «Law and Technology» (diritto e tecnologia) si occupa così del mutamento del diritto in connessione al cambiamento della tecnologia e della scienza, sempre più rapido nell'era digitale.

Quest'opera si inserisce nella collana inaugurata da Roberto Caso con il primo manuale «aperto» dal titolo «La società della mercificazione e della sorveglianza: dalla persona ai dati. Casi e problemi di diritto civile» pubblicato nel 2021 da Ledizioni. Da tale scritto il presente lavoro trae origine, impostazione e scelte metodologiche di fondo, tra cui il metodo casistico-problematico. Questo metodo richiede di inserire casi giurisprudenziali reali o casi immaginati dai docenti per apprendere il sapere dichiarativo e sviluppare alcune abilità, tra cui la formulazione e risoluzione di problemi giuridici grazie all'argomentazione, che cerca le regole rilevanti da applicare ai problemi. Occorre riferirsi al precedente manuale per gli approfondimenti in tema di metodo casistico-problematico [Caso 2021, Capitolo 1], di argomenti interpretativi [Capitolo 2], ossia degli schemi di discorso ricorrenti nei testi dei giuristi per giustificare una determinata interpretazione di un testo legislativo, di tecnica argomentativa del bilanciamento dei diritti [Capitolo 3], necessaria in presenza di più interessi in gioco e di tecniche per il reperimento delle informazioni giuridiche all'interno delle banche dati e dei siti web [Capitolo 5].

Il volume è diviso in due parti.

Una prima parte è dedicata alla disciplina «tradizionale» in materia di riservatezza e di protezione dei dati personali. Con il termine privacy, infatti, si dovrebbe comprendere sia la dimensione del diritto alla riservatezza, ossia alla protezione della vita privata e familiare, quale declinazione di un diritto della personalità dell'individuo, sia il diritto alla protezione dei dati personali, in altre parole il diritto al controllo dei dati personali. Alla luce dell'origine della privacy come «diritto ad essere lasciati soli» si utilizzerà questo termine per riferirsi alla prima dimensione. Al contempo, gli ordinamenti di common law utilizzano tale concetto

anche per la seconda accezione, a protezione delle informazioni personali. Perciò, per tali sistemi, si specificherà di volta in volta «privacy» e «informational privacy».

Non si è cercato, nella prima parte, il dettaglio dell'analisi del diritto positivo. Si è puntato, piuttosto, a fornire al lettore aspetti più generali, le ratio sottese all'istituto analizzato, anche al fine di dimostrare pregi e difetti della sua applicazione al mondo dei dati ed alla società dell'informazione. La prospettiva di partenza attorno alla quale è stata costruita la struttura logica ed espositiva dei contenuti di questi primi capitoli (salvo alcune parti esplicitamente dedicate ad altri contesti normativi) è quella dell'ordinamento dell'Unione europea (con alcuni approfondimenti verticali alle esperienze nazionali), in un costante dialogo con il sistema statunitense, modello privilegiato per l'analisi di soluzioni giuridiche che qui ci interessano, ma anche e soprattutto attore protagonista a livello globale per quel che concerne la creazione di banche dati e i trattamenti di dati personali e non.

Oltre all'analisi della disciplina tradizionale verranno approfonditi problemi di riservatezza e protezione dei dati personali in particolari contesti: il trasferimento internazionale dei dati, le comunicazioni elettroniche, il trattamento di dati in ambito di prevenzione, investigazione e repressione dei reati, il diritto all'oblio nelle sue varie declinazioni, l'uso di informazioni in un rapporto di lavoro, il danno e il suo risarcimento.

La seconda parte dell'opera, invece, affronta alcune tematiche specifiche e avanzate della nuova era tecnologica. Innanzitutto, sono state oggetto di approfondimento l'annosa questione relativa all'anonimizzazione e alla pseudonimizzazione dei dati, ed il fenomeno dei Big Data, il quale determina e condiziona altri contesti applicativi quali quello dell'intelligenza artificiale e dell'Internet delle cose. Tema rilevantissimo e di frontiera con riferimento al trattamento dei dati è, inoltre, quello rappresentato dalla sanità digitale della quale è stata proposta una descrizione relativamente ai diversi scenari applicativi ed alle connesse criticità giuridiche. Ampio spazio è stato dedicato al tema della ricerca scientifica, con particolare attenzione al contesto della ricerca medica, biomedica ed epidemiologica. Chiudono l'opera un approfondimento sulla blockchain e sulle forme di sorveglianza e controllo.

Come anticipato, il riferimento a casi (giurisprudenziali) reali o inventati è funzionale all'adozione del metodo casistico-problematico per in-

dividuare i problemi giuridici e potersi esercitare nella loro risoluzione. Molti capitoli della prima e della seconda parte così presentano uno o più fattispecie di origine giurisprudenziale, descrivono l'evoluzione della disciplina giuridica e si concludono con uno o più casi, lasciando agli studenti il compito di cercare e studiare le decisioni di riferimento. Talora, si aggiungono anche alcune domande a corredo della spiegazione. Altri capitoli contengono, invece, trattazioni più generali.

Il libro è corredato da una bibliografia con riferimenti essenziali e da un indice delle abbreviazioni e degli acronimi. Nel testo si troveranno anche diretti richiami alla normativa, alla dottrina e alla giurisprudenza con utilizzo dell'infratesto, riconoscibile perché composto da margini differenti. Si è scelto di limitare i riferimenti alla dottrina per fornire le coordinate indispensabili in un manuale senza eccedere con le note, doverose invece in altri contesti.

Fornire gli strumenti fondamentali per comprendere la privacy e la protezione dei dati personali è necessario oggigiorno non solo per introdurre un ambito così innovativo del diritto, ma anche per consentire di acquisire la corretta consapevolezza sui rischi che la società dell'informazione porta con sé.

Paolo Guarda
Giorgia Bincoletto

PARTE I
Il diritto alla riservatezza e il diritto alla protezione dei dati personali. Problemi tradizionali

CAPITOLO 1.
Il diritto alla privacy negli Stati Uniti d'America

Giorgia Bincoletto

1.1 L'origine del diritto alla privacy: the right to be let alone

Il diritto alla privacy è nato all'interno dell'ordinamento statunitense.

All'origine dell'esigenza di riconoscere questo nuovo diritto vi era il fenomeno del cd. «yellow journalism», una nuova tipologia di giornalismo basata sul sensazionalismo e sull'esagerazione nella scrittura delle notizie con dettagli intimi dei protagonisti per attirare il maggior numero di lettori possibile. Ciò era possibile anche grazie all'invenzione della macchina fotografica portatile, la «snap camera» della Eastman Kodak Company, che consentiva per la prima volta di ottenere istantanee sulla vita personale delle persone, più o meno note alla stampa.

Nel 1888, il giudice Cooley usava l'espressione *the right to be let alone* nel suo libro «Law of torts» per indicare l'aspettativa del singolo individuo a non subire interferenze nei suoi aspetti privati a scopo di gossip [Cooley 1888].

Nel 1890 Warren e Brandeis pubblicarono il celebre articolo «The Right to Privacy» sull'Harvard Law Review, coniando l'espressione per la quale sono oggi ricordati [Warren, Brandeis 1890]. Si tratta del più importante contributo mai scritto sulla privacy [Solove, Schwartz 2021, 10]. Questo saggio contiene la prima riflessione teorica volta a trovare una fonte ad un nuovo diritto alla privacy all'interno del sistema giuridico americano, non essendo presente alcun riferimento allo stesso nella Costituzione.

Come indicato da Solove e Schwartz, lo scritto potrebbe essere stato ispirato dalle vicende personali di Samuel Warren, importante avvocato di Boston, che aveva sposato Mabel Bayard, figlia di un senatore dello stato di Delaware. Warren e i suoi familiari erano divenuti oggetto di articoli scandalistici che riportavano le loro vicende personali «*in lurid detail*» nella *Saturday Evening Gazette* [Solove, Schwartz 2021, 12]. Infastidito da tali ricorrenti pubblicazioni, Warren decise di scrivere un contributo con l'amico e collega Louis Brandeis sulla possibilità di «essere lasciati soli» dalla stampa. Più tardi Brandeis diventerà giudice della Corte Suprema degli Stati Uniti.

In assenza di un'esplicita tutela all'interno dell'ordinamento giuridico, per poter sostenere l'esistenza di un right to privacy i due giuristi hanno dovuto interpretare le regole esistenti. Il punto di partenza dei due autori è il common law, che già allora proteggeva gli individui dalla pubblicazione illecita di manoscritti e opere d'arte, tramite il riconoscimento del copyright e del diritto di inedito. Questi due diritti consentivano al soggetto di determinare «to what extent his thoughts, sentiments, and emotions shall be communicated to other» [Warren, Brandeis 1890, 198]. Warren e Brandeis indagarono, in particolare, se tale prerogativa fosse paragonabile a ciò che il diritto di proprietà garantiva in termini di controllo su un bene materiale (p. 201):

> What is the nature, the basis, of this right to prevent the publication of manuscripts or works of art? It is stated to be the enforcement of a right of property; and no difficulty arises in accepting this view, so long as we have only to deal with the reproduction of literary and artistic compositions. They certainly possess many of the attributes of ordinary property: they are transferable; they have a value; and publication or reproduction is a use by which that value is realized. But where the value of the production is found not in the right to take the profits arising from publication, but in the peace of mind or the relief afforded by the ability to prevent any publication at all, it is difficult to regard the right as one of property, in the common acceptation of that term.

Gli esistenti rimedi di common law, perciò, proteggevano l'espressione artistica (la forma dell'idea), ma non potevano prevenire una pubblicazione o la descrizione di un fatto privato.

Di conseguenza, i *mental pain and distress* causati dalla pubblicazione di una lettera o di un fatto privato non avrebbero potuto trovare ristoro sulla base del copyright o del diritto di inedito. In aggiunta, operare un'analogia con il diritto di proprietà, legato concettualmente ad un bene materiale, non poteva garantire la possibilità di prevenire invasioni altrui in aspetti intimi, non tangibili della persona. Gli autori così argomentavano la necessità di utilizzare un diverso principio (pag. 205):

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

Esclusi i diritti di copyright, inedito e proprietà, il right to privacy potrebbe trovare fondamento nel principio di common law alla tutela di «un'inviolata personalità». Come si vedrà, il concetto di «personalità» avrà primaria importanza in Europa per il riconoscimento del diritto alla riservatezza [vedi → Capitolo 2]. La privacy, secondo i due celebri giuristi, consisterebbe non solo nella protezione degli scritti personali, ossia della corrispondenza, ma anche nel diritto di chi non è un soggetto pubblico di impedire che la stampa riporti affari privati (pag. 213).

Tuttavia, secondo gli autori non si trattava di diritto assoluto. Questo incontrava alcune limitazioni (pag. 214). In primo luogo, il diritto alla privacy non impediva la pubblicazione di fatti che erano di interesse pubblico, in quanto non potevano rimanere privati perché assumevano un'importanza per la società. La riservatezza di un fatto, perciò, dipendeva

dal soggetto a cui fosse riferito: se ad un individuo «privato», esso non avrebbe potuto essere divulgato, se invece questi fosse stato una persona pubblica o che svolgeva un compito sociale, sì. Il diritto proteggeva la cd. *private life* (pag. 215):

> In general, then, the matters of which the publication should be repressed may be described as those which concern the private life, habits, acts, and relations of an individual, and have no legitimate connection with his fitness for a public office which he seeks or for which he is suggested, or for any public or quasi public position which he seeks or for which he is suggested, and have no legitimate relation to or bearing upon any act done by him in a public or quasi public capacity.

Secondo Warren e Brandeis il secondo limite alla privacy riguardava l'applicazione della *law of slander and libel*. Il diritto ad essere lasciati soli non vietava la comunicazione di qualsiasi argomento, anche se di natura privata, quando la pubblicazione avveniva in circostanze legittime secondo la legge sulla calunnia e sulla diffamazione. In base a questa normativa, il diritto alla privacy non risultava violato se la pubblicazione avveniva in una corte di giustizia, da parte di organi legislativi, o in un contesto pubblico, quando fosse presente una possibilità di divulgazione lecita secondo le regole di common law (pag. 216).

Gli autori ritenevano, poi, che esistesse una terza limitazione: non avrebbe dovuto essere concesso alcun risarcimento per la violazione della privacy da parte di una pubblicazione orale che non causava uno *special damage*. Ciò per tutelare la libertà di manifestazione del pensiero (pag. 217).

Infine, il diritto alla privacy non si doveva riconoscere per la pubblicazione di fatti compiuta direttamente dall'individuo o con il suo consenso (p. 218).

Qualora la pubblicazione fosse comunque avvenuta, la verità dei fatti o l'assenza di malizia del giornalista o dell'editore non costituivano una difesa. I rimedi in caso di invasione della privacy, secondo i due giuristi, dovevano essere costituiti dall'*action of tort for damages*, volta a ottenere un ristoro monetario, o in una *injuction* per impedire nuove offese (pag. 219).

A partire da questo articolo la giurisprudenza ha iniziato a riconoscere il diritto alla privacy e alcuni stati hanno emanato degli *statute* per conferire delle *cause of action* specifiche in materia (ad es., lo stato di New York nel 1903 con il N.Y. Civil Rights Act) [Caso 2021, 173].

Il concetto di «inviolata personalità» non ha guadagnato attenzione nell'ordinamento statunitense, ma le parole di Warren e Brandeis hanno influenzato altri giuristi nel riconoscere e creare una specifica *common law tort action for privacy invasions* [Solove, Schwartz 2021, 24-27; vedi → Capitolo 11].

1.2 La protezione della privacy nella giurisprudenza statunitense

Nel 1960, dopo la diffusione del pensiero di Warren e Brandeis, il giurista William Prosser analizzò trecento casi giurisprudenziali riguardanti il right to privacy e classificò quattro *tort* che consentivano una tutela giurisdizionale in presenza di particolari violazioni del «diritto ad essere lasciati soli» [Prosser 1960 e Solove, Schwartz 2021, 27-34].

Questi quattro privacy *tort* sono stati ripresi anche nel Restatement (Second) of Torts del 1977, trattato pubblicato dall'American Law Institute (ALI):

– *intrusion upon seclusion or solitude, or into the plaintiff's private affairs*, *tort* che poteva essere invocato con riferimento alla divulgazione di informazioni veritiere riguardanti una persona, considerate imbarazzanti, molto offensive per una «reasonable person» e non di interesse pubblico, ottenute attraverso un'intrusione nello spazio privato del singolo. A titolo di esempio, nel caso *Hamberger v. Eastman* 206 A. 2d 239 (1964) la corte ha applicato il *tort* per l'installazione di un dispositivo nascosto da parte di un padrone di casa nella camera da letto di una coppia che vi alloggiava;
– *public disclosure of embarrassing private facts*, rimedio utilizzabile in caso di ottenimento di informazioni private, senza che ne venisse data pubblicità, quindi solo a livello visivo ed uditivo, e qualora le informazioni fossero considerate imbarazzanti e molto offensive per una «reasonable person». Nel caso *Barber v. Time Inc.*, 159 S.W.2d 291 (Mo. 1942) la corte ha ritenuto che la pubblicazione di un articolo con la foto di una donna, ricoverata in ospedale per un particolare

disturbo fisico e non personaggio pubblico, costituisse una violazione del suo diritto alla privacy;
– *appropriation of name or likeness*, *tort* che poteva tutelare il soggetto in caso di appropriazione ingiusta del suo nome o delle sue caratteristiche. Nel caso *Carson v. Here's Johnny Portable Toilets, Inc.*, 698 F.2d 831 (6th Cir. 1983) la corte ha riconosciuto la violazione della privacy per l'uso della frase «here's Johnny» di un personaggio famoso del «The Tonight Show» su servizi igienici portatili e senza il suo consenso;
– *false light in the public eye*, che consentiva di ottenere un rimedio in presenza di pubblicazione o divulgazione di fatti che ponevano il soggetto pubblicamente in una *false light*, come nel caso *Wood v. Hustler Magazine, Inc.*, 736 F.2d 1084 (1984) in cui una fotografia rubata di nudo era stata pubblicata su un giornale pornografico, senza verificare l'identità della persona ritratta quale modella. Questa figura è simile al concetto di civil law di diffamazione.

Questi primi *privacy tort* sono utilizzati ancora oggi nella giurisprudenza statunitense, quale parte fondamentale della *privacy protection in tort law*, a cui si sono aggiunti gli ulteriori rimedi di *defamation*, *breach of confidence*, *infliction of emotional distress* e il tradizionale *trespass* [vedi → Capitolo 11].

La Costituzione americana non menziona la privacy tra i diritti e le libertà tutelate nel Bill of Rights. Tuttavia, la giurisprudenza protegge questo diritto attraverso l'interpretazione di alcuni emendamenti e in presenza di alcune circostanze. In particolare, la privacy negli Stati Uniti si è evoluta a partire dall'utilizzo del Primo, Quarto, Quinto e Nono Emendamento:

> Amendment I: Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.
>
> Amendment IV: 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.
>
> Amendment V: No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offence to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.
>
> Amendment IX: The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people.

La protezione è stata riconosciuta gradualmente. In un primo momento, infatti, sembrava che gli emendamenti non potessero essere interpretati estensivamente, ossia oltre il dato letterale. Successivamente, la giurisprudenza ha iniziato ad utilizzare la *constitutional penumbral theory* che riconosceva nel testo costituzionale la possibilità di apertura a maggiori tutele, tra cui anche la protezione del right to privacy.

Nel 1928 il Giudice Holmes usava queste parole nella sua famosa *dissenting opinion* del caso della Corte Suprema *Olmstead v. United States* 277 U.S. 438 (1928):

> The protection guaranteed by the Amendments is much broader in scope. The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings, and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be let alone – the most comprehensive of rights, and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment. And

> the use, as evidence in a criminal proceeding, of facts ascertained by such intrusion must be deemed a violation of the Fifth. Applying to the Fourth and Fifth Amendments the established rule of construction, the defendants' objections to the evidence obtained by wiretapping must, in my opinion, be sustained. It is, of course, immaterial where the physical connection with the telephone wires leading into the defendants' premises was made. And it is also immaterial that the intrusion was in aid of law enforcement. Experience should teach us to be most on our guard to protect liberty when the Government's purposes are beneficent. Men born to freedom are naturally alert to repel invasion of their liberty by evil-minded rulers. The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well meaning but without understanding.

Il caso riguardava un contrabbandiere di alcolici, sospettato di aver violato il «Prohibition Act» allora in vigore nel paese. La polizia aveva intercettato le sue attività tramite degli strumenti di *wiretapping* posizionati nel sotterraneo di un edificio preposto ad ufficio e sulle linee di comunicazione sulla strada vicino alla sua abitazione. Il soggetto, agendo in giudizio, lamentava la violazione del Quarto Emendamento per l'invasione illegittima nelle sue comunicazioni private. Tuttavia, la Corte Suprema, chiamata a decidere sul punto, non ritenne che tale norma si applicasse al caso di specie perché non vi era stato un ingresso fisico nella casa di Olmstead, quanto piuttosto l'uso di strumenti all'esterno. Il Giudice Holmes, invece, avrebbe voluto ampliare la lettera del testo costituzionale a tutela del *right to be let alone* poiché il Quarto Emendamento, a suo dire, era stato previsto dai padri costituenti per assicurare la possibilità della «ricerca della felicità» del cittadino e in quanto tale poteva essere interpretato estensivamente anche per un'invasione non materiale e non fisica nella sfera di libertà dell'individuo.

La teoria delle *constitutional penumbras*, delle aree grigie di interpretazione costituzionale, è stata poi formalmente applicata nel caso *Griswold v. Connecticut*, 381 U.S. 479 (1965), riconoscendo una tutela alla «privacy coniugale» fondata sul Primo e sul Quattordicesimo Emendamento. Il caso riguardava due medici titolati di una clinica per il «controllo delle nascite» (*Planned Parenthood Center of New Haven*), la quale forniva informazioni sui sistemi di contraccezione alle coppie. Nello stato in cui operavano vigeva una legge che puniva chi faceva uso o agevolava

l'utilizzo di tali sistemi di controllo. I due venivano, quindi, sanzionati. A seguito di tale sanzione, i medici impugnavano il provvedimento ritenendo la legge incostituzionale e contraria, in particolare, al Primo e Quattordicesimo Emendamento. La Corte Suprema decideva per l'incostituzionalità della normativa statale, riconoscendo un diritto alla privacy nelle penombre del testo costituzionale, soprattutto con riferimento alla libertà delle scelte della vita privata coniugale.

Questa concezione della privacy è stata definita *decisional or reproductive privacy*: il diritto ad autodeterminarsi nelle scelte che riguardano la sfera personale [Solove 2002]. In un primo momento, con la sentenza *Roe v. Wade*, 410 U.S. 113 (1973) la Corte Suprema ha ritenuto che tale concezione della privacy ricomprendesse il diritto di una donna a terminare una gravidanza, statuendo, così, l'incostituzionalità di una legge texana che proibiva l'aborto.

Recentemente, la stessa Corte Suprema, pur supportando un *constitutional right to personal privacy*, ha, tuttavia, negato che tra le decisioni tutelabili vi sia tale prerogativa. Il celebre caso *Dobbs v. Jackson Women's Health Organization*, 945 F. 3d 265 (2022) è, perciò, un *overruling* di *Roe v. Wade* sul diritto all'aborto, indicando che per il riconoscimento tramite l'interpretazione degli Emendamenti è necessario verificare se la situazione giuridica posta all'esame della corte sia profondamente radicata nella storia e nella tradizione degli Stati Uniti [Palmieri, Pardolesi 2022]. Negando tale prospettiva, non è possibile il radicamento costituzionale del diritto all'aborto e i singoli Stati possono regolamentarlo e vietarlo.

Il Quarto Emendamento è stato successivamente impiegato per proteggere i cittadini da invasioni anche non «fisiche» della loro abitazione, operate attraverso intercettazioni o sistemi di sorveglianza (sulla scia di quanto anticipato dal Giudice Holmes nel 1928) [Solove, Schwartz 2021, 277-299].

Nel caso *Katz v. United States*, 389 U.S. 347 (1967) la Corte Suprema ha ritenuto che l'uso di un *telephone bug* da parte dell'FBI in una cabina telefonica pubblica per indagare su scommesse illecite fosse illegittimo perché il Quarto Emendamento proteggerebbe la privacy delle persone, e non dei luoghi, dalle invasioni dello Stato, in assenza di un valido mandato di perquisizione. Katz poteva ragionevolmente aspettarsi di non essere ascoltato nelle sue comunicazioni effettuate dalla cabina. Questo caso rappresenta l'*overruling* di *Olmstead v. United States*. Tuttavia,

la Corte non riconobbe un «general constitutional right to privacy», ma una «individual privacy against certain kind of governmental intrusion». Nella *concurring opinion* del Giudice Harlan comparve per la prima volta il concetto di «reasonable expectation of privacy» [Solove, Schwartz 2021, 290-291]. Secondo questa opinione era ragionevole ritenere che una casa è un luogo in cui ci si aspetta di avere privacy, mentre le attività compiute all'esterno *in plain view* non avrebbero avuto la stessa aspettativa. Il discrimine per le comunicazioni era il trovarsi in un luogo che è «temporarily private place whose momentary occupants' expectations of freedom from intrusion are recognized as reasonable». Il *reasonable expectation of privacy test* era così composto:

– l'esistenza di una soggettiva e attuale aspettativa di privacy;
– la corrispondenza tra questa aspettativa e quella che la società è pronta a riconoscere come ragionevole.

Perciò, il Quarto Emendamento non tutelerebbe l'aspettativa di privacy che solo un criminale ritiene di avere, ma quella ragionevole di una persona comune.

Il test di «ragionevole aspettativa della privacy» è stato in seguito limitato dalla *third party doctrine*: la comunicazione di alcune informazioni senza mandato all'autorità pubblica non violerebbe la privacy quando queste informazioni sono già state fornite volontariamente dal soggetto a terzi, come banche, compagnie telefoniche, fornitori di servizi Internet, non essendoci un'oggettiva «ragionevole aspettativa di privacy» su tali informazioni [Solove, Schwartz 2021, 299-310]. Questo approccio è stato criticato sia dalla dottrina che dalla giurisprudenza, che però in alcuni casi applica la limitazione di tutela. La *third party doctrine* circoscrive di fatto la protezione ad aspetti mai divulgati all'esterno; in ogni caso, in alcune circostanze potrebbero essere invocati i diritti derivanti dalla *informational privacy* [vedi *infra*], piuttosto che l'interpretazione della carta costituzionale su cui si basa il test di «reasonable expectation of privacy».

Nel 2001 la Corte Suprema utilizza questo test nel caso *Kyllo v. United States*, 533 U.S. 27 (2001) per stabilire che il requisito del mandato richiesto da Quarto Emendamento deve essere presente sin dall'utilizzo dello strumento tecnologico che invade la privacy del cittadino. In questo caso, infatti, la polizia aveva ottenuto delle immagini termografiche

della casa di Kyllo senza un mandato, sospettando che coltivasse marijuana. Nonostante i sospetti fossero fondati, come verificato una volta all'interno dell'abitazione con un legittimo mandato, l'intrusione della polizia è stata considerata in violazione della Costituzione perché il soggetto poteva ragionevolmente aspettarsi di non essere sorvegliato tramite un *thermal-imaging device*, prima che fosse stato emesso un mandato. In altre parole, la giustificazione all'intrusione deve essere valida fin dal principio.

Anche l'adozione di sistemi di videosorveglianza o geolocalizzazione deve limitarsi a quanto formalmente autorizzato. Nel caso *U.S. v. Jones*, 132 S. Ct. 945 (2012) la Corte Suprema ha ritenuto che l'utilizzo di un *global-positioning system tracking device* sull'auto di un individuo fosse soggetto ai limiti del Quarto Emendamento perché la vettura di proprietà è un luogo fisico in cui si potrebbe avere una ragionevole aspettativa di privacy.

Nel caso *Riley v. California*, 136 S. Ct. 506 (2015), invece, la Corte ha considerato una violazione del Quarto Emendamento e del diritto alla privacy l'analisi del traffico di un cellulare ottenuto tramite una perquisizione. Il soggetto era stato fermato mentre si trovava in macchina per violazione del codice della strada. Ispezionando anche il suo cellulare la polizia scoprì la sua appartenenza ad un gruppo che era stato coinvolto in una sparatoria, decidendo di incriminare Riley anche per altri reati. Ebbene, la Corte Suprema considerò illegittima la raccolta delle informazioni dal cellulare perché anche un uomo arrestato poteva avere la ragionevole aspettativa che il suo telefono non fosse perquisito senza uno specifico mandato. Secondo la Corte le informazioni presenti in un cellulare possono persino essere particolarmente sensibili. Le perquisizioni non saranno sempre illegittime, ma servirà un adeguato mandato per effettuarle. Ciò a meno che non esistano particolari eccezioni previste nell'ordinamento che escludano la necessità di una tale richiesta (ad es., per finalità specifiche previste da una normativa di settore).

Peraltro, anche l'accesso a registri storici sui dati delle comunicazioni tramite cellulare (*cell phone signals*) deve essere tutelato e valutato con il test della *reasonable expectation of privacy* (*Carpenter v. United States*, 138 S. Ct. 2206 (2018), peraltro critica nei confronti della *third party doctrine*). Come si vedrà, questo concetto e il test sono stati impiegati anche in altri sistemi di common law [vedi → Capitolo 5].

La tutela alla privacy fornita dall'interpretazione degli Emendamenti è limitata al rapporto pubblico-privato e così alle violazioni compiute da un'autorità. Con riferimento al rapporto tra privati, le tutele sono previste a livello legislativo, sia federale che statale [vedi *infra*].

È comunque necessario segnalare che in alcuni stati la tutela del right to privacy è stata esplicitamente inserita a livello costituzionale. È il caso, ad esempio, della California che all'art. 1, § 1, della Costituzione prevede che «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». Quest'ultima viene, ancora una volta, in modo evocativo accostata al concetto di raggiungimento della felicità.

1.3 *Informational privacy*

Negli anni Sessanta e Settanta l'invenzione del calcolatore ha aumentato il dibattito in materia di privacy [sul processo di evoluzione vedi → Capitolo 3].

Nel 1973, l'Education & Welfare US Department of Health degli Stati Uniti definì alcuni principi, i Fair Information Practices, applicabili a tutti i processi di utilizzo automatizzato di *personal information* alla luce dell'evoluzione tecnologica in corso:

> 1. There must be no personal-data record-keeping systems whose very existence is secret;
> 2. There must be a way for an individual to find out what information about him is in a record and how it is used;
> 3. There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent;
> 4. There must be a way for an individual to correct or amend a record of identifiable information about him;
> 5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data.

I Fair Information Practices richiedevano, quindi, la trasparenza nell'utilizzo delle informazioni, implicavano l'esistenza di una finalità per l'uso delle stesse, riconoscevano il diritto alla correzione e imponevano requisiti di sicurezza per i sistemi utilizzati.

Questi principi sono divenuti punti di riferimento sia per l'emanazione di normative negli Stati Uniti, sia a livello internazionale per la definizione delle regole a protezione dei dati personali [vedi → Capitoli 4 e 5].

Il concetto di *informational privacy* fece capolino nella giurisprudenza nel caso *Whalen v. Roe*, 429 U.S. 589 (1977) in cui la Corte Suprema si occupò della validità di una legge dello Stato di New York che imponeva l'archiviazione di informazioni sull'acquisto di farmaci. In questo caso la Corte usò l'espressione di *constitutional right to informational privacy* come volto alla protezione di due interessi: «the individual interest in avoiding discousure of personal matters» e «the interest in independence in making certain kinds of important decisions». Non si tratterebbe, dunque, solo di un controllo su ciò che viene divulgato all'esterno, ma anche della protezione a compiere delle scelte personali sulle proprie informazioni.

Nello stesso anno la Corte Suprema non ha riconosciuto questo diritto a Nixon, in quanto i Nixon's papers non potevano essere considerati privati (*Nixon v. Administrator of General Services*, 433 U.S. 425 (1977).

Nonostante l'utilizzo di tale espressione nella giurisprudenza successiva, anche a livello statale, nel 2011 la Corte Suprema ha dubitato dell'esistenza di un «constitutional right to informational privacy» (*National Aeronautics and Space Administration v. Nelson*, 131 S. Ct. 746 (2011)). In particolare, la Corte ribadisce l'esistenza di un «individual interest in avoiding disclosure of personal matters» e riconosce la tutela della privacy a livello costituzionale grazie all'interpretazione degli Emendamenti, ma non ritiene sussistente un'identità separata all'*informational privacy* [Solove, Schwartz 2021, 587].

La nozione di *personal identifiable information* o *personal information* non è equivalente a quella di dato personale. Come si vedrà, nel diritto europeo il dato personale è definito come «qualsiasi informazione riguardante una persona fisica identificata o identificabile» direttamente o indirettamente (art. 4, pt. 1, GDPR). La *personal information*, invece, non è circoscritta in modo univoco. In generale, è possibile affermare che un'informazione è personale se è collegata ad una persona identi-

ficata [Solove, Schwartz 2014]. Rimarrebbe esclusa l'indiretta identificazione. La differenza tra le definizioni non è di poco conto, dal momento che la nozione europea appare più ampia di quella statunitense. Le tutele, perciò, differirebbero per l'oggetto e i due termini (dato personale e *personal information*) non dovrebbero essere trattati come sinonimi. Ciò rileva anche con riferimento ai meccanismi per il trasferimento transfrontaliero delle informazioni perché l'ordinamento statunitense non proteggerebbe le informazioni che possono indirettamente identificare un individuo [sui meccanismi, vedi → Capitolo 6].

La disciplina dell'*informational privacy* è frammentata, settoriale e la legislazione è spesso legata a situazioni emergenziali [Giovanella 2017, 153]. Secondo gli stessi giuristi statunitensi la *data privacy law* è un «bewildering assortment of numerous federal and state laws that differ significantly from each other» [Solove, Schwartz 2022].

A partire dagli anni Settanta sono stati emanati vari *statute* o *act* che regolano precisi ambiti di trattamento delle *personal information* sia a livello federale che statale. Con riferimento al primo livello si segnalano, in ordine temporale [Solove, Schwartz 2021]:

– Fair Credit Reporting Act del 1970, dedicato all'ambito delle agenzie di credito;
– Privacy Act del 1974, che disciplina il trattamento di informazioni raccolte in banche dati di agenzie federali e che adotta i Fair Information Practices, prevedendo come regola di base il consenso del soggetto e varie eccezioni che non lo richiedono, come nel caso di esigenze di giustizia o per uso di routine. Questa normativa è considerata una risposta al «Watergate scandal» avvenuto sotto la presidenza Nixon [Giovanella 2017, 154];
– Family Educational Rights and Privacy Act del 1974 per la protezione dei registri scolastici;
– Right to Financial Privacy Act del 1978, che richiede un mandato per l'accesso ai registri finanziari privati;
– Foreing Intelligence Surveillance Act (FISA) del 1978, disciplinante le agenzie di intelligence e le loro attività sulle informazioni provenienti dall'estero. Quest'ultimo atto è stato modificato nel 2008 e nel 2012 e governa l'accesso alle informazioni da parte delle agenzie di intelligence [su questa normativa e le questioni relative al trasferimento transfrontaliero vedi → Capitolo 6];

- Privacy Protection Act del 1980, riferito all'ambito giornalistico ed editoriale;
- Cable Communications Policy Act del 1984, che riguarda i registri detenuti dalle società televisive;
- Electronic Communications Privacy Act del 1986, che ha previsto tutela rispetto alla Federal electronic surveillance law, la quale consente l'utilizzo delle informazioni sulle comunicazioni per finalità di sorveglianza e tramite sistemi tecnologici;
- Computer Matching and Privacy Protection Act del 1988, dedicato alle investigazioni compiute da agenzie federali su documenti contenuti proprio nei computer;
- Employee Polygraph Protection Act del 1988, che governa l'utilizzo del poligrafo da parte dei dipendenti;
- Video Privacy Protection Act del 1988, che riguarda le informazioni nel contesto del noleggio di videocassette ed è stato modificato nel 2012;
- Telephone Consumer Protection Act del 1991, che fornisce alcuni rimedi in caso di telemarketing;
- Driver's Privacy Protection Act del 1994, che impedisce di comunicare o vendere le informazioni sui registri della motorizzazione;
- Health Insurance Portability and Accountability Act (HIPAA) del 1996, che costituisce la normativa chiave in materia di utilizzo di informazioni sanitarie, fornendo anche dei requisiti sia tecnici che organizzativi per i trattamenti, ma che si applica solo ad una serie di entità legate alla sanità. Peraltro, la nozione di «personal health information» è molto vicina a quella europea di «dato relativo alla salute» [Bincoletto, 2021a, 318-327; sulla definizione europea vedi → Capitolo 3];
- Identity Theft and Assumption Deterrence Act del 1998, che criminalizza alcuni usi di informazioni, come in caso di furto d'identità;
- Children's Online Privacy Act del 1998, che limita l'utilizzo di informazioni di minori sotto gli anni 13 da parte dei siti Internet se raccolte a partire dagli stessi minori;
- Gramm-Leach-Bliley Act del 1999, che richiede un'*information policy* per i soggetti in caso di comunicazione di informazioni da parte di istituzioni finanziarie ad altre società;
- USA Patriot Act del 2001, che è stato emanato a seguito dell'attacco alle torri gemelle e consente il trattamento e così la sorveglianza di informazioni per esigenze di sicurezza nazionale con lo scopo di pre-

venire attacchi terroristici e in presenza di una *reasonable cause* per l'accesso. Tra le agenzie che possono accedere a tali informazioni vi sono l'FBI (*Federal Bureau of Investigation*), la CIA (*Central Intelligence Agency*), la NSA (*National Security Agency*) e l'ODNI (*The Office of the Director of National Intelligence*);
– CAN-SPAM Act del 2003, disciplinante sanzioni in caso di invio di comunicazioni indesiderate nella casella di posta elettronica [su questo settore e il fenomeno *spam* vedi → Capitolo 7];
– Fair and Accurate Credit Transactions Act del 2003, dedicato alla protezione dei cittadini in caso di furto d'identità;
– Video Voyeurism Prevention Act del 2004, che criminalizza l'utilizzo di immagini di nudo in presenza di una «ragionevole aspettativa di privacy»;
– Health Information Technology for Economic and Clinical Health Act (HITECH Act) del 2009, che riguarda aspetti di sanità elettronica e che ha modificato la HIPAA [Bincoletto 2021a, 327-329].

Anche a livello statale la protezione è settoriale. Tra tutti la California ha svolto un ruolo chiave, quale «privacy superregulator, catalyzing privacy laws in the United States» [Chander et al. 2021]. Il California Consumer Privacy Act (CCPA) è stato emanato nel 2018, ma divenuto applicabile dal 2020. Esso rappresenta «one of the strongest state privacy laws in the United States», superando molte delle leggi federali sopra richiamate [Solove, Schwartz 2021, 970-973]. Il CCPA deve essere rispettato da tutte le società che raccolgono e conservano informazioni di cittadini californiani per finalità commerciali e i) conseguono annualmente degli utili superiori a 25 milioni di dollari, ii) trattano informazioni di più di 50.000 californiani su base annuale, iii) ottengono almeno il 50% degli utili annuali dalla vendita di informazioni di californiani. La normativa non si applica, invece, a banche, società di brokeraggio, assicurazioni e agenzie di credito soggette alla regolazione federale. Anche alcuni trattamenti in ambito sanitario sono esclusi dall'ambito materiale.

Il CCPA è stato inserito all'interno del Civil Code, nella Part 4, Title 1.81.5. Questa normativa prevede alcuni diritti in capo al consumatore, tra cui:
– il diritto a ricevere informazioni sulle categorie di *personal information* raccolte, sulla finalità dell'uso, sui diritti che possono essere invocati.

Le informazioni saranno indicate all'interno di una apposita *privacy policy*;
- il diritto a ricevere informazioni sulle comunicazioni a terze parti;
- il diritto a modificare le informazioni non più corrette;
- il diritto alla cancellazione e alla portabilità delle informazioni;
- il diritto di opt-out alla vendita delle informazioni a terze parti.

Non sono, invece, presenti principi generali per il trattamento delle informazioni, ma vari obblighi in capo al soggetto commerciale che raccoglie i dati, tra cui doveri informativi, limitazioni dell'uso alla finalità della raccolta, obblighi di concludere degli accordi con le terze parti che ricevono le informazioni o con i soggetti che le trattano per suo conto, e l'implementazione di misure di sicurezza (Section 1798.100).

In generale, l'approccio alla tutela delle informazioni è basato sul meccanismo *notice and choice*, ossia sul consenso dell'individuo a seguito di brevi informazioni. Non è prevista la nozione di base giuridica del trattamento, tipica del contesto europeo.

Nell'ordinamento statunitense non è stata emanata una normativa omnicomprensiva sulla protezione dei dati personali, come avvenuto, invece, nell'UE [vedi → Capitolo 3]. L'American Law Institute ha spiegato che applicare l'approccio normativo europeo sarebbe in conflitto con troppi *statute* e incompatibile con alcuni valori americani. Ha così proposto una serie di principi generali che possano modernizzare l'*information privacy* anche alla luce di regole presenti in altri contesti giuridici, prendendo le mosse dai Fair Information Practices [Solove, Schwartz 2022; vedi → Capitolo 4]. Propone, tra l'altro, di utilizzare la nozione di *personal data* («any data that is identified or identifiable to a specific living individual») per armonizzare il concetto statunitense con quello presente a livello internazionale.

Il sistema federale, inoltre, non ha previsto un organismo indipendente dedicato esclusivamente alla protezione della privacy o alle problematiche di regolamentazione di Internet. Tuttavia, la Federal Trade Commission degli Stati Uniti ha assunto dei compiti di sorveglianza e da qualche anno svolge anche un ruolo regolatorio che va ben oltre la vigilanza a cui è preposta [Bincoletto 2019, 55]. La determinazione delle pratiche commerciali scorrette e dannose per la privacy dei consumatori statunitensi è contenuta in vari Report e negli ordini a carattere inibitorio disposti nei

procedimenti contenziosi promossi dall'agenzia ai sensi della Section 5 del Federal Trade Commission Act[1].

Si segnala comunque la proposta di un generale American Data Privacy and Protection Act (H.R. 8152) introdotta presso la Camera dei Rappresentanti nell'ottobre 2022 «to provide consumers with foundational data privacy rights, create strong oversight mechanisms, and establish mea-ningful enforcement». Attualmente il diritto alla privacy negli Stati Uniti incorpora diverse dimensioni [Solove 2002]:

– *right to be let alone* di Warren e Brandeis;
– *limited access to the self*, ossia la capacità di proteggersi da accessi indesiderati da parte di altri;
– *secrecy*, cioè l'occultamento di determinate questioni agli occhi altrui, nella dimensione pubblico-privato;
– *control over personal information*, ossia la privacy informativa;
– *personhood*, la protezione della propria personalità, individualità e dignità;
– e *intimacy*, cioè il controllo o l'accesso limitato alle relazioni intime o agli aspetti della vita privata.

Secondo Solove, per definire la privacy è necessario un approccio empirico che valuti le pratiche sociali in essere e trovi i meccanismi di tutela rispetto alle possibili intrusioni del prossimo [Solove 2006]. Secondo DeVries, invece, il diritto può essere suddiviso in sole due dimensioni: «the traditional physical and decisional "right to be let alone"» e «the more recent notion of control over (or rights concerning) personal information» [DeVries 2003].

In passato era sufficiente proteggere l'intimità privata nel domicilio; in seguito, con la rivoluzione tecnologica, le barriere sono divenute immateriali [Lessig 1999]. Dall'analisi di problemi tradizionali si giungerà all'approfondimento delle sfide dell'era digitale.

1 Si v. il sito ufficiale in https://www.ftc.gov/.

CAPITOLO 2.
Il diritto alla riservatezza nell'ordinamento italiano ed europeo

Giorgia Bincoletto

2.1 La categoria dei diritti della personalità

Con riferimento all'ordinamento italiano ed europeo la nozione di privacy e la sua tutela comprendono due diverse dimensioni:
– il diritto alla riservatezza, ossia alla protezione della vita privata e familiare, della sfera personale più intima e personale dell'individuo;
– il diritto alla protezione dei dati personali vale a dire il diritto alla titolarità dei dati personali e alla loro protezione [Tosi 2019, 29].

Questo capitolo si concentrerà sulla prima dimensione, ricostruendone le origini e tracciandone l'evoluzione nei sistemi giuridici italiano ed europeo. L'elaborazione dottrinale e giurisprudenziale relativa ai diritti della personalità rappresenterà il necessario punto di partenza.

Nessuna norma positiva dei sistemi vigenti contiene una definizione di questa categoria di diritti fondamentali. La concettualizzazione è stata oggetto di discussione dottrinale. Secondo Resta, la nozione si riferisce ad una formula che ha avuto origine nell'ambito degli ordinamenti di civil law, diffondendosi poi in altre tradizioni giuridiche, come i sistemi misti del Québec e della Luisiana, per indicare una tipologia di diritti soggettivi dotati di caratteristiche tendenzialmente omologhe, tra cui l'assolutezza, l'imprescrittibilità, l'inalienabilità, l'irrinunziabilità, l'indisponibilità e l'intrasmissibilità, e a cui è possibile riferire uno specifico modello di tutela civile della sfera personale, nella sua dimensione corporea e immateriale

[Alpa, Resta 2019, 145-151]. I diritti della personalità avrebbero, dunque, connotati antitetici rispetto ai diritti patrimoniali [Resta 2014, 73].

Questa categoria dogmatica non è traducibile nei sistemi di common law, in cui la tutela della persona è piuttosto ricompresa nella nozione di privacy e azionata tramite i vari *tort*. Anche per questa ragione è opportuno specificare che la parola privacy non necessariamente coincide con «riservatezza», ma potrebbe riferirsi alla dimensione a protezione delle informazioni. Il comparatista, perciò, dovrà di volta in volta differenziare i termini tra *privacy* e *information privacy* o *digital privacy*.

La tradizione civilistica dell'Europa continentale ha iniziato a riflettere sulla categoria concettuale dei diritti della personalità sin da fine Ottocento. La pandettistica tedesca (Gareis, Kohler e von Gierke), l'attività giurisdizionale delle corti francesi, ma anche la dottrina italiana (Fadda, Bensa, Scialoja, Ravà), hanno per decenni elaborato varie nozioni relative agli attributi della personalità e alle possibili forme di tutela [Alpa, Resta 2019]. I primi diritti ad essere riconosciuti furono il diritto al nome, all'onore, all'immagine e il diritto morale d'autore. La tutela veniva connessa ai rimedi allora esistenti per il danno non patrimoniale, ossia alla tutela inibitoria e risarcitoria.

I fondamenti normativi dei diritti della personalità sono stati, poi, tipizzati in disposizioni legislative, come nelle leggi sul diritto d'autore, in leggi penali e speciali, ma anche all'interno dei codici civili, tra cui il BGB tedesco (§ 12 sul nome come diritto della persona) e il Codice Civile italiano del 1942 (art. 5 sull'integrità del corpo, artt. 6-9 sul diritto al nome e allo pseudonimo, art. 10 sull'immagine). Il diritto positivo rimase inevitabilmente parziale e incompleto.

La Dichiarazione universale dei diritti dell'uomo dell'Organizzazione delle Nazioni Unite (ONU) del 1948 ha poi universalmente affermato il valore fondamentale della persona umana riconoscendone libertà e diritti e proteggendola da interferenze arbitrarie nella vita privata, nella famiglia, nella casa, e nella corrispondenza (art. 12).

Nel 1950 è stata firmata a Roma la Convenzione Europea di Strasburgo per la salvaguardia delle libertà fondamentali del Consiglio d'Europa. L'articolo 8 ha così previsto il diritto di ogni persona al rispetto della vita privata e familiare, del domicilio e della corrispondenza.

Grazie alla lettura dei principi costituzionali e delle carte dei diritti sia in Italia che in altri paesi oggi appartenenti all'Unione europea è stato

possibile riconoscere diritti della personalità «atipici» adeguando i sistemi giuridici ad istanze di tutela emergenti. La nozione dei diritti della personalità è evoluta ed evolve in funzione delle esigenze della società e di protezione della persona [Alpa, Resta 2019, 164].

Nel catalogo aperto ed eterogeneo dei diritti della personalità sono oggi ricompresi: il diritto al nome, all'immagine, all'onore e alla reputazione, il diritto morale d'autore, il diritto all'identità personale, all'integrità fisica e psichica, e i diritti alla riservatezza e alla protezione dei dati personali. Questa lista non è esaustiva, essendo aperta al riconoscimento di nuove posizioni giuridiche soggettive meritevoli di tutela della persona nella realtà sociale, culturale e negli ambiti in cui ha capacità e possibilità di realizzarsi.

La giurisprudenza ha svolto e svolge in questo senso un ruolo chiave di formante del diritto. Si pensi, ai diritti di matrice giurisprudenziale, quali quello a conoscere le proprie origini [Mascia 2008, 272-277], quello all'autodeterminazione in ordine all'identità di genere, quello alla vita [Anelli et al. 2019, 124 ss.].

Gli studi sui diritti della personalità si sono sviluppati separatamente dalla trattazione in tema di diritti fondamentali e diritti di libertà, come la manifestazione del pensiero; tuttavia, i primi condividono con i secondi i caratteri dell'assolutezza, dell'efficacia *erga omnes*, la necessità di porre in bilanciamento diversi interessi in gioco, l'essere diritti o libertà riferibili alla «persona» e prospettive a cui si interfacciano sia il diritto privato che il diritto pubblico [Galgano 1988].

Tradizionalmente, i diritti della personalità sono stati considerati: a) necessari, appartenendo a tutte le persone fisiche, ed eventualmente anche a quelle giuridiche in casi determinati; b) imprescrittibili, in quanto non si estinguono per il non uso protratto nel tempo; c) assoluti, proteggendo *erga omnes* i consociati; d) non patrimoniali, tutelando valori non suscettibili di valutazione economica; e) indisponibili, in quanto non rinunciabili [Anelli et al. 2019, 124-125].

Peraltro, le caratteristiche omologhe a cui i diritti della personalità sono stati storicamente associati hanno subito dei cambiamenti dovuti alla complessità dei nuovi fenomeni sociali [Resta 2014, 87-96]. A titolo di esempio, è attualmente ammessa la valutazione economica e la trasmissibilità di alcune facoltà relative a diritti della personalità, come nel caso dei diritti patrimoniali relativi alla diffusione dell'immagine di

una persona nota (*right of publicity*), a livello contrattuale o successorio [Caso 2021, 133-142].

Perciò, le posizioni protette potrebbero assumere delle caratteristiche peculiari che si discostano dalla nozione storica di diritto della personalità, impedendo l'individuazione di una sola concettualizzazione della nozione [Pardolesi 2005]. Allo stesso tempo, è possibile affermare che tutte le situazioni soggettive si riferiscono alla tutela della persona in quanto tale e ai suoi attributi materiali o immateriali (come il corpo, l'identità, l'onore, il dato personale).

Il diritto alla riservatezza, come anticipato, è considerato uno dei diritti della personalità e ne condivide, quindi, i connotati sopra esposti.

I primi riferimenti ad un diritto alla riservatezza in Europa vanno rintracciati nei contributi di quanti hanno analizzato l'articolo di Warren e Brandeis e studiato le pronunce giurisprudenziali statunitensi sul *right to be let alone* [Alpa, Resta 2019, 275]. Il diritto è stato elaborato dalla dottrina e ha poi trovato riconoscimento nell'art. 8 della Cedu, nella successiva giurisprudenza delle corti nazionali, per poi essere inserito nella Carta dei diritti fondamentali dell'Unione europea all'articolo 7, quale uno di diritti fondamentali dell'individuo nell'ordinamento giuridico.

Le prossime sezioni presenteranno l'origine e lo sviluppo del diritto negli ordinamenti italiano ed europeo sia a livello normativo, dottrinario che giurisprudenziale.

2.2 Le origini del diritto alla riservatezza in Italia

In Italia, le prime riflessioni su un diritto alla riservatezza sono riscontrabili nella dottrina privatistica degli anni Trenta. Nel 1937 Adolfo Ravà scriveva che alla persona doveva essere riservata «una certa sfera, relativa ai lati più gelosi e più intimi di essa e della sua attività, nella quale non sia lecito ad alcuno di ingerirsi e di entrare» [Ravà 1937, 211]. In un saggio dello stesso anno Massimo Ferrara Santamaria ripercorreva la riflessione pandettistica sui diritti della personalità unitamente all'apporto fondamentale della giurisprudenza francese e presentava il «diritto alla illesa intimità privata» [Ferrara Santamaria 1937, 170]. L'ampia categoria giuridica potrebbe tutelare

> tutti quei casi in cui la persona non è disposta a consentire, intorno alla sua esperienza intima, una pubblicità qualsiasi o una pubblicità oltrepassante il minimo strettamente necessario, imposto dalle esigenze sociali e dalle idee comunemente accolte dalla morale e dal buon costume dei nostri tempi.

Lo studioso riconosceva nelle disposizioni legislative a protezione della segretezza della corrispondenza un possibile fondamento della vita intima del singolo individuo. La relatività e discrezionalità nel definire il limite di intrusione lecita nell'intimità lasciava aperta la questione di come potesse in concreto essere riconosciuto e tutelato questo diritto in sede giurisdizionale. Secondo Ferrara Santamaria, il riconoscimento del diritto alla illesa intimità privata era «indispensabile» e poteva persino derivare da una «contestazione di buon senso» della realtà sociale e dei suoi continui mutamenti.

La legge 22 aprile 1941, n. 633 (l.d.a.) introdusse la disciplina a protezione del diritto d'autore e di altri diritti connessi e, in aggiunta, agli articoli 96, 97 e 98 alcune disposizioni a tutela del ritratto. Senza il consenso della persona il ritratto non può essere esposto, riprodotto o messo in commercio (art. 96), a meno che la riproduzione di quest'immagine sia giustificata dalla notorietà o dal ruolo pubblico ricoperto dalla persona, da necessità di giustizia o di polizia, da scopi scientifici, didattici o culturali, ovvero quando la riproduzione sia collegata a fatti, avvenimenti, cerimonie aventi un pubblico interesse o svoltisi in pubblico (art. 97, co. 1). Tuttavia, il ritratto della persona non può essere esposto se ciò rechi pregiudizio all'onore, alla reputazione o al decoro del soggetto ritrattato (art. 97, co. 2). Tali disposizioni vanno lette in combinato disposto con l'art. 10 del Codice Civile, sull'abuso di immagine altrui, che prevede la tutela inibitoria e risarcitoria qualora l'immagine sia pubblicata illecitamente o con pregiudizio del decoro e della reputazione della persona o dei suoi congiunti.

Nel secondo dopoguerra la giurisprudenza italiana ha cominciato ad occuparsi del diritto alla riservatezza in relazione alla protezione della sfera intima delle persone notorie [Pascuzzi 2020, 77]. Era il tempo in cui la stampa iniziava ad interessarsi alle vicende private dei soggetti famosi, per poi pubblicarle a fini scandalistici. Vista la scriminante del consenso dell'art. 97 l.d.a. per il ritratto in presenza di notorietà della persona non

era chiaro se la diffusione di immagini e notizie private fosse lecita o meno.

Il primo caso in cui si fece esplicito riferimento ad un possibile diritto alla riservatezza fu *Caruso v. Tirrena Asso Film*. Il tenore Enrico Caruso fu ritratto nel film «Leggenda di una voce» come una persona incline all'ubriachezza, in conflitto con l'Erario e che aveva tentato il suicidio a seguito di un insuccesso. Alla luce di queste vicende private raccontate in forma scenica, i suoi eredi citarono in giudizio la casa produttrice del film, in sede cautelare, presso la Pretura di Roma, richiedendo il sequestro della pellicola e sostenendo che essa ledeva la memoria, l'onore e la riservatezza del tenore. Il primo grado si concluse nel 1951 con una decisione di rigetto circa l'esistenza di un interesse pubblico alla conoscenza delle vicende, anche private, di persone celebri (Pretore di Roma, 19 novembre 1951). Nel merito fu poi adito il Tribunale di Roma, che si espresse per una diversa soluzione: la riproduzione di fatti o avvenimenti della vita privata di un soggetto, seppur celebre, era considerabile illecita se offriva soddisfazione soltanto per il desiderio di curiosità e di indiscrezione del pubblico e, quando lecita, non doveva riguardare fatti che recassero pregiudizio all'onore, al decoro o alla reputazione della persona (Tribunale di Roma, 14 settembre 1953).

Il medesimo principio di diritto fu sostenuto nel caso del film su Caruso «The Great Thenor», prodotto dalla Metro Goldwin Mayer, deciso dal Tribunale e dalla Corte di Appello di Roma [Alpa, Resta 2019, 276].

Tuttavia, la decisione del Tribunale di Roma del 1953 fu criticata da una parte della dottrina che non riteneva esistente un presupposto normativo per una tale tutela alla riservatezza, e successivamente fu capovolta dalla Corte di Cassazione, in terzo grado (Cass. 22 dicembre 1956, n. 4487), poiché appunto

> Nessuna disposizione di legge autorizza a ritenere che sia stato sancito, come principio generale, il rispetto assoluto all'intimità della vita privata e tanto meno come limite alla libertà dell'arte. Sono soltanto riconosciuti e tutelati, in modi diversi, singoli diritti soggettivi della persona.
>
> […] fuori dei limiti fissati, l'aspirazione alla privatezza non riceve protezione, salvo che l'operato dell'agente, offendendo l'onore o il decoro o la reputazione della persona, ricada nello schema generale del fatto

> illecito. Quando la conoscenza delle vicende della vita altrui non sia stata ottenuta con mezzi di per sé illeciti o che impongano l'obbligo del segreto, non è vietato comunicare i fatti, sia privatamente ad una o più persone, sia pubblicamente a mezzo della stampa, di opere teatrali, o cinematografiche, di discorsi, ecc.
>
> Il semplice desiderio di riserbo non è stato ritenuto dal legislatore un interesse tutelabile; chi non ha saputo o voluto tener celati i fatti della propria vita non può pretendere che il segreto sia mantenuto dalla discrezione altrui; la curiosità ed anche un innocuo pettegolezzo, se pur costituiscono una manifestazione non elevata dell'animo, non danno luogo di per sé ad un illecito giuridico.

Nel caso Caruso la Corte di Cassazione non riscontrò alcuna norma positiva a fondamento della protezione della vita privata e non utilizzò quale strumento interpretativo la Costituzione.

Tale ultima scelta era probabilmente dovuta al fatto che la Prima Parte della Carta costituzionale veniva considerata meramente programmatica. Soltanto dalla pronuncia 5 giugno 1956, n. 1 la Corte costituzionale mutò interpretazione, riconoscendo la natura pienamente vincolante delle disposizioni costituzionali, anche per le leggi emanate in precedenza. L'articolo 2 della Costituzione a protezione dei diritti inviolabili dell'uomo, sia come singolo, che nelle formazioni sociali dove si svolge la sua personalità, si rivelerà indispensabile per riconoscere una tutela al diritto alla riservatezza.

Negli anni Cinquanta un'altra parte della dottrina italiana insisteva per il riconoscimento di un diritto alla protezione della vita privata, anche in assenza di una specifica disposizione normativa. Secondo De Cupis, il diritto italiano tutelava la persona in due dimensioni: 1) nell'«interesse ad essere rappresentata non diversa da quella che è» («verità personale»), e 2) nell'«interesse alla non rappresentazione di sé» («contro la verità personale»). Nel 1954 sempre De Cupis, in risposta alle critiche di Pugliese, scriveva che questo diritto era esistente e autonomo, quale «qualità» e «modo di essere della persona», oltre alla percezione che di essa si ha nel sociale [De Cupis 1954]. L'interesse al diritto alla riservatezza veniva considerato differente rispetto al diritto all'onore, alla reputazione e al segreto e poteva essere riconosciuto per analogia di specifiche norme dell'ordinamento, quali le disposizioni sul diritto all'immagine.

Secondo Giampiccolo, studioso della pandettistica, l'interesse alla «privatezza» rifletteva l'aspirazione di un soggetto a conservare una tranquillità di spirito e una pace interiore che un'indesiderata pubblicità poteva turbare [Giampiccolo 1958]. Questa aspirazione era un'esigenza ritenuta meritevole di tutela dalla coscienza sociale. Una norma specifica per tutelare tale diritto non era necessaria perché la categoria dei diritti della personalità presente nel sistema giuridico doveva assumere un valore unitario. Un unico diritto della personalità a contenuto indefinito si riteneva proteggere l'individuo e il suo riserbo nel sistema giuridico già composto dall'art. 2 della Costituzione, dalle norme penali e in materia di diritto d'autore, ma anche segnato dal costume e dalle concezioni dominanti nella coscienza sociale.

Il secondo caso giurisprudenziale da considerare per studiare l'affermazione del diritto alla riservatezza in Italia è *Petacci v. Palazzi* dell'inizio degli anni Sessanta. La Corte d'appello di Milano si trovò a decidere su un caso di pubblicazione di un libro contenente delle vicende private di Claretta Petacci e della sua famiglia, riconoscendo la sussistenza nell'ordinamento italiano di un diritto al «riserbo, come facoltà giuridica di escludere ogni invadenza estranea dalla sfera della propria intimità personale e familiare». Il fondamento di tale diritto veniva identificato nell'art. 8 della Cedu, sul diritto di ogni persona al rispetto della vita privata e familiare.

La Cassazione fu investita della vicenda (Cass. 20 aprile 1963, n. 990). Richiamando la decisione sul caso Caruso, la Corte proponeva un mutamento della sua giurisprudenza. I diritti della personalità esplicitamente riconosciuti (come il diritto al nome) potevano essere considerati come «specifiche previsioni» che avevano riferimento «alla personalità considerata in particolari aspetti», a cui dovevano essere aggiunte «possibilità di manifestazioni concrete nel campo della vita e in quello sociale». Il fondamento di questa apertura andava ravvisato nell'art. 2 della Costituzione poiché questa norma presumeva un diritto di libera autodeterminazione della persona nello svolgimento della sua personalità e nei limiti di solidarietà.

Tuttavia, in mancanza di un'esplicita previsione legislativa la Corte non ritenne possibile interpretare per analogia dei singoli diritti della personalità «un autonomo diritto soggettivo ad una non precisata riservatezza», quanto piuttosto opportuno ammettere una tutela nel caso di

violazione del «diritto assoluto di personalità inteso quale diritto *erga omnes* alla libertà di autodeterminazione nello svolgimento della personalità dell'uomo come singolo». In concreto, pur respingendo le censure alla sentenza della Corte d'Appello, la Cassazione negò la tutela al diritto al riserbo degli attori. Tale interpretazione sollevò reazioni contrastanti da parte della dottrina [Alpa, Resta 2019, 302-304].

Soltanto a metà negli anni Settanta si arrivò al famoso *leading case* in materia di diritto alla riservatezza: *Soraya Esfandiari v. Rusconi Editore* (Cass. 27 maggio 1975, n. 2129). I fatti riguardavano la pubblicazione sul periodico «Gente» di alcune fotografie ritraenti la principessa Soraya, famosa perché ex-consorte dello scià di Persia, in atteggiamenti intimi, all'interno delle mura della sua villa, precisamente nel giardino, mentre baciava il regista Franco Indovina. Le fotografie venivano ottenute tramite un teleobiettivo. La principessa conveniva in giudizio la casa editrice proprietaria del periodico, lamentando la violazione del suo domicilio, della riservatezza e della sua immagine, con pregiudizio del decoro, dell'onore e della reputazione (artt. 10 c.c., 96 e 97 l.d.a) e chiedendo il sequestro del periodico e il risarcimento dei danni subiti.

Adito in via d'urgenza, il Pretore di Milano accoglieva la richiesta attorea concedendo il provvedimento cautelare, e nel merito il Tribunale in primo grado confermava il sequestro e liquidava il risarcimento del danno sulla base della violazione del diritto all'immagine. La Corte di Appello di Milano adita dalla società Rusconi confermava la condanna al risarcimento del danno, escludendo tuttavia il sequestro in assenza dei presupposti dell'art. 21 della Costituzione (App. Milano 19 gennaio 1971). Questa Corte non riteneva violato un diritto alla riservatezza, non considerandolo un autonomo diritto della personalità.

A questo punto, la principessa Soraya proponeva ricorso per cassazione. L'argomentazione della Corte è apprezzabile non solo per il primo riconoscimento del diritto alla riservatezza, ma anche per l'interpretazione offerta della categoria giuridica dei diritti della personalità sulla base dell'art. 2 della Costituzione.

In primo luogo, la Corte di Cassazione fornisce un'interpretazione restrittiva delle esimenti al consenso della persona ritratta: il concetto di notorietà trova un limite nell'ambito territoriale in cui la persona è considerata nota e deve sussistere un interesse pubblico prevalente alla diffusione dell'immagine, altrimenti non trova applicazione la giustifica-

zione prevista dalla l.d.a.; sarebbe, quindi, necessario un interesse all'informazione ulteriore rispetto all'interesse lucrativo commerciale di chi pubblica il ritratto (art. 41, co. 2 Cost.). Il diritto di cronaca, tutelato dalla Costituzione all'art. 21, incontra i limiti della verità del fatto esposto, della rispondenza ad un interesse pubblico (c.d. pertinenza) e del rispetto della riservatezza e onorabilità della persona nell'usare una forma espositiva civile (c.d. continenza).

Anche le persone notorie potrebbero avere diritto a proteggersi da intrusioni non giustificate da una rilevanza sociale. La notorietà, quindi, non legittima di per sé la pubblicazione di immagini della persona. È necessario uno scopo informativo di interesse pubblico.

Secondariamente, la Corte espone l'esigenza di trovare una soluzione che, pur ancorata alle norme costituzionali ed alle altre disposizioni dell'ordinamento, sia «sensibile al contemperamento della tutela dei diversi interessi, alla luce di una vasta tendenza, anche di diritto internazionale, ad estendere la difesa della personalità umana, sia nei confronti dell'abuso dei pubblici poteri, che nei rapporti intersoggettivi individuali».

Nel dibattito dottrinale esistente la Corte individua tre aspetti di un diritto alla riservatezza:

> Da una parte si tende a restringere rigorosamente l'ambito di questo diritto al riserbo della «intimità domestica», collegandola al concetto ed alla tutela del domicilio. A questa concezione corrisponde forse il «the right to be alone» degli anglosassoni. All'opposto, vi sono formulazioni molto generiche - «il riserbo della vita privata» da qualsiasi ingerenza, o la c.d. «privatezza» (privacy) - cui corrisponderebbe un sostanziale ambito troppo vasto o indeterminato della sfera tutelabile. Una concezione intermedia, che riporta in limiti ragionevoli la portata di questo diritto, può identificarsi nelle formule che fanno riferimento ad una certa sfera della vita individuale e familiare, alla illesa intimità personale in certe manifestazioni della vita di relazione, a tutte quelle vicende, cioè, il cui carattere intimo è dato dal fatto che esse si svolgono in un domicilio ideale, non materialmente legato ai tradizionali rifugi della persona umana (le mura domestiche o la corrispondenza).

Per trovare una base normativa a quest'ultima concezione intermedia del diritto alla riservatezza vengono considerate varie disposizioni posi-

tive (tra cui, artt. 96 e 97 l.d.a., art. 614 c.p., l. 8 aprile 1974, n. 98 sulla segretezza delle comunicazioni) e ripercorse le precedenti decisioni giurisprudenziali sul punto. L'interpretazione a partire dalle norme sull'immagine e sul segreto deve considerarsi superata.

Il fondamento è piuttosto l'art. 2 della Costituzione quale «unico fondamento del diritto assoluto della personalità, che risulta violato dalla divulgazione delle notizie della vita privata». Anche gli artt. 3, 13, 14 e 15 della Costituzione proteggono la dignità e la libertà dell'uomo in diverse dimensioni e sia la Dichiarazione Universale dei diritti dell'uomo che la Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali tutelano la persona contro le ingerenze nella sua vita privata (art. 8).

La definizione di diritto della riservatezza viene così sintetizzata:

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

Nell'ordinamento italiano esiste, dunque, un generale diritto alla riservatezza come situazione giuridicamente tutelabile. La nozione di domicilio domestico rimanda ad un luogo ideale in cui non dovrebbero esserci ingerenze da parte dell'esterno, perché non concorre un interesse rilevante ad entrarci.

La Corte di Cassazione considerò illecita la pubblicazione delle foto sul periodico perché non giustificata da un effettivo e apprezzabile interesse sociale all'informazione, anche se tale pubblicazione non ledeva l'onore, il decoro e la reputazione dell'attrice.

A partire da questa importante pronuncia il diritto alla riservatezza viene annoverato tra i diritti della personalità e considerato un diritto soggettivo che, se violato, può giustificare il risarcimento del danno.

2.3 La protezione della riservatezza nell'ordinamento italiano

Nel caso Soraya la categoria dei diritti della personalità si arricchisce del diritto alla riservatezza. Questo approccio presuppone l'adesione ad una concezione c.d. «pluralistica» di questi diritti: l'ordinamento riconosce positivamente tanti diritti della personalità, da azionare separatamente, e non uno solo di carattere generale.

Attualmente, invece, la dottrina e la giurisprudenza maggioritarie adottano una concezione «monista», nell'ottica di proteggere un unico generale diritto della personalità che si compone di più aspetti. Se nella prima prospettiva è necessario argomentare per analogia nel riconoscere nuove tutele a situazioni soggettive - come avviene nel caso Soc. Austria Tabakwarke GmbH v. Veronesi & Istituto nazionale per lo studio e la cura dei tumori per il diritto all'identità personale (Cass. 22 giugno 1985, n. 3769) - nella seconda concezione la personalità individuale è tutelata dal nucleo fondativo rappresentato direttamente dall'art. 2 della Costituzione (Caso Re Cecconi, Cass. 7 febbraio 1996, n. 978). Questa norma si considera la clausola aperta del diritto della personalità.

Il diritto alla riservatezza rappresenta, quindi, un aspetto del generale diritto della personalità, che assicura la non rappresentazione all'esterno delle proprie vicende personali non aventi per i terzi un interesse socialmente apprezzabile e preminente. Questo diritto può essere invocato da chiunque. La persona nota può vedere tutelata la sua riservatezza quando non vi è un'utilità sociale all'interferenza nella sua vita privata e familiare.

La lesione del diritto alla riservatezza, ove generatrice di un danno ingiusto, dà luogo a responsabilità ai sensi dell'art. 2043 c.c.; il danno non patrimoniale può essere risarcito grazie all'attuale interpretazione costituzionalmente orientata dell'art. 2059 c.c. [vedi → Capitolo 11]. Assume, in aggiunta, particolare importanza la tutela cautelare ai sensi dell'art. 700 c.p.c., che consente interventi in urgenza qualora vi siano i presupposti del *fumus boni iuris* (probabile esistenza del diritto cautelare) ed *il periculum in mora* (pericolo di un pregiudizio imminente ed irreparabile).

Una disciplina specifica sul diritto alla riservatezza è stata inserita all'interno dello Statuto dei Lavoratori [vedi → Capitolo 9]. Anche il diritto penale tutela la sfera privata della persona tramite la previsione

dei reati di violazione di domicilio (artt. 614 e 615 c.p.), di interferenze illecite nella vita privata (art. 615-*bis* c.p.), all'interno dei delitti contro la persona, ed in particolare contro l'inviolabilità del domicilio, e dei delitti contro la inviolabilità dei segreti (art. 616 ss. c.p.).

Il diritto alla riservatezza può essere posto in bilanciamento con altri diritti fondamentali, quali la libertà di manifestazione del pensiero e il diritto di cronaca (art. 21 Cost.). Per comporre i diversi interessi si suggerisce di tracciare un (sempre mobile) confine tra fatti la cui conoscenza ha una rilevanza politica e sociale e fatti che sollecitano la curiosità, senza che vi sia una ragione sufficiente per ledere la riservatezza del singolo individuo [Alpa, Resta 2019, 351].

La divulgazione di notizie lesive del diritto alla riservatezza deve considerarsi lecita espressione del diritto di cronaca, non comportando responsabilità civile, ove ricorrano, oltre all'interesse pubblico preminente rispetto al riserbo, le tre condizioni di:

– utilità sociale della notizia;
– verità dei fatti divulgati (anche se soltanto putativa);
– forma civile dell'esposizione dei fatti e della loro valutazione, che non sia «eccedente rispetto allo scopo informativo ed improntata a serena obiettività, con esclusione di ogni preconcetto intento denigratorio» (Decalogo del Giornalista, Cass. 18 ottobre 1984 n. 5259).

Un particolare aspetto del diritto alla riservatezza emerso in relazione al bilanciamento con il diritto di cronaca è il diritto all'oblio, inteso quale «interesse di ogni persona a non restare indeterminatamente esposta ai danni ulteriori che arreca al suo onore e alla sua reputazione la reiterata pubblicazione di una notizia in passato legittimamente divulgata» (Cass. 9 aprile 1998, n. 3679). Il diritto all'oblio quale particolare dimensione del tradizionale diritto alla riservatezza è diverso rispetto al diritto alla cancellazione dei dati personali (*right to be forgotten*) o alla de-indicizzazione di un link in un motore di ricerca contenente una notizia (Caso Google Spain). Esso si riferisce a situazioni in cui l'intrusione nella sfera privata è stata in passato lecitamente giustificata da un interesse pubblico preminente, ma la reiterazione dell'invasione, ad esempio con una nuova pubblicazione di fatti o di un'immagine, non è più giustificata da un interesse pubblico attuale [vedi → Capitolo 8].

Una differente dimensione del diritto alla riservatezza riguarda il possibile anonimato durante un processo [Resta 2014, 154-193]. La dimensione necessariamente pubblica e trasparente di un processo, dei suoi atti e delle sentenze potrebbe difatti scontrarsi con l'interesse del singolo al riserbo su vicende intime e delicate di sé o della famiglia. Nell'esperienza nordamericana l'utilizzo di pseudonimi (es. John Doe) è storicamente molto diffuso. In Italia, il problema è emerso a seguito della digitalizzazione delle sentenze e dell'utilizzo di banche dati o comunque della rete Internet per la diffusione delle informazioni giudiziarie. La giurisprudenza ritiene che le disposizioni processuali non consentano l'occultamento delle generalità delle parti negli atti processuali [Resta 2014, 179]. Soltanto il d.l. 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali, contiene una norma che consente in presenza di alcuni presupposti di proteggere l'anonimato nella riproduzione della sentenza (art. 52). Nel caso di divulgazione di notizie su indagini e sui processi da parte dei *media*, il diritto alla riservatezza dovrà essere bilanciato con l'accesso alle informazioni di interesse pubblico e il diritto di cronaca. Anche in tale contesto il Codice Privacy fornisce un criterio per il bilanciamento: le informazioni divulgate devono essere essenziali [Resta 2014, 240].

Un ulteriore aspetto del diritto alla riservatezza e dell'anonimato è rilevabile nella disciplina a protezione dell'identità della madre biologica dell'adottato, la quale può dichiarare al momento del parto di non voler essere nominata ai sensi dell'art. 30 del d.p.r. 3 novembre 2000, n. 396 («parto anonimo»). Questa dimensione della riservatezza può essere posta in bilanciamento con un altro aspetto del diritto della personalità non della donna, ma del figlio, ossia il diritto a conoscere le proprie origini, esercitabile a partire dai 25 anni (art. 28 della l. 4 maggio 1983, n. 184 sull'adozione). Nel 2013 la Corte Costituzionale ha sancito la possibilità per il figlio di interpellare la madre che ha dichiarato di non voler essere nominata per la revoca di tale decisione di riservatezza (Corte cost. 18 novembre 2013, n. 278). Se la donna non dovesse revocare la sua scelta, prevarrebbe la sua riservatezza e l'anonimato rimarrebbe per tutta la durata della sua vita (Cass., sez. un., 25 gennaio 2017, n. 1946; Cass. 22 settembre 2020, n. 19824). Qualora l'interpello non fosse possibile perché la donna non risultasse più in vita, il diritto alla conoscenza dello

status di figlio potrebbe prevalere in quanto la riservatezza sarebbe inevitabilmente attenuata.

Il panorama giurisprudenziale in materia di riservatezza riguarda frequentemente casi di diritto all'oblio (si veda, ad es. Cass. 26 giugno 2013, n. 16111) e di violazione della riservatezza in connessione con il diritto all'immagine, all'onore e alla reputazione e con il diritto alla protezione dei dati personali (Cass., sez. un, 22 luglio 2019, n. 19611; Cass., sez. un. 22 luglio 2020 n. 19681).

Con l'emersione degli strumenti e calcolatori informatici la nozione di privacy evolve, infatti, dal diritto ad essere lasciati soli nella propria sfera intima, al controllo dei dati personali [Rodotà 2012]. I cambiamenti tecnologici hanno portato, quindi, all'emersione di nuove esigenze di tutela, oggi rappresentate dal riconoscimento del diritto alla protezione dei dati personali, tutelato in Italia a partire dalla l. 31 dicembre 1996, n. 675, poi abrogata dal Codice Privacy, attualmente in vigore. In questa materia assume un ruolo centrale il Regolamento Generale sulla protezione dei dati (GDPR) emanato nel 2016 dall'Unione europea e divenuto applicabile dal 25 maggio 2018, a cui il Codice italiano è stato adeguato nel 2018 [vedi → Capitoli 3 e 5].

2.4 Il diritto alla riservatezza nel diritto europeo

All'interno dell'UE il diritto alla riservatezza è direttamente tutelato all'art. 7 della Carta dei Diritti Fondamentali dell'Unione europea, il quale sancisce che «ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni». La Carta di Nizza ha lo stesso valore giuridico dei Trattati europei, elevando il rango dei suoi diritti a livello costituzionale. Tale diritto deve essere salvaguardato in sede di applicazione delle norme dell'ordinamento europeo.

A partire dagli anni Novanta del secolo scorso l'UE ha svolto un ruolo chiave per la ridefinizione del concetto di privacy nella dimensione del diritto a protezione dei dati personali. Le tre disposizioni normative che hanno iniziato questo processo sono:

– Direttiva 95/46/CE, «relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati»;

– Direttiva 97/66/CE, «sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni»;
– Direttiva 2002/58/CE, «relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche».

Il prossimo capitolo si concentrerà su questa seconda dimensione del diritto alla privacy nell'ordinamento italiano ed europeo.

L'Unione è altresì vincolata alla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, che, come visto, prevede una specifica norma sulla vita privata e sulla segretezza della corrispondenza (art. 8).

La Corte Europea dei Diritti dell'Uomo di Strasburgo si è più volte pronunciata in materia di protezione della riservatezza intesa come tutela della vita privata dell'individuo anche in contesti pubblici (ad es. Corte Edu 24 settembre 2004, no. 59320/00, *von Hannover v. Germania*; Corte Edu 7 febbraio 2012, no. 39954/08, *Axel Springer v. Germania*), utilizzando il parametro della «ragionevole aspettativa di riservatezza» e nella dimensione della protezione del segreto nelle comunicazioni ed intercettazioni (ad es., Corte Edu 2 agosto 1984, no. 8691/79, *Malone v. Regno Unito*; Corte Edu 24 aprile 1990, no. 11105/84, *Huvig v. Francia*).

In particolare, nel caso *Axel Springer v. Germania*, riguardante la pubblicazione di due articoli su un attore televisivo molto conosciuto localmente in cui si riferiva che fosse stato arrestato all'Oktoberfest di Monaco in possesso di cocaina, la Corte ha fornito alcuni criteri utili per il bilanciamento dell'art. 8 con la libertà di manifestazione del pensiero e il diritto di cronaca, specificando che:
– il diritto al rispetto della vita privata include la protezione dalla divulgazione di fatti che l'individuo legittimamente si aspetta non vengano divulgati senza il suo consenso (par. 83);
– l'art. 8 può essere invocato quando la violazione ha un livello di gravità tale da pregiudicare il godimento personale del diritto al rispetto della vita privata, non potendo, invece, essere invocato per lamentarsi di una perdita di una reputazione che è la conseguenza prevedibile delle proprie azioni come, ad esempio, la commissione di un reato;
– la divulgazione dei fatti o delle immagini deve contribuire ad un dibattito di interesse pubblico generale (par. 90);

– un ruolo importante nel bilanciamento è rivestito dal ruolo (privato o notorio) della persona coinvolta (par. 91) e dal comportamento assunto prima e dopo la divulgazione (par. 92);
– altrettanto rilevante è la modalità con cui le informazioni sul soggetto sono raccolte, la loro veridicità (par. 93), e con cui sono pubblicate e quanto sono diffuse e disseminate (par. 94).

Questi criteri si aggiungono a quelli stabiliti dalla Corte di Cassazione nel Decalogo del Giornalista e sull'attualità della notizia.

2.5 Casi 2-1, 2-2, 2-3

I prossimi casi richiamano fatti relativi ad alcune pronunce giurisprudenziali in materia di diritto alla riservatezza. Eventuali prospettive relative alla violazione del diritto a protezione dei dati personali non vanno, in questa sede, analizzate.

Caso 2-1

Il quotidiano a tiratura nazionale Alfa pubblica una notizia corredata da fotografie scattate da paparazzi e relativa all'attivista e attrice Caia, notoriamente impegnata in ambito culturale e politico per la protezione dell'ambiente, mentre si trovava sul catamarano di un facoltoso proprietario di impianti petroliferi, in topless, e sembrava intrattenersi in atteggiamenti intimi con lo stesso. A partire da questo articolo, molti altri quotidiani commentano la notizia e ripubblicano le fotografie accusando Caia di non essere un'attivista coerente con quanto professato per anni. Caia adisce il giudice civile per tutelare i suoi diritti.
Qual è il problema giuridico?
Qual è la soluzione del problema?
Applicare la regola e argomentare.

Caso 2-2

La rete televisiva Beta trasmette un servizio in cui il famoso cantante Tizio, all'uscita di un ristorante nel quale si era intrattenuto a cena con amici, veniva avvicinato da una troupe, che richiedeva all'artista il

rilascio di un'intervista. Tizio non nascondeva il proprio disappunto per la presenza degli inviati della trasmissione e rifiutava in modo secco e perentorio quanto richiestogli. L'episodio veniva registrato e mandato in onda nella trasmissione della domenica pomeriggio con il titolo «più antipatici e scorbutici del mondo dello spettacolo». Il conduttore accompagnava il servizio con il commento sarcastico: «Chissà perché è così nervoso? Ma a Natale non si dovrebbe essere più buoni?». Tizio adisce il tribunale lamentando la violazione dei suoi diritti.
Qual è il problema giuridico?
Qual è la soluzione del problema?
Applicare la regola e argomentare.

Caso 2-3

Il Comune Gamma pubblica una notizia sul proprio sito relativa alle fasi del processo di un suo cittadino, Sempronio, imputato per furto di energia elettrica, corredandola con la foto segnaletica effettuata dalla polizia locale. Sempronio, consigliato dall'avvocato, decide di agire in sede civile per tutelare i suoi diritti.
Qual è il problema giuridico?
Qual è la soluzione del problema?
Applicare la regola e argomentare.

CAPITOLO 3.
Il diritto alla protezione dei dati personali in Europa ed il Regolamento Generale sulla Protezione dei Dati

Paolo Guarda

3.1 Premessa: dal diritto ad essere lasciati soli alla protezione dei dati personali

Vi è un rapporto complesso tra la storia delle idee e lo sviluppo tecnologico. Quest'ultimo, infatti, può provocare cambiamenti economici, oltre che trasformazioni nelle istituzioni sociali. Tale meccanismo è stato alla base dell'affermazione nel nostro ordinamento del diritto alla protezione dei dati personali e coincide con l'inizio della capillare diffusione dei calcolatori.

L'evoluzione dell'informatizzazione può dividersi in tre grandi periodi. Il primo copre gli anni '70 del secolo scorso ed è caratterizzato dalla presenza di pochi grandi calcolatori: dato il costo elevato, solo le pubbliche amministrazioni potevano permettersi l'utilizzo di queste macchine. Durante gli anni '80 i computer costano meno e diventano poco ingombranti: essi potevano, così, essere utilizzati anche da parte di grandi imprese private (ad es. banche, assicurazioni, ecc.). Il terzo periodo si situa nella prima metà degli anni '90 quando i computer cominciano ad avere prezzi più economici e sono oramai presenti in tutte le abitazioni private. A tutto ciò si aggiunga, poi, l'ulteriore evoluzione verificatasi successivamente e coincidente con l'utilizzo di massa delle reti telematiche e, più in particolare, di Internet [Pascuzzi 2020, 79-82].

L'avvento dei computer e la loro crescente diffusione ha determinato la presa di coscienza che tali strumenti sono capaci di muovere quantità enormi di informazioni, sottoponendo l'individuo ad una nuova forma di dominio sociale: il potere informatico. Quindi, da «diritto ad esser lasciati soli» si è passati al «diritto al controllo sulle informazioni che riguardano l'individuo» [Frosini 1984, 32-33].

La novità fondamentale introdotta dall'elaboratore consiste non tanto nell'archiviazione di masse enormi di dati, quanto nella possibilità di accedere e di far circolare in tempi ridottissimi tutti i dati memorizzati, nell'interconnessione tra i sistemi e nell'aggregazione e combinazione in modi diversi delle notizie, la quale consente di riorganizzare le informazioni disperse e di renderle «informazioni organizzate» [Rodotà 1973, 14].

Torniamo alla periodicizzazione in precedenza abbozzata e concentriamo la nostra attenzione sul formante legale, ed in particolare sul tema della privacy nel continente europeo. Nel torno di anni sopra descritto si è assistito ad una proliferazione di normative emanate con l'intento di disciplinare il trattamento dei dati personali attraverso l'utilizzo di calcolatori elettronici. Tali normative risentono dell'evolversi della rivoluzione digitale tanto che si parla di leggi di prima, di seconda e di terza generazione [Pardolesi 2003, 32].

In Europa i primi interventi si sono verificati nella Germania Federale con le leggi dei Länder Assia (del 7 ottobre 1970) e Baviera (del 12 ottobre 1970) a cui ha fatto seguito nel 1977 una legge federale sulla protezione dei dati (Bundesdatenschutzgesetez, Bdsg), che prevedeva in particolare la figura di un Garante per la protezione dei dati personali sia per le persone fisiche che giuridiche *(Datenschutz).* Nel 1981, tutti i Länder avevano già una legge sulla protezione dei dati personali. Un'altra tra le prime discipline europee ad entrare in vigore fu quella svedese del 11 maggio 1973, n. 289 (Data Lag), modificata con legge 1° luglio 1982, n. 446, che si fonda sul controllo pubblico delle raccolte di dati, riconoscendo tuttavia al cittadino il diritto di accesso. Sono seguite, poi, le leggi emanate in Francia (1978), Lussemburgo (1979), Danimarca (1979), Austria (1980), Norvegia (1980), Islanda (1982), Gran Bretagna (1984), Finlandia (1988), Olanda (1990), Portogallo (1991), Spagna (1993), Belgio (1993) e Svizzera (1993). Inoltre, Spagna, Portogallo, Austria, Olanda, Germania e Grecia hanno inserito apposite norme sulla privacy nelle loro Costituzioni.

Nella classifica - in termini temporali - dell'adozione di una legislazione specifica in materia di protezione dei dati tra i paesi occidentali l'Italia è riuscita ad anticipare solamente la Grecia con la legge 31 dicembre 1996, n. 675 «Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali» [Giannantonio, Losano, Zeno-Zencovich 1997].

A partire dalla seconda metà degli anni '80 gli organismi internazionali e comunitari presero coscienza delle problematiche connesse alla protezione dei dati personali e cominciarono ad emanare una serie di atti, sia di carattere prettamente normativo che di puro indirizzo politico.

Il 23 settembre 1980 l'OCSE adottò un documento contenente le linee guida per la tutela della privacy e del flusso transfrontaliero dei dati[1]. Un ruolo fin da subito importante fu giocato dal Consiglio d'Europa, il quale, oltre ad aver prodotto un copioso numero di raccomandazioni e risoluzioni in materia, si fece promotore della «Convenzione per la protezione degli individui con riguardo al trattamento automatizzato di dati personali», firmata a Strasburgo il 28 gennaio 1981. La Convenzione si proponeva di garantire l'enforcement dei diritti, delle libertà fondamentali ed in particolare del diritto alla vita privata all'interno di tutti gli ordinamenti degli Stati aderenti e nei confronti di tutti gli individui, a prescindere dalla nazionalità o dalla residenza. Seguirono le linee guida delle Nazioni Unite, adottate dall'Assemblea Generale e promosse dall'Alto Commissariato per i diritti umani il 14 dicembre 1990, relative al trattamento computerizzato dei dati personali.

Nel 1995 venne, poi, emanata dal Comitato dei Ministri dell'Unione europea la raccomandazione R(65)4, sulla protezione dei dati a carattere personale nella gestione dei servizi di telecomunicazione, con particolare riguardo ai servizi telefonici.

1 Queste si sostanziano in una serie di principi di base che devono servire come standard di riferimento: a) collection limitation principle; b) data quality principle; c) purpose specification principle; d) use limitation principle; e) security safeguards principle; f) openness principle; h) openness principle; i) individual participation principle; l) accountability principle. Il documento è reperibile sul portale dell'Organizzazione per la Cooperazione e lo Sviluppo Economico, da cui l'acronimo OCSE (o Organisation for Economic Co-operation and Development - OECD in sede internazionale): http://www.oecd.org.

Il regime giuridico che regola il trattamento dei dati personali a livello europeo è ora espressione dell'articolo 8 della Carta dei diritti fondamentali dell'UE, che riconosce la protezione dei dati personali come diritto fondamentale e autonomo rispetto alla protezione della vita privata (Art. 7) e agli altri diritti fondamentali, e dell'articolo 16 del TFUE (Trattato sul funzionamento dell'Unione europea), che consente all'Unione di legiferare in materia.

La disciplina di riferimento nel contesto dell'UE è stata per più di vent'anni basata sulla Direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 [Linksey 2015b e Bygrave 2014]. Questa ha rappresentato il primo e più complesso tentativo di normazione organica della materia a livello internazionale. La *ratio* della disciplina è volta a trovare un equo bilanciamento tra gli interessi, a volte opposti, alla tutela dei diritti fondamentali degli individui, da un lato, e alla libera circolazione delle informazioni, dall'altro.

Il modello europeo di protezione dei dati personali si è fin da subito caratterizzato per le seguenti peculiarità [Bygrave 2014, 100 e ss.]:

– è applicabile sia al settore pubblico che privato;
– riguarda tanto il trattamento manuale che quello automatizzato;
– ha un ambito di applicazione molto ampio, dovuto all'elasticità della definizione di dato personale;
– si basa su un nucleo di principi procedurali che garantiscono un elevato livello di protezione durante tutto il ciclo di vita dell'informazione;
– prevede una regolamentazione specifica e più restrittiva nei confronti di particolari categorie di dati (cd. dati sensibili, ovvero quei «dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché il trattamento di dati relativi alla salute e alla vita sessuale»[2]);
– vieta il trasferimento dei dati al di fuori dello Spazio Economico Europeo (che comprende tutti gli Stati Membri dell'UE più l'Islanda, il Liechtenstein e la Norvegia), a meno che il Paese «ricevente» non fornisca un livello di tutela adeguato;
– prevede la creazione di Autorità indipendenti nazionali, dotate di poteri investigativi, di intervento e di promozione di azioni giudiziarie,

2 Art. 8, par. 1, Direttiva 95/46/CE.

che vigilino sull'implementazione della normativa in materia di protezione dei dati personali;
– in capo all'interessato (cioè il soggetto cui si riferiscono i dati) sono riconosciuti una serie di diritti, quale quello di aggiornamento, di modifica, di conoscenza, di accesso, di cancellazione dei dati nonché quello di opporsi al trattamento stesso;
– in caso di violazione delle norme sul trattamento, prevede la possibilità di adire alternativamente l'Autorità di controllo nazionale o il giudice ordinario;
– si avvale a livello integrativo-interpretativo dei Codici di condotta.

L'obiettivo finale perseguito da tutte le normative sul trattamento computerizzato dei dati è quello di assicurare all'interessato il controllo sul flusso delle informazioni che lo riguardano. Per dirla con le parole di Rodotà [Rodotà 1999, 201]:

> la privacy può in primo luogo essere definita come il diritto di mantenere il controllo sulle proprie informazioni.

In Italia, infine, il riferimento normativo è ora il d.lgs. 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali (o Codice Privacy), che ha dapprima recepito la Direttiva 95/46/CE, ed è poi stato adeguato al GDPR dal d.lgs. 10 agosto 2018, n. 101 «Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE)» [vedi → Cap 5].

3.2 Il Regolamento generale sulla protezione dei dati

Il 27 aprile 2016 è stato approvato il Regolamento UE 2016/679 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), meglio conosciuto come «GDPR», acronimo di «General Data Protection Regulation». Si tratta di una riforma, a lungo attesa, che ha aggiornato la normativa con impatto diretto in tutti gli Stati membri dell'Unione, essendo concepito per uniformare la regole operative superando le con-

traddizioni o le possibili incongruenze emerse dai diversi recepimenti nazionali della precedente direttiva. Dopo un periodo di due anni, previsto dal legislatore europeo per permettere ai vari soggetti interessati (non ultimi i legislatori nazionali) di adeguarsi alla nuova disciplina, il Regolamento ha trovato definitiva applicazione il 25 maggio 2018.

Questo regolamento è di grande importanza perché rivede gli strumenti volti a tutelare i dati personali di fronte alle nuove sfide tecnologiche, creando un modello di protezione che si sta dimostrando una sorta di *benchmark* globale, con un «effetto domino» (*Brussel effect)* su altri ordinamenti giuridici, anche oltreoceano [Bradford 2020].

Il GDPR non rappresenta una rivoluzione legislativa. Esso si pone, infatti, nel solco della disciplina precedente di cui alla Direttiva 95/46/CE, confermandone per larga parte impostazione e principi. Certamente, però, è un momento importante di aggiornamento volto ad adeguare l'arsenale normativo al mutato contesto tecnologico: nuove definizioni, principi e regole applicative trovano, così, un approccio uniforme a livello europeo.

Senza alcuna pretesa di esaustività, di seguito si presenteranno alcune definizioni e concetti che verranno poi ripresi e, talvolta, saranno oggetto di approfondimento nei capitoli successivi. Tra le altre questioni non si è fatto, infine, riferimento a temi di carattere generale che saranno oggetto di apposita trattazione, quali: il trasferimento transfrontaliero dei dati [vedi → Capitolo 6]; poteri e ruoli delle autorità garanti per la protezione dei dati personali [vedi → Capitolo 10]; la responsabilità derivante da trattamento illecito di dati personali [vedi → Capitolo 11].

3.2.1 Ambito materiale, definizione di dato personale e ambito territoriale

L'art. 2 prevede l'ambito di applicazione materiale:

> Il presente regolamento si applica al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi.

Anzitutto, occorre definire con precisione cosa si intenda per dato personale (art. 4, pt. 1) [Bygrave, Tosoni 2020, 103-115]:

> 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.

La portata di questa definizione è molto ampia. Il concetto di «identificabilità» gioca un ruolo fondamentale. Il Regolamento innova rispetto alla Direttiva 95/46/CE fornendo una lista di identificativi: appunto il nome, un qualsiasi numero identificativo quale il codice fiscale, il codice cliente, ecc., dati relativi all'ubicazione (come CAP o posizione GPS), ecc. Un'informazione collegata ad un identificativo è da considerarsi come dato personale. Inoltre, il Considerando 26 aggiunge:

> 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. Per accertare la ragionevole probabilità di utilizzo dei mezzi per identificare la persona fisica, si dovrebbe prendere in considerazione l'insieme dei fattori obiettivi, tra cui i costi e il tempo necessario per l'identificazione, tenendo conto sia delle tecnologie disponibili al momento del trattamento, sia degli sviluppi tecnologici.

Il concetto di trattamento riceve poi una definizione particolarmente estesa, di fatto volta a ricomprendere qualsiasi tipo di attività che riguarda i dati personali. L'art. 4, pt. 2 così recita:

> qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione,

> il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

Non tutti i trattamenti ricadono nell'ambito di applicazione del GDPR. Il secondo paragrafo dell'art. 2, tra gli altri, esclude espressamente il trattamento effettuato dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse (lett. d) [che è oggetto di specifica disciplina → Capitolo 7] e quelli effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico (lett. a) (la c.d. «household exemption»).

Infine, l'art. 3 regola l'ambito di applicazione territoriale. Il primo paragrafo ripropone la regola tradizionale già adottata nella disciplina precedente:

> Il presente regolamento si applica al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione.

Il secondo paragrafo ha una portata sicuramente innovativa ed è volto a determinare quell'effetto domino cui si faceva cenno sopra:

> Il presente regolamento si applica al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano:
> – l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure
> – il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione.

Il GDPR diviene così una sorta di *benchmark* globale in quanto la stragrande maggioranza dei provider di servizi digitali dovrà fare i conti con la sua applicazione.

3.2.2 Categorie particolari di dati

Com'è noto il legislatore europeo ha sempre fatto della speciale protezione dedicata ad alcuni tipi di dati ritenuti sensibili un punto di forza. È così che la Direttiva madre 95/46/CE già codificava l'importanza della categoria dei dati sensibili fornendone, all'art. 8, par. 1, una definizione seppur indiretta:

> Gli Stati membri vietano il trattamento di dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché il trattamento di dati relativi alla salute e alla vita sessuale.

Il legislatore italiano riprendeva tale impostazione e riconosceva alla suddetta tipologia di dati un posto d'onore nella disposizione riportante le definizioni utilizzate nel testo normativo. L'art. 4, comma 2, lett. e), del Codice Privacy così recitava, infatti:

> «dati sensibili», i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

L'elencazione fornita era da intendersi di natura tassativa e non esemplificativa [Finocchiaro 2012, 57-61]. I dati sensibili, quali informazioni di carattere personale che riguardano la personalità etico-sociale dell'individuo e le sue caratteristiche psico-sanitarie, rappresentano un tipico caso di *numerus clausus*. Vi era, però, nel testo un elemento di elasticità e flessibilità. Quell'«idonei a rivelare» tingeva di riferibilità la relazione tra l'informazione e la peculiare caratteristica sensibile. La potenzialità di un dato a far scorgere la qualità in oggetto determina, quindi, che anche una semplice scelta alimentare o la geo-localizzazione in un luogo particolare sono in grado di disvelare, ad esempio, la credenza religiosa di un soggetto.

Il GDPR, anche su questo punto si pone nel solco della tradizione. L'innovazione più evidente è sicuramente quella relativa alla modifica dell'espressione terminologica. Per non indurre più in possibili errori e

fraintendimenti legati all'uso dell'aggettivo «sensibile», il Regolamento opta per un nuovo nomenclatore: le «categorie particolari di dati personali» [Granieri 2017]. Utilizzando, allora, la stessa tecnica di drafting normativo del provvedimento precedente, sancisce all'art. 9, par. 1, un divieto generale di trattamento dei dati *ivi* elencati:

> i dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

Il trattamento di questi dati, che con più facilità potrebbero portare a forme di discriminazione, implica l'osservanza, anche dal punto di vista formale, di regole più rigorose; la tutela del diritto del singolo viene garantita da più stringenti requisiti ed obblighi di carattere giuridico e tecnico in capo al titolare del trattamento.

Tipologia paradigmatica di categoria particolare di dato personale è quella che riguarda i dati relativi allo stato di salute. Questi sono talvolta definiti come «sensibilissimi» poiché costituiscono quelle informazioni maggiormente idonee a creare un danno rilevante all'interessato in caso di illecito trattamento. Talvolta si ricorre anche all'espressione «dato sanitario» che sarebbe, però, da circoscrivere ai dati trattati nel contesto medico-ospedaliero [Guarda 2017].

Il GDPR ha, infine, assurto i dati relativi alla salute al rango di definizione. L'art. 4, par. 1, n. 15 del GDPR, infatti, così recita:

> «dati relativi alla salute»: 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.

Il Considerando 35 si premura di meglio specificare:

> Nei dati personali relativi alla salute dovrebbero rientrare tutti i dati riguardanti lo stato di salute dell'interessato che rivelino informazioni connesse allo stato di salute fisica o mentale passata, presente o futura dello stesso. Questi comprendono informazioni sulla persona fi-

> sica raccolte nel corso della sua registrazione al fine di ricevere servizi di assistenza sanitaria o della relativa prestazione di cui alla direttiva 2011/24/UE del Parlamento europeo e del Consiglio […].

3.2.3 Altre definizioni di dati

Il GDPR ha aggiornato le definizioni della Direttiva 95/46 e ne ha introdotte di nuove. Di seguito alcune rilevanti ed utili per i fini di quest'Opera:

> «dati genetici»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione (art. 4, n. 13 GDPR);
>
> «dati biometrici»: 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 (art. 4, n. 14 GDPR);
>
> «pseudonimizzazione»: 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 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 (art. 4, pt. 14);
>
> «informazioni anonime», si intende le 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 (Considerando 26 del GDPR);
>
> «dati giudiziari»: i dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza (art. 10 GDPR).

3.2.4 Tra vecchi e nuovi principi

L'art. 5, par. 1 del GDPR elenca i principi base relativi al trattamento dei dati personali, riprendendo, con qualche novità, l'elencazione già presente nel quadro giuridico precedente [De Terwangne 2020]. Vediamo brevemente di seguito. I dati personali devono

– «essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato ("liceità, correttezza e trasparenza")» (lett. a):
  - per quanto concerne la «liceità», si tratta di un principio per certi versi ridondante, il cui scopo sarebbe quello di assicurare che il trattamento di dati rispetti non solo il GDPR ma anche tutte le carte sovranazionali dei diritti e le altre leggi nazionali, rispettando così il corretto bilanciamento tra gli interessi coinvolti. Un trattamento è lecito poi soltanto se per sua ciascuna attività è individuata una base giuridica o «base legittima»;
  - il concetto di «correttezza», invece, richiama l'obbligo per il titolare ed il responsabile di trattare i dati in modo tale da non abusare della posizione di squilibrio nei confronti degli interessati, anche se formalmente rispettoso delle norme di legge;
  - il principio di trasparenza è centrale nel nuovo assetto regolatorio stabilito dal GDPR e si connette ad una serie di maggiori obblighi informativi stabiliti in capo al titolare nell'informativa (artt. 13 e 14), alla più estesa portata del diritto di accesso (art. 15), delle comunicazioni in caso di violazione dei dati (art. 33), ecc.
– «raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»)» (lett. b):
  - la finalità gioca un ruolo centrale nel trattamento dei dati; in modo conforme ad essa si costruisce la modalità del trattamento. Si tratta di un principio tra i più importanti nel GDPR e sancisce appunto che la raccolta dei dati ed il loro successivo trattamento possano essere svolti solo in diretta connessione con la finalità esplicita e legittima che è stata dichiarata all'interessato.

- «adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»)» (lett. c):
  - questo principio è diretta conseguenza del principio di limitazione della finalità e impone che i dati personali raccolti non siano in alcun modo superflui, inutili o sovrabbondanti rispetto alla finalità.
- «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 («esattezza»)» (lett. d):
  - è interesse sia dell'interessato che del titolare che i dati raccolti siano accurati e rappresentino fedelmente la realtà.
- «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»)» (lett. e):
  - anche questo principio è direttamente connesso a quello relativo alla finalità, la quale determina il periodo di ritenzione dei dati; eccezioni a tale periodo possono permettere conservazioni più prolungate possono essere previste per fini di archiviazione nel pubblico interesse e ricerca, nel rispetto delle misure previste.
- «trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»)» (lett. f):
  - principio che impone la necessità che ogni trattamento assicuri l'adozione di adeguate misure tecnologiche ed organizzative volte a garantire la sicurezza e la protezione dei dati. Richiama i concetti di «confidentiality» e di «security by design».

Vera novità del GDPR è l'enfasi che viene posta sul concetto di «accountability» (o di «responsabilizzazione», se vogliamo usare la non felice versione italiana). Se nel quadro giuridico precedente, forzando e semplificando, si poteva sostenere che l'approccio fosse a «check-list» e che quindi il titolare dovesse in qualche modo adottare una serie di misure di sicurezza che venivano dettagliate dal legislatore nazionale, ora alcun riferimento preciso e fisso viene fornito. La valutazione del contesto e la scelta delle soluzioni atte a mitigarne i rischi sono completamente in capo a chi esegue il trattamento. Il par. 2 dell'art. 5 obbliga quest'ultimo all'osservanza di tutti i principi appena elencati:

> Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»).

L'art. 24 relativo alle responsabilità del titolare del trattamento è ancora più esplicito al paragrafo 1:

> 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.

Si sottolinea come non solo è importante adottare queste misure tecniche ed organizzative adeguate, ma occorre anche esser in grado di dimostrare la bontà delle valutazioni e delle scelte poste in essere. Questo enfatizza il ruolo della parte documentale delle previsioni del GDPR (e si lega ad alcuni nuovi requisiti, quali la tenuta del registro dei trattamenti di cui si dirà *ultra*).

L'accountability trova la sua prima espressione operativa nella cosiddetta «data protection by design». Il GDPR codifica, infatti, questo principio che è ritenuto essere centrale nell'approccio alla costruzione di piattaforme atte a gestire i dati sanitari. L'art. 25, par. 1, «Protezione dei dati fin dalla progettazione» impone, così, di incorporare i principi e le regole in materia di protezione dei dati personali a partire dalla progettazione del processo, anche e soprattutto a livello di soluzioni tecni-

co-informatiche. La previsione è ripresa e spiegata al Considerando n. 78, dove si richiede al titolare di adottare politiche interne e misure che soddisfino i principi della protezione dei dati fin dalla progettazione e per impostazione predefinita (ad es., la riduzione al minimo dell'utilizzo dei dati, la pseudonimizzazione, una maggiore trasparenza sulle funzioni e sullo stesso trattamento, ecc.). Questo tipo di considerazioni da porre in essere al momento della programmazione di un nuovo trattamento è sicuramente fondamentale nei contesti digitali, dove la costruzione di piattaforme digitali deve necessariamente essere guidata da un approccio di carattere interdisciplinare e tenere in debita considerazione, sin dalle fasi iniziali, l'importanza del fatto che i principi giuridici siano correttamente incorporati e realizzati nell'architettura informatica. La data protection by design si collega ad un altro principio: la cosiddetta «data protection by default», che richiede, infatti, l'adozione di misure tecniche e organizzative adeguate a garantire che solo i dati personali necessari per ogni specifica finalità del trattamento vengano elaborati (art. 25, par. 2, GDPR) [vedi → Capitolo 4] [Bincoletto 2021, Bygrave 2020b e Ratti 2021].

3.2.5 Base legittima del trattamento

Il trattamento di dati personali è lecito solo se consentito dal diritto dell'Unione europea sulla protezione dei dati. Pertanto, il titolare deve poter basare il proprio trattamento su uno specifico caso di liceità affinché l'attività che pone in essere non sia da considerarsi illecita appunto.

L'art. 6 stabilisce le condizioni per le quali un trattamento di dati personali può considerarsi lecito:

a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;
d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;

e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

Il «consenso» è una tra le possibili basi che legittimano il trattamento. Esso ha rappresentato storicamente la scelta di campo del legislatore europeo che ha fortemente enfatizzato il modello di «opt-in» per legittimare il trattamento dei dati (relegando lo schema, invece, basato sul c.d. «opt-out» (tratto i dati fino a che non mi viene chiesto il contrario) a una possibilità del tutto marginale quando non espressamente vietata). L'art. 4, pt. 11 così lo definisce:

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

Il GDPR ha introdotto dei profili più stringenti per la sua raccolta. Così recita l'art. 7:

1. 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.
2. Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Nessuna parte di una tale dichiarazione che costituisca una violazione del presente regolamento è vincolante.
3. L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di esprimere

il proprio consenso, l'interessato è informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato.
4. Nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto.

Elemento di novità è rappresentato dall'art. 8, il quale prevede la possibilità che, per quanto riguarda l'offerta diretta di servizi della società dell'informazione, i minori possano esprimere un consenso valido qualora abbiano compiuto almeno 16 anni (riducibile fino a 13 dal legislatore nazionale) [vedi → Capitolo 5].

Per quanto concerne il trattamento di categorie particolari di dati, come ricordato, l'art. 9, par. 1 apre con un divieto generale al loro trattamento. Tale divieto può essere superato qualora si configuri una tra le eccezioni previste al paragrafo 2:

a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1;
b) il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato;
c) il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso; d) il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità

e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato;

e) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;

f) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;

g) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato;

h) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al paragrafo 3;

i) il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale;

j) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

Si prevede, inoltre, che per il trattamento di dati genetici, biometrici o relativi alla salute gli Stati membri possano mantenere o introdurre ulteriori condizioni o limitazioni (art. 9, par. 4).

L'art. 9 va applicato in modo coordinato all'art. 6.

3.2.6 Ruoli

La disciplina europea in materia di protezione di dati personali si è sempre contraddistinta per aver cercato di associare ad un grande potere (quello relativo alla possibilità di trattare enormi quantità di dati) una grande responsabilità. Per far ciò vengono previsti una serie di ruoli che i vari soggetti impegnati nel trattamento devono ricoprire.

Al vertice di questa piramide c'è il «titolare del trattamento», ovvero

> 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 (art. 4, n. 7 GDPR).

Il titolare (*data controller*) riveste un ruolo chiave per le attività di trattamento perché, appunto, ne definisce finalità (il «perché») ed i mezzi, ossia le modalità e le misure con cui viene realizzato (il «come»). Qualora più titolari determinino congiuntamente le finalità e i mezzi del trattamento, ci troveremo in una situazione di «contitolarità». Diventerà allora obbligatorio redigere un apposito accordo interno volto a determinare in modo trasparente

> 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 (…) (art. 26, par. 1).

Qualora si renda, invece, necessario delegare alcune fasi del trattamento ad un soggetto esterno, avremo a che fare con il «responsabile del trattamento» (*data processor*), ovvero:

> la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento (art. 4, n. 8 GDPR).

Il titolare deve designare il responsabile con apposito contratto o accordo che definisca istruzioni e misure da applicare (art. 28, par. 3 GDPR). Questi è da individuarsi tra coloro 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 (art. 28, par. 1).

In questa categoria rientrano soggetti esterni e «legalmente separati», ad esempio quando si deleghi ad una società terza la gestione della posta elettronica della propria organizzazione, o la redazione delle buste paga dei propri dipendenti, ecc. Il quadro giuridico precedente al GDPR riconosceva il ruolo di responsabile anche a soggetti interni all'organizzazione: si pensi al caso del direttore della filiale di una banca, o del direttore di un dipartimento universitario. L'attuale regola ha obbligato ad escogitare nuovi nomenclatori per riferirsi a possibili partizioni della propria realtà organizzativa, per le quali non è più prevista una definizione a livello normativo, nonostante la loro fondamentale importanza come misure di sicurezza di carattere organizzativo. Le soluzioni trovate sono le più disparate (e questo può rappresentare un problema e creare confusione a livello pratico): «preposto al trattamento», «responsabile interno», ecc.

Elemento, infine, di novità è la previsione della possibilità per il responsabile di nominare un sub-responsabile, opzione non presente nel contesto normativo precedente e che molte difficoltà aveva creato nel mappare correttamente flussi di dati e scenari applicativi che vedevano il coinvolgimento di catene di *sub-contractor* legati al responsabile, ma che non avevano alcun collegamento, invece, con il titolare. Ai sensi del par. 2 dell'art. 28 ora il responsabile può ricorrere ad altro responsabile previa autorizzazione scritta, specifica o generale del titolare.

Nell'organigramma interno dei ruoli privacy troviamo, infine, l'«autorizzato», ovvero chiunque agisca sotto l'autorità del titolare o del responsabile del trattamento (art. 29 GDPR). Si tratta delle persone fisiche che materialmente trattano i dati personali. È fondamentale che la struttura documentale del titolare mappi correttamente i flussi di dati, tracciando ed autorizzando in modo coerente i singoli uffici e/o partizioni della pro-

pria realtà organizzativa in funzione dei trattamenti realmente necessari e posti in essere.

Una novità del GDPR, che ha ripreso una soluzione già adottata in altri Stati membri, è l'introduzione del «Responsabile della protezione dei dati», per riferirsi al quale nella prassi si usa più comunemente la versione inglese: «Data Protection Officer» (DPO). Questi è esperto nella protezione dei dati i cui compiti sono valutare ed organizzare la gestione del trattamento dei dati personali all'interno di ciascuna organizzazione (artt. 37, 38 e 39 GDPR). Il DPO dovrà informare e consigliare i vari soggetti coinvolti nel trattamento (titolare e responsabile), verificare l'esatta applicazione della disciplina in tema di protezione dei dati personali; fornire pareri in merito alla valutazione dell'impatto ed alla ottimizzazione delle misure adottate; fungere da contatto per gli interessati in merito al trattamento dei loro dati. Tale figura per agire efficacemente dovrà godere di una reale indipendenza e terzietà rispetto al titolare o al responsabile al trattamento. La nomina del DPO è obbligatoria in alcune circostanze (art. 37, par. 1):

> a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;
> b) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; oppure
> c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 [categorie particolari di dati] o di dati relativi a condanne penali e a reati di cui all'articolo 10 [dati giudiziari].

La designazione del DPO è, invece, una scelta in tutti i casi non esplicitamente previsti ma dove l'individuazione di questa figura potrebbe rappresentare una buona misura organizzativa per mitigare il rischio del trattamento.

Da ultimo abbiamo il c.d. «interessato al trattamento», ovvero la persona fisica cui si riferiscono i dati personali.

3.2.7 Obblighi di sicurezza e nuovi requisiti

Come visto il principio di integrità e riservatezza (art. 5, par. 1, lett. f)) impone l'adozione di misure di sicurezza adeguate. Il principio di accountability, poi, mette in capo al titolare il rispetto di questi principi e in generale la garanzia della protezione dei dati.

Collegata a questi principi è la previsione di cui all'art. 32 GDPR in tema di «Obblighi di sicurezza» che al primo paragrafo così recita [Esposito 2021]:

> 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
> b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
> c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
> d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Alcune, seppur brevi, precisazioni sono necessarie.

Anzitutto l'articolo fa riferimento a misure di sicurezza sia di carattere tecnico (come era sempre stato scontato) che di natura organizzativa: si chiarisce finalmente che la corretta mappatura dei flussi di dati, l'allocazione dei ruoli privacy, la gestione degli aspetti documentali relativi all'organizzazione del trattamento dei dati divengono veri e propri obblighi di sicurezza.

L'art. 32, inoltre, impone tali adempimenti non solo al titolare del trattamento, ma anche al responsabile il quale, per quanto di sua competenza, è investito di un obbligo esplicito e quindi direttamente azionabile all'implementazione di misure adeguate.

L'elencazione poi delle possibili misure di sicurezza ha natura solo esemplificativa e non è da considerarsi esaustiva (con ciò rimarcando ancora una volta il cambio di passo del GDPR rispetto al quadro giuridico precedente che, nelle declinazioni nazionali, presentava in modo dettagliato le soluzioni tecniche da garantire).

Infine, merita di essere sottolineato anche il paragrafo 4:

> Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

La formazione degli autorizzati diviene in modo esplicito misura di sicurezza: pertanto, la non corretta gestione di questo tipo di attività intra-organizzazione può divenire oggetto di sanzione da parte del Garante o dell'Autorità giudiziaria.

L'art. 32 in materia di obblighi di sicurezza è collegabile ad altre previsioni di cui al GDPR.

Anzitutto l'art. 30 prevede l'obbligo da parte del titolare e del responsabile della tenuta di un registro delle attività di trattamento, dove si richiama la necessità di porre in essere la descrizione dell'analisi dei rischi e soprattutto delle misure di sicurezza da implementare (par. 1, lett. g e par. 2, lett. d):

> 1. Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità. Tale registro contiene tutte le seguenti informazioni:
> a) il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
> b) le finalità del trattamento;
> c) una descrizione delle categorie di interessati e delle categorie di dati personali;
> d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;

e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.
2. Ogni responsabile del trattamento e, ove applicabile, il suo rappresentante tengono un registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento, contenente:
a) il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati;
b) le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;
c) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.
(…)

Sempre nella prospettiva di un potenziato diritto ad essere informato per l'interessato si deve fare riferimento alla «Notifica di una violazione dei dati personali all'autorità di controllo» sancita all'art. 33 (c.d. «data breach»): in caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente entro settantadue ore dal momento in cui ne è venuto a conoscenza. Nel caso in cui, però, tale violazione sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, e quindi certamente nell'ipotesi riguardante il trattamento di dati sanitari, l'obbligo di notifica viene esteso anche nei confronti dell'interessato (art. 34). Facciamo un esempio applicativo. Nel caso vi sia una vio-

lazione del sistema informativo di gestione dei dati di login (di studenti o personale) tale da creare un pericolo concreto per le credenziali gestite dal sistema, il Titolare (eventualmente supportato dal Responsabile, se individuato) eseguirà una valutazione prudenziale della violazione. Per il caso di specie, si potrebbero delineare tre scenari esemplificativi:

– scenario A - il sistema di gestione delle credenziali usato dal titolare archivia in chiaro le credenziali: il titolare deve notificare, entro 72 ore dal momento in cui ne è venuto a conoscenza, la violazione all'Autorità di Controllo e agli interessati;
– scenario B - il sistema di gestione delle credenziali usato dal titolare cifra le credenziali in modo irreversibile: il titolare deve notificare, entro 72 ore dal momento in cui ne è venuto a conoscenza, la violazione all'Autorità di Controllo e facoltativamente agli interessati;
– scenario C - il sistema di gestione delle credenziali usato dal titolare cifra le credenziali in modo irreversibile e ha una gestione separata dei sistemi di login rispetto alle risorse che le identificano: il titolare valuta se notificare la violazione all'autorità di controllo.

Infine, come sopra ricordato la data protection by design impone a chi tratta dati personali di operare già in fase di progettazione una ponderazione delle criticità che le attività comportano per gli utenti. L'analisi dei rischi diviene, pertanto, un aspetto caratteristico del Regolamento, il quale prevede la necessità di porre in essere una valutazione d'impatto sulla protezione dei dati («Data Protection Impact Assessment» – DPIA). L'art. 35, par. 1, del GDPR stabilisce, infatti, che:

> 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.

Una valutazione deve almeno contenere (par. 7):

– una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento;

– una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
– una valutazione dei rischi per i diritti e le libertà degli interessati;
– le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al GDPR, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione

La DPIA va sicuramente realizzata nei casi previsti nell'Allegato 1 al Provvedimento n. 467 dell'11 ottobre 2018 del Codice Privacy (e dalle «Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679», adottate dal WP29 il 4 aprile 2017).

3.2.8 Diritti dell'interessato

Marchio di fabbrica del legislatore europeo e ancora una delle parti più rilevanti del Regolamento è quella dedicata ai diritti dell'interessato, previsti agli articoli 13-22 [Calisai 2019]:
– diritto a ricevere informazioni (artt. 13 e 14);
– diritto di accesso (art. 15);
– diritto alla rettifica (art. 16);
– diritto alla cancellazione («diritto all'oblio») (art. 17) [vedi → Capitolo 8];
– diritto alla limitazione di trattamento (art. 18);
– diritto alla portabilità dei dati (art. 20);
– diritto di opposizione (art. 21);
– diritto a non essere sottoposto ad una decisione interamente automatizzata [vedi → Capitolo 13].

Questi diritti operano secondo particolari circostanze: non sono quindi sempre applicabili e possono essere limitati in presenza di alcune condizioni. Dovrà, pertanto, essere valutato di volta in volta l'operatività del diritto esercitabile dall'interessato.

Una specifica menzione merita il riconoscimento di un nuovo diritto: il «diritto alla portabilità» (*right to data portability*) di cui all'art. 20 [Falce 2021]:

1. L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti.

a) il trattamento si basi sul consenso ai sensi dell'articolo 6, paragrafo 1, lettera a), o dell'articolo 9, paragrafo 2, lettera a), o su un contratto ai sensi dell'articolo 6, paragrafo 1, lettera b); e

b) il trattamento sia effettuato con mezzi automatizzati.

2. (…) L'interessato ha il diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro, se tecnicamente fattibile.

Questa previsione impatta fortemente sull'attività dei titolari che devono porsi il problema di sviluppare soluzioni di carattere tecnico atte a rispondere alle richieste di portabilità dei dati. Essa è, però, fondamentale per far rimanere aperto il mercato dei service provider i quali altrimenti avrebbero di fatto negli anni goduto di una posizione di monopolio dovuta all'inevitabile effetto di lock-in tecnologico degli utenti con le piattaforme. Permette anche all'interessato di rimanere nel controllo dei propri dati personali potendo così scegliere verso quale società di servizi dell'informazione rivolgersi.

3.2.9 Certificazioni e codici di condotta

L'art. 42 GDPR prevede le certificazioni: strumento a carattere volontario ed accessibile seguendo un'apposita procedura trasparente. Gli Stati membri, le autorità di controllo, l'European Data Protection Board e la Commissione incoraggiano l'istituzione di meccanismi di certificazione della protezione dei dati nonché di sigilli e marchi di protezione dei dati allo scopo di dimostrare la conformità alla disciplina europea in materia di protezione dei dati personali. Il titolare del trattamento o il responsabile del trattamento che sottopone il trattamento effettuato al meccanismo di certificazione fornisce all'organismo di certificazione o all'autorità di controllo competente tutte le informazioni e l'accesso alle attività di trattamento necessarie a espletare la procedura di certificazione (par. 6).

La certificazione è rilasciata al titolare del trattamento o responsabile del trattamento per un periodo massimo di tre anni e può essere rinno-

vata alle stesse condizioni purché continuino a essere soddisfatti i criteri pertinenti (par. 7). In ogni caso, la certificazione ai sensi del GDPR non riduce la responsabilità del titolare del trattamento o del responsabile del trattamento riguardo alla conformità al Regolamento e lascia impregiudicati i compiti e i poteri delle autorità di controllo competenti.

L'art. 40 GDPR prevede, invece, i «codici di condotta»:

> Gli Stati membri, le autorità di controllo, il comitato e la Commissione incoraggiano l'elaborazione di codici di condotta destinati a contribuire alla corretta applicazione del presente regolamento, in funzione delle specificità dei vari settori di trattamento e delle esigenze specifiche delle micro, piccole e medie imprese.

Le associazioni e gli altri organismi rappresentanti le categorie di titolari del trattamento o responsabili del trattamento possono elaborare i codici di condotta, modificarli o prorogarli, allo scopo di precisare l'applicazione del Regolamento relativamente a (par. 2):

a) il trattamento corretto e trasparente dei dati;
b) i legittimi interessi perseguiti dal responsabile del trattamento in contesti specifici;
c) la raccolta dei dati personali;
d) la pseudonimizzazione dei dati personali;
e) l'informazione fornita al pubblico e agli interessati;
f) l'esercizio dei diritti degli interessati;
g) l'informazione fornita e la protezione del minore e le modalità con cui è ottenuto il consenso dei titolari della responsabilità genitoriale sul minore;
h) le misure e le procedure di cui agli articoli 24 e 25 e le misure volte a garantire la sicurezza del trattamento di cui all'articolo 32;
i) la notifica di una violazione dei dati personali alle autorità di controllo e la comunicazione di tali violazioni dei dati personali all'interessato;
j) il trasferimento di dati personali verso paesi terzi o organizzazioni internazionali; o k) le procedure stragiudiziali e di altro tipo per comporre le controversie tra titolari del trattamento e interessati in materia di trattamento, fatti salvi i diritti degli interessati ai sensi degli articoli 77 e 79.

Il codice di condotta deve contenere i meccanismi che consentono all'Autorità Garante di effettuare il controllo obbligatorio del rispetto delle norme del codice da parte dei titolari del trattamento o dei responsabili del trattamento che si impegnano ad applicarlo, fatti salvi i compiti e i poteri delle autorità di controllo competenti (par. 4).

L'adesione ad un codice di condotta o ad un meccanismo di certificazione approvato può essere utilizzata come elemento per dimostrare la conformità e il rispetto degli obblighi da parte del titolare del trattamento. Il Garante al momento di decidere se infliggere una sanzione amministrativa pecuniaria e fissare l'ammontare della stessa affinché questa risulti, per ogni singolo caso, effettiva, proporzionata e dissuasiva, potrà tenere in debito conto anche dell'adesione ai codici di condotta approvati ai sensi dell'articolo 40 o ai meccanismi di certificazione approvati ai sensi dell'articolo 42.

CAPITOLO 4.
Data protection by design e by default

Giorgia Bincoletto

4.1 Code is law e Privacy by design

Il GDPR ha modificato e aggiornato il quadro normativo europeo in materia di protezione dei dati personali, adeguandolo alle esigenze di tutela richieste dall'era digitale e prevedendo, rispetto al passato, ancor più stringenti obblighi per i titolari del trattamento e principi e diritti a tutela degli interessati. In questo capitolo si affrontano due degli approcci più innovativi in materia di protezione dei dati personali positivizzati dal Regolamento: la protezione dei dati fin dalla progettazione, o «Data Protection by Design» (DPbD), e la protezione per impostazione predefinita, o «Data Protection by default» (DPbDf).

Per approfondire questi temi è necessario presentare brevemente la nozione di «code is law» e ripercorrere il processo ultraventennale di evoluzione dal concetto di *privacy by design* - che nasce come elaborazione dottrinale in Canada e viene poi adottato a livello di policy in alcuni ordinamenti giuridici, tra cui gli Stati Uniti - alla definizione di due distinti obblighi codificati nel diritto europeo a protezione dei dati personali.

Come emerge dai precedenti capitoli, la rivoluzione tecnologica ha provocato importanti conseguenze per la tutela dei diritti alla riservatezza e alla protezione dei dati personali. Le nuove tecnologie digitali e le pratiche commerciali ad esse collegate raccolgono ingenti quantità di dati personali e invadono la vita privata e l'intimità degli individui.

Il *design* di queste tecnologie e dei processi organizzativi influisce sulle sfere giuridiche dei soggetti e sui loro diritti della personalità. Così si esprime Woodrow Hartzog, Professor of Law and Computer Science della Northeastern University, School of Law [Hartzog 2018, 34]:

> If the first truth of design is that it is everywhere, the second truth of design is that it is also a form of power. Power has been defined as «the capacity or ability to direct or influence the behaviour of others or the course of events». Given how design can shape our perceptions, behaviour, and values, power and design often feel like synonyms. Design is power because people react to design in predictable ways. This means that with the right knowledge, design can impose some form of order on chaos.

Il *design*, inevitabilmente, plasma le scelte, condiziona i comportamenti degli utenti e dei consumatori e si rivela una fonte di potere. Si pensi, ad esempio, alle funzioni esistenti sui social network che hanno influenzato e creato un nuovo modo di comunicare, ricevere e fornire informazioni.

Nell'era digitale le regole che governano i fenomeni e risolvono i problemi non sono poste soltanto dal diritto, e così, come definito dai comparatisti, dai suoi formanti legislativo, giurisprudenziale e dottrinale [Sacco, Rossi 2019]. Le regole derivano anche dal mercato, dalla società e dalla tecnologia [Lessig 1999]. La tecnologia, infatti, può incorporare delle regole e influenzare i comportamenti umani.

La regolamentazione attraverso la tecnologia è parallela al diritto, al mercato e alle norme sociali ed è stata definita «lex informatica» dalla dottrina giuridica statunitense del secolo scorso [Reidenberg 1998]. Le norme tecniche operano automaticamente, secondo la strutturazione, i vincoli e i limiti che vengono predefiniti dallo sviluppatore. Secondo Lawrence Lessig, Roy L. Furman Professor of Law and Leadership alla Harvard Law School, il codice informatico ha una portata normativa, in altre parole: «code is law» [Lessig 1999].

Se nello spazio reale sono le norme giuridiche, come le costituzioni, i codici, le pronunce giurisprudenziali, a regolamentare i fenomeni, nel cyberspazio è principalmente il codice, nelle sue componenti software e hardware, che li rende possibili e li governa. Come la rampa di accesso condiziona la raggiungibilità di un edificio nel mondo reale, o i limiti

settati al motore di un autoveicolo ne regolano la velocità massima, il meccanismo di autenticazione in un sito determina l'accessibilità di un servizio e la modalità di una firma elettronica garantisce l'autenticità della sua provenienza.

Generalmente, le regole di condotta operano in confini giurisdizionali, sono definite per guidare i consociati, che sono liberi di assecondarle o meno, sono prodotte da un sistema di fonti e interpretate da un giudice o un altro operatore del diritto *ex post*. Il codice, inteso come tecnologia, invece, regola i fenomeni *ex ante*, secondo una configurazione che si esegue in modo automatico, non dipende da un ordinamento giuridico, poiché il suo spazio è la Rete, ed è previamente stabilita dallo sviluppatore, ossia, nella maggior parte dei casi, da un soggetto privato [Bincoletto 2021a, 39].

Diritto e tecnologia sono entrambi fonti di regole nell'era digitale. Il *design* della tecnologia incorpora principi e valori e non è mai neutro. L'approccio informatico di Value Sensitive Design promuove infatti lo sviluppo delle tecnologie in una modalità che possa tenere conto di valori riconosciuti dall'uomo come particolarmente rilevanti [Davis et al. 2015].

Ciò posto, il diritto può utilizzare la tecnologia come strumento e influenzarne lo sviluppo per creare nuove forme di tutela e normatività. Si prospetta, quindi, uno scenario in cui le regole del diritto dell'era digitale possono essere incorporate dalla tecnologia stessa, secondo l'approccio di *code is law* [Spedicato 2009].

Un ambito giuridico nel quale l'incorporazione delle regole è stata largamente utilizzata è la proprietà intellettuale. In particolare, si segnalano le norme in materia di protezione del diritto d'autore disciplinate negli Stati Uniti dal Digital Millennium Copyright Act del 1998, che ha introdotto i «digital rights management» (DRM), misure tecnologiche che consentivano ai titolari del copyright e dei diritti connessi di controllare l'accesso e l'utilizzo delle opere creative o di altri materiali protetti [Caso 2004].

In concreto, i DRM sono sistemi di sicurezza, come la cifratura, implementati direttamente nei supporti digitali quali computer, apparecchi di riproduzione e file system, per impedire che un contenuto protetto dal copyright o da un diritto connesso sia copiato o riprodotto senza autorizzazione. Si ricorda che i DVD dei film non potevano essere masterizzati senza l'utilizzo di una licenza e la loro decodifica illegale risultava in

una condotta di pirateria. Oggigiorno, gli e-book file non possono essere riprodotti da dispositivi diversi da quelli che li hanno acquistati o che dispongono dei requisiti di accesso.

Per evitare violazioni del diritto d'autore, sono stati sviluppati meccanismi di controllo delle opere protette fin dalla progettazione del supporto attraverso il quale sono distribuite ed utilizzate. Da ciò si ottiene una protezione *ex ante* del diritto tutelato. Nell'Unione europea la direttiva 2001/29/EC «sull'armonizzazione di tali aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione», tuttora in vigore, ha previsto la creazione di misure tecnologiche destinate a impedire o limitare atti non autorizzati su opere e materiali protetti, e così limitare la copiatura e la riproduzione indiscriminata (art. 6).

A partire dagli anni Novanta del secolo scorso, l'approccio di *code is law* è stato adattato all'ambito di protezione della riservatezza e dei dati personali, intese come privacy and *informational* privacy. È così iniziato lo sviluppo delle Privacy Enhancing Technologies (PETs), misure tecnologiche atte a preservare la confidenzialità e l'identità degli individui nella Rete, per tutelare l'anonimato e la segretezza delle comunicazioni elettroniche [Bygrave 2017].

La canadese Ann Cavoukian, quale Information and Privacy Commissioner dell'Ontario dal 1997 al 2014, ha per prima elaborato la nozione di «privacy by design» (PbD). Secondo questa studiosa, è intesa PbD la realizzazione di un progetto che consideri la privacy fin dal principio, a partire dalla creazione di un prodotto o dalla progettazione di un servizio [Cavoukian 2010].

Sette principi fondativi chiariscono questa prospettiva [Cavoukian 2012]:

– *Proactive not reactive, Preventative not remedial* (Proattivo non reattivo, preventivo non correttivo). L'approccio di PbD aspira a prevenire i rischi per la riservatezza identificandoli proattivamente durante un iniziale «privacy impact assessment». A ciò consegue che le invasioni della riservatezza e sui dati sono preventivate e prevenute, e che un programma di protezione è definito fin dal principio da chi gestisce le informazioni;
– *Privacy as the Default Setting* (Privacy come impostazione predefinita). Questo principio richiede che i dati personali siano automaticamente protetti nel sistema tecnologico utilizzato e durante le pratiche

commerciali, in modo che, anche quando non sia richiesta un'azione positiva da parte dell'individuo, la sua privacy sia protetta per impostazione predefinita; a questo fine, si consiglia, ad esempio, di minimizzare la raccolta del dato;
– *Privacy Embedded into design* (Privacy incorporata nella progettazione). Il terzo principio richiede di integrare la privacy nel design dei prodotti come essenziale componente della funzionalità della tecnologia, inserendola direttamente nella sua architettura, tramite specifiche misure;
– *Full functionality – Positive-sum, Not zero-sum* (Massima funzionalità, valore positivo e non valore zero). L'approccio intende soddisfare tutti gli interessi e gli obiettivi in gioco, effettuando un bilanciamento in concreto, anche in materia di sicurezza e non limitando l'innovazione;
– *End-to-end security – full lifecycle protection* (Sicurezza e protezione fino alla fine, durante tutto il ciclo di vita del prodotto o servizio). La protezione proattiva deve essere mantenuta per tutta la durata del trattamento dei dati, affinché la sua gestione sia conforme alla normativa e sicura dall'inizio alla fine del ciclo di vita delle informazioni;
– *Visibility and transparency – keep it Open* (Visibilità e trasparenza). Il singolo utente deve poter verificare e controllare le operazioni compiute sui suoi dati personali. Le pratiche commerciali devono, quindi, essere trasparenti e chiare;
– *Respect for User Privacy – keep it User-Centric* (Rispetto per la privacy dell'utente, centralità dell'utente). La PbD, infine, impone di considerare gli interessi dell'individuo al centro del sistema e degli aspetti organizzativi; perciò, devono innanzitutto essere garantite informative e impostazioni predefinite a suo primario vantaggio.

In Europa, nel 2009, l'approccio di PbD è stato richiamato dal WP29 e dal Working Party on Police and Justice nel documento «Future of Privacy» quale principio da inserire nel quadro giuridico unionale a protezione dei dati personali. Secondo queste autorità, la *privacy by design* può rappresentare uno strumento per innovare il sistema normativo e proteggere, assieme alle PETs, gli interessati durante l'uso delle tecnologie digitali.

L'anno successivo ha rappresentato un punto di svolta per il principio. La trentaduesima International Conference of Data Protection Authorities and Privacy Commissioners - conferenza che vede partecipi autorità di 76 paesi nel mondo - ha elaborato il documento programmatico «Resolution on Privacy by Design», in cui l'approccio è stato considerato fondamentale per affrontare i cambiamenti tecnologici, vista l'insufficienza della regolamentazione esistente, ed è stato promosso come principio olistico di diritto internazionale in materia di protezione dei dati. Nel 2010, la riflessione sulla PbD è mutata da un livello dottrinale ad un piano più organizzativo, nella prospettiva di sua promozione a livello di policy e di riforma legislativa.

La prima proposta di legge contenente un esplicito riferimento al principio deriva dal lavoro di due senatori statunitensi che nel 2011 hanno promosso il Commercial Privacy Bill inserendo una sezione contenente un obbligo per le società commerciali (se «covered entities») di incorporare nelle loro pratiche commerciali delle misure protettive della privacy per tutto il ciclo di vita delle informazioni (Section 103). Questa proposta non è mai stata approvata dal Congresso, ma il dibattito sul tema è stato colto dalla Federal Trade Commission degli Stati Uniti che nel 2012 ha inserito la PbD quale pratica commerciale raccomandata per proteggere i dati dei consumatori.

Nel report «Protecting Consumer Privacy in an Era of Rapid Change, Recommendations for Business and Policy Maker» l'autorità statunitense include la PbD tra le sue «best commercial practice» ed esorta il Congresso a pianificare una riforma legislativa per tutelare i consumatori. Negli anni successivi alcune pratiche commerciali di società operanti nel territorio americano sono state sanzionate per attività scorrette sulla base della Section 5 del Federal Trade Commercial Act e di politiche non rispettose di un approccio organizzativo orientato alla privacy by design [Bincoletto 2019]. Tuttavia, un riconoscimento a livello legislativo è tuttora assente nell'ordinamento giuridico statunitense sia a livello federale che statale. Anche l'ordinamento canadese, seppur culla delle prime riflessioni sul tema, non ha ancora incluso una normativa specifica che incentivi l'adozione di misure proattive per proteggere la privacy.

Soltanto nella proposta europea di Regolamento sulla protezione dei dati (2012) e nella versione definitiva del Regolamento poi (2016) è stato inserito formalmente un obbligo che può essere considerato comparabi-

le al concetto di privacy by design. Prima di analizzare l'art. 25 del GDPR, è opportuno chiarire opportunità e sfide dell'adozione di un tale principio giuridico per la protezione dei dati personali.

Come anticipato, il concetto di privacy by design impone l'incorporazione delle regole e dei principi della privacy nelle soluzioni tecnologiche e nelle pratiche commerciali per rendere più effettiva la protezione dei soggetti interessati e prevenire i rischi. La PbD incentiva sia una metodologia di *privacy-by-architecture*, ossia l'implementazione nel *design* della tecnologia di misure protettive dei diritti (es. la crittografia), sia la *privacy-by-policy*, quale insieme di strategie organizzative e burocratiche (es. la predisposizione di documentazione e policy). La ratio della PbD è, dunque, di rafforzare la tutela già prevista dai principi e dai diritti dell'ordinamento giuridico, che risultano spesso insufficienti nel contesto digitale.

Come principi, a livello internazionale è possibile fare riferimento ai «Principles of Fair Information Practices», riferiti alla nozione di *informational* privacy. Questi sono stati definiti per la prima volta nel 1973 dall'Education & Welfare US Department of Health degli Stati Uniti, e successivamente rielaborati dall'Organisation for Economic Cooperation and Development (OECD) nel 1980. Nel 2013 l'OECD Privacy framework è stato revisionato, assumendo un ruolo chiave per la creazione di regole nazionali in ambito di protezione dei dati personali e nuove tecnologie. I suoi principi, che hanno influenzato la legislazione di molti ordinamenti giuridici, sono così riassumibili:

– *Collection Limitation*. La raccolta dei dati personali dovrebbe essere limitata e i dati dovrebbero essere ottenuti con mezzi leciti e corretti e, se del caso, con conoscenza o consenso dell'individuo;
– *Data Quality*. I dati personali dovrebbero essere pertinenti alle finalità e, nella misura necessaria per tali finalità, dovrebbero essere accurati, completi e aggiornati;
– *Purpose Specification*. Le finalità dovrebbero essere specificate al più tardi al momento della raccolta del dato e l'uso secondario dovrebbe essere limitato alla finalità principale o risultare compatibile con essa;
– *Use Limitation*. I dati personali non dovrebbero essere divulgati, resi disponibili o altrimenti utilizzati per finalità diverse da quelle specificate se non con il consenso della persona interessata o di un'autorità;

– *Security Safeguards*. I dati personali dovrebbero essere protetti con ragionevoli garanzie di sicurezza contro i rischi;
– *Openness*. Ci dovrebbe essere una politica generale di apertura e chiarezza sulla gestione dei dati personali;
– *Individual Participation*. Gli individui dovrebbero avere il diritto di ottenere informazioni, di cancellazione e rettifica con riferimento ai propri dati;
– *Accountability*. Il titolare del trattamento dei dati dovrebbe essere responsabile per l'adeguamento ai principi generali.

Questi principi, comparabili, ma non sovrapponibili, con quelli del GDPR, orientano verso una tutela complessiva e trasparente dei dati personali.

L'American Law Institute (ALI), prominente organizzazione di ricerca degli Stati Uniti [vedi → Capitolo 1], ha recentemente proposto una serie di principi per modernizzare i FIPs, introducendo, sulla scia del «Brussel Effect» [vedi → Capitolo 3], alcune nozioni simili a quelle dell'art. 5 del GDPR [Solove, Schwartz 2022]. In particolare, i principi della «data privacy law» sono: «transparency, individual notice, consent, confidentiality, use limitation, access and correction rights, data retention and disposal duties, data portability, data security, onward transfer, and accountability and enforcement». Nella descrizione dell'ultimo principio gli studiosi specificano che [Solove, Schwartz 2022, 27]:

> As part of achieving accountability, the Principles require an organization to develop a reasonable comprehensive privacy program. Such a program should include written privacy and security policies and procedures, personal-data inventory, risk assessment, training program, privacy and security by design, and privacy and security by default. For privacy by design, the Principles do not specify design choices. Mandating specific technological design is quite a challenging undertaking for law, and moreover, would likely face unified and strong opposition from the tech industry. Although the law probably should do more to regulate design, we were concerned about how to do this well while also being practical about not pushing U.S. law too far. The Principles, therefore, opt merely to require that «[d]esign choices and the reasoning that supports them shall be documented». Policymakers, regulators, and other actors can then evaluate these decisions. We leave it

> up to these parties to delve into the substance of design decisions on a case-by-case basis.

Incorporare le regole giuridiche nel *design* è molto complesso. Affinché l'approccio sia legittimato ed effettivamente implementato è opportuna una sua chiara codificazione legislativa, che preveda altresì sanzioni in caso di violazione. In un sistema di common law la sua affermazione potrebbe anche derivare dalla giurisprudenza. Tuttavia, vista la diversità delle regole in materia di protezione dei dati personali nei diversi sistemi giuridici, la PbD potrebbe essere adottata diversamente a seconda dei principi ritenuti vincolanti in un dato contesto applicativo.

Una previsione contenente la PbD dovrebbe essere definita in modo tecnologicamente neutrale per evitare che l'evoluzione e l'innovazione dei prodotti e dei servizi ne determini una rapida obsolescenza.

L'adozione di misure protettive e proattive dovrà, inoltre, avvenire caso per caso, tenendo conto del particolare contesto tecnologico e organizzativo in cui i dati sono raccolti e trattati. Incorporare le regole giuridiche è un'attività complessa poiché richiede:

- un'analisi di tutte le regole giuridiche in materia di protezione dei dati personali applicabili al dato contesto;
- un'interpretazione delle norme giuridiche da parte dell'operatore del diritto, consapevole che non tutte le previsioni sono codificabili e che tale operazione è necessariamente flessibile, dinamica e mutevole nel tempo;
- un'analisi interdisciplinare del contesto che coinvolga i vari operatori e portatori di interessi (tra cui, i soggetti con ruoli privacy, gli esperti di management, il giurista, l'informatico e l'ingegnere);
- un bilanciamento *ex ante* tra i diversi interessi e valori in gioco, che potrebbero essere in conflitto;
- una trasformazione del linguaggio naturale in un comando comprensibile dalla macchina e ingegnerizzabile;
- una trasformazione del linguaggio giuridico in una misura organizzativa chiara ed applicabile in concreto dagli operatori del settore;
- un aggiornamento delle soluzioni implementate, alla luce dello stato dell'arte della tecnologia e delle pratiche, secondo un programma operativo per tutto il ciclo di vita del dato personale.

La PbD comporta un approccio globale alla gestione dei dati, specifici investimenti e innovazioni. Un ruolo chiave dovrebbe essere assunto dagli sviluppatori dei prodotti e da chi crea e fornisce i servizi. Tale ruolo dovrebbe, in aggiunta, essere svolto con trasparenza, per rendere il più possibile comprensibili e accessibili le scelte compiute sul *design*. L'adozione di misure di PbD dovrebbe contribuire a costruire un sistema di fiducia nei confronti delle nuove tecnologie e contrastare le dinamiche dell'attuale sistema di capitalismo della sorveglianza operato dai giganti del Web [Zuboff 2019].

La nozione di PbD è rimasta un approccio olistico promosso dagli studiosi e dalle autorità fino alla previsione di una regola specifica e vincolante all'interno del GDPR, che richiede l'adozione di misure tecniche ed organizzative fin dalla progettazione del trattamento dei dati personali.

4.2 L'art. 25 del GDPR

Nel GDPR la norma di riferimento è l'art. 25, rubricato «protezione della vita privata fin dalla progettazione e protezione per impostazione predefinita, il quale prevede che:

1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.
2. Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per im-

postazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.

3. Un meccanismo di certificazione approvato ai sensi dell'articolo 42 può essere utilizzato come elemento per dimostrare la conformità ai requisiti di cui ai paragrafi 1 e 2 del presente articolo.

Questa norma è di complessa interpretazione [Jasmontaite 2018 e Rubinstein, Good 2019].

Richiamando all'attenzione le nozioni e le categorie del GDPR [vedi →Capitolo 3], si può affermare che la disposizione prescrive due obblighi generali del titolare del trattamento dei dati. Il responsabile del trattamento dovrà cooperare con questa figura secondo le istruzioni fornite nel contratto di nomina affinché le misure siano concretamente adottate (art. 28, Cons. 78 del GDPR). La mancata adozione di questi obblighi è soggetta a sanzione (artt. 82 e 83 GDPR). L'European Data Protection Board (EDPB) ha chiarito che l'esclusione degli sviluppatori dallo scopo della previsione legislativa è una rilevante limitazione, ma che le società produttrici dei prodotti e fornitrici di servizi dovranno adeguarsi e fornire le adeguate tutele per rimanere competitive nel mercato [EDPB 2020].

L'obbligo di adottare misure di data protection by design e by default è stato inserito anche nella Direttiva 2016/680 «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» (art. 20) e nel Regolamento 2018/1745 «con riguardo al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione europea» (artt. 27 e 85).

Con riferimento al primo paragrafo dell'art. 25, il titolare del trattamento deve implementare sia misure tecniche che organizzative, che risultano una parte di tutte le misure che devono essere adottate secondo il Regolamento (es. art. 24 in materia di accountability e 32 in materia di sicurezza).

Le misure devono essere appropriate e adeguate, come nel caso della pseudonimizzazione [vedi → Capitolo 12], e possono essere scelte secondo un bilanciamento che tenga conto sia di criteri oggettivi che soggettivi, ossia:

– dello stato dell'arte della tecnologia e delle pratiche, ossia di ciò che è attualmente presente sul mercato e riconosciuto come il più efficace per proteggere i dati personali;
– dei costi di attuazione, da intendersi come fattibilità economica. Perciò le misure potranno variare dalla dimensione e dal ruolo dell'organizzazione del titolare e dovranno considerare le tempistiche e le risorse, anche umane, che l'implementazione richiede;
– dei rischi posti dal trattamento che possono assumere diverse gravità per i diritti degli interessati e probabilità di verificarsi. Dovrà quindi essere compiuta un'adeguata analisi dei rischi, ulteriore rispetto alla valutazione di impatto o DPIA (art. 35 GDPR). Ciò conferma la centralità del concetto di rischio per il GDPR;
– delle caratteristiche concrete del trattamento, ossia della sua natura, dell'ambito di applicazione, del contesto e delle finalità. Per comprendere questi elementi si suggerisce di rispondere a queste domande: in cosa consistono le attività di trattamento dei dati personali? Quali sono le categorie di dati personali trattati? Qual è la finalità del trattamento? Quali sono i mezzi utilizzati (automatici o non)? Dove avvengono le attività? Quali sono le categorie di interessati coinvolti? Quali sono i destinatari dei dati?

Inoltre, le misure devono attuare in modo efficace i principi di protezione dei dati (art. 5) e integrare nelle attività di trattamento delle garanzie capaci di soddisfare i requisiti del Regolamento e di tutelare i diritti e le libertà degli interessati, ossia quanto previsto dagli artt. 12-22 GDPR e dalla Carta dei diritti fondamentali dell'Unione Europea (Carta di Nizza).

Di conseguenza, il titolare del trattamento deve implementare misure che rispettino ciascun principio e diritto stabilito dalla normativa. Una guida preziosa per individuare le varie misure è fornita dall'EDPB nelle «Guidelines 4/2019 on Article 25 Data Protection by Design and by Default», che forniscono degli elenchi (non esaustivi) di misure a seconda dei principi e dei diritti da garantire e suggeriscono l'utilizzo di «key performance indicators» per valutare a livello qualitativo e quantitativo quanto implementato [Bincoletto 2020].

La norma lascia ampia autonomia e discrezionalità al titolare del trattamento. Le misure, tuttavia, devono essere adottate fin dalla determinazione dei mezzi per il trattamento e per tutta la sua durata, ossia fino

alla cancellazione o effettiva anonimizzazione dei dati personali [su questa tecnica vedi → Capitolo 12]. Potrà, peraltro, essere necessaria una revisione delle scelte compiute e un adeguamento allo stato dell'arte e ai cambiamenti delle attività di trattamento.

Il secondo paragrafo dell'art. 25, inoltre, introduce l'obbligo di *data protection by default*. Il titolare del trattamento deve adottare misure tecniche e organizzative per minimizzare, per impostazione predefinita, la quantità di dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità dei dati. In questo modo, solo i dati personali necessari per ogni specifica finalità del trattamento saranno trattati ed essi non saranno accessibili indiscriminatamente senza un intervento dell'interessato che lo renda possibile.

Questo obbligo è volto alla particolare attuazione dei principi di minimizzazione, limitazione della finalità e della conservazione dei dati ed è espressione del diritto di accesso dell'interessato. La previsione incentiva la creazione di impostazioni predefinite a suo diretto vantaggio: se nulla viene modificato da un intervento dell'individuo, i dati sono tutelati con il grado maggiore di protezione possibile. Ciò ha un diretto impatto su come deve essere sviluppato il *design* della tecnologia.

In aggiunta, il terzo paragrafo della disposizione apre alla possibilità per il titolare di ottenere una certificazione che attesti la conformità delle attività del trattamento alla normativa. Tale meccanismo deve rientrare tra quelli riconosciuti come validi ai sensi degli artt. 42 e ss. del Regolamento. In Italia, ad esempio, è competente Accredia, Ente Unico nazionale di accreditamento.

L'art. 25 è una norma centrale all'interno del GDPR, ma non potrà essere compresa e applicata senza la lettura delle previsioni in materia di sicurezza (art. 32 GDPR), che richiedono l'adozione di ulteriori misure per l'integrità e confidenzialità dei dati personali, e senza un approccio interdisciplinare supportato da esperti sia legali che tecnici. Specifici approcci dell'ingegneria informatica studiano le metodologie adatte ad incorporare *by design* i requisiti normativi nei moduli funzionali del software e dei sistemi [Bincoletto 2021a, 377-403]. Solo uno sforzo congiunto creativo, che superi i limiti di comprensibilità e linguaggio tra le diverse professioni potrà determinare le soluzioni adeguate e appropriate per il contesto applicativo.

Da una comparazione con il concetto di PbD è possibile svolgere alcune considerazioni finali. Innanzitutto, la PbD è solitamente collegata ai FIPs, mentre la DPbD è stabilita nel quadro della protezione dei dati dell'UE. In generale, questa disciplina risulta più ampia e tutelante sia di quella riconosciuta nel contesto internazionale che di quella, ad esempio, derivante dai principi proposti dall'American Law Institute. Peraltro, dovrà essere considerata anche la Carta dei diritti fondamentali dell'UE (Carta di Nizza) perché l'art. 25 include le salvaguardie ai «diritti e alle libertà», dopo aver menzionato i requisiti del GDPR.

Entrambi i concetti rappresentano approcci proattivi. La PbD è un concetto internazionale percepito come un principio e sostenuto da studiosi e autorità che si occupano della protezione della privacy e dei dati personali. Come si evince dai sette principi fondativi, essa include la protezione per impostazione predefinita. La DPbD e la DPbDf sono, invece, disciplinate separatamente.

Mentre la DPbD è un obbligo pienamente applicabile, la PbD è ancorata ad una dimensione più visionaria ed etica. È evidente che la DPbD sia stata ispirata dal concetto di PbD, ma assume una connotazione molto più concreta e definita. Sono, tuttavia, entrambi molto complessi da attuare e lasciano ampio spazio a soluzioni personalizzate. Il GDPR non mira a creare barriere all'innovazione, ma a fornire un quadro di protezione dei dati più forte e coerente. In ogni caso, le due nozioni non dovrebbero essere utilizzate in modo intercambiabile. La DPbD non è sovrapponibile al concetto di PbD alla luce dei seguenti criteri [Bincoletto 2021a, 159]:

CRITERIO	PbD	DPbD
Ordinamento giuridico di riferimento	Riconoscimento a livello internazionale	Unione europea
Natura giuridica	Pratica raccomandata e principio	Obbligo e principio generale
Ambito giuridico	Riservatezza e protezione dei dati personali	Protezione dei dati personali
Principi da attuare	FIPs	Principi del GDPR e della Carta di Nizza
Diritti da attuare	Non specificato	Artt. 12-22 GDPR e della Carta di Nizza

Tempistica	Per tutto il ciclo di vita delle informazioni	Per tutto il ciclo di vita del trattamento dei dati
Flessibilità del concetto	Sì	Sì
Neutralità tecnologica del concetto	Sì	Sì
Soggetti che devono attuare	Tutti i portatori di interesse	Titolare del trattamento
Presenza del concetto di Privacy by Default	Incluso nella nozione	Obbligo separato
Presenza degli aspetti di sicurezza	Incluso nella nozione	Obbligo separato

4.3 Casi 4-1, 4-2, 4-3

Caso 4-1

La società di telefonia Alfa, stabilita in Lussemburgo, raccoglie i dati dei clienti, inclusi indirizzi e numeri di telefono, per fornire i suoi servizi in vari stati, tra i quali l'Italia. Tra le sue attività essa intende promuovere nuove offerte e promozioni con una rete di venditori terzi a sé associati (c.d. telemarketing). Centinaia di interessati lamentano continui contatti telefonici promozionali indesiderati. In particolare, da un'istruttoria emerge che ad essere contattati sono sia clienti che ex-clienti della società e che le telefonate vengono effettuate da call-center partner di Alfa. Le liste di contatti vengono ricavate direttamente dai sistemi gestionali di Alfa, disponibili in cloud.
Qual è il problema giuridico?
In cosa consistono le attività di trattamento dei dati personali?
Quali sono le categorie di dati personali trattati?
Qual è la base giuridica applicabile e la finalità del trattamento?
Quali sono i mezzi utilizzati?
Quali sono gli interessi da porre in bilanciamento?
Quali misure tecniche possono essere implementate per tutelare gli interessati?
Quali misure organizzative?

Caso 4-2

La rete televisiva Beta produce il programma «Gli sciacalli» in cui si trasmettono servizi di cronaca ed attualità. Durante una puntata viene

riprodotta un'intervista a Tizio, medico di base di una piccola cittadina, a cui il giornalista, con telecamera nascosta e sotto mentite spoglie, chiedeva insistentemente se le numerose morti della zona a causa di tumori fossero ricollegabili ad un impianto di smaltimento rifiuti presente a pochi chilometri dal centro abitato e alla cattiva gestione dei proprietari. La voce e l'immagine di Tizio vengono alterate, ma la sua identità rimane riconoscibile. A seguito della trasmissione, il medico viene denunciato dai gestori dell'impianto per diffamazione. A questo punto, Tizio si rivolge al Garante per la protezione dei dati personali lamentando la violazione delle regole del GDPR.
Qual è il problema giuridico?
Chi è il titolare del trattamento?
In cosa consistono le attività di trattamento dei dati personali?
Qual è la base giuridica applicabile e la finalità del trattamento?
Quali sono i mezzi utilizzati?
Quali sono gli interessi da porre in bilanciamento?
Quali misure tecniche possono essere implementate per tutelare l'interessato?
Quali misure organizzative?

Caso 4-3

La società Gamma si dota di un gestionale per la segnalazione interna di condotte illecite e scorrette dei dipendenti, dei collaboratori e dei vertici aziendali (c.d. Whistleblowing). Le segnalazioni sono effettuabili tramite l'utilizzo delle credenziali aziendali e i dati sono archiviati in un cloud storage fornito da una società privata responsabile del trattamento fornitrice del sistema. Per impostazione predefinita solo un soggetto indipendente dai vertici aziendali dovrebbe accedere ai dati delle segnalazioni. Durante un indagine dell'autorità Garante emerge tuttavia che gli amministratori delegati della società Gamma e della società responsabile dispongono di credenziali di accesso per entrare nel sistema di segnalazione.
Qual è il problema giuridico?
In cosa consistono le attività di trattamento dei dati personali?
Qual è la base giuridica applicabile e la finalità del trattamento?
Quali sono i mezzi utilizzati?
Quali sono gli interessi da porre in bilanciamento?
Quali misure tecniche possono essere implementate per tutelare l'interessato?
Quali misure organizzative?

CAPITOLO 5.
Il diritto alla protezione dei dati: una prospettiva comparata

Giorgia Bincoletto

5.1 Le regole a protezione dei dati personali

Il diritto alla protezione dei dati personali può essere definito come il diritto al controllo sul flusso, sulla circolazione, dei dati personali che identificano o possono identificare la persona fisica, o come diritto all'autodeterminazione informativa, ossia ad autodefinirsi e determinarsi in prima persona sulla cessione e sull'uso dei dati. In poche parole, questo diritto riguarda la titolarità dei dati personali e la loro protezione [Tosi 2019]. Il controllo sui dati ha un'ampia portata e si estende dall'accesso alla rettifica [Finocchiaro 2019]. Questo diritto è spesso definito con le espressioni inglesi «informational privacy» o «data privacy», che pongono attenzione al nucleo informazionale del dato personale, concetto di volta in volta definito dall'ordinamento giuridico.

La comparazione giuridica assume particolare importanza. Lo studio del diritto comparato, infatti, mira a stabilire le similarità e le differenze tra gli ordinamenti, consente di conoscere meglio non solo altri contesti, ma anche quello interno, e impone di analizzare sia le norme positive che le decisioni giurisprudenziali e gli approdi dottrinali [Resta, Somma, Zeno Zencovich 2020, Sacco, Rossi 2019, Somma 2019 e Monateri 2014]. Si possono comparare singole regole giuridiche (micro-comparazione) o la complessità delle tutele previste dall'intero sistema (macro-comparazione).

Come anticipato, il diritto alla protezione dei dati personali è uno dei diritti fondamentali dell'Unione europea per la presenza dell'art. 8 della Carta di Nizza. Secondo questa disposizione ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano e tali dati devono essere trattati secondo il principio di lealtà, utilizzati per finalità determinate (finalità del trattamento) e raccolti in base al consenso della persona interessata o ad un altro fondamento legittimo previsto dalla legge (base giuridica del trattamento). Ogni individuo ha il diritto di accedere ai dati raccolti e di ottenerne la rettifica, qualora siano mutate e variate le circostanze. Il rispetto delle regole in materia è soggetto al controllo di un'autorità indipendente. L'art. 16, par. 2, del Trattato sul funzionamento dell'Unione Europea costituisce la base per introdurre norme in materia a livello legislativo. Così è stato previsto il GDPR [vedi → Capitolo 3], che si sta rilevando un modello di protezione imitato in altri ordinamenti giuridici.

A livello internazionale il primo strumento vincolante in materia di protezione dei dati personali è stato la Convenzione del Consiglio d'Europa del 28 gennaio 1981, n. 108 sulla protezione delle persone rispetto al trattamento automatizzato di dati personali, entrata in vigore nel 1985. Questa Convenzione, modificata con il Protocollo CETS No. 223 nel 2018, e oggi conosciuta come Convention 108+, è ancora oggi l'unica normativa cogente di tale portata, sottoscritta da 55 paesi in tutto il mondo ed espressione dell'art. 8 della Cedu. La Convenzione può essere ratificata anche da paesi non appartenenti al Consiglio d'Europa (art. 27).

In breve, questa normativa richiede che il trattamento dei dati sia proporzionato alla legittima finalità perseguita, rappresenti l'esito di un adeguato bilanciamento tra tutti gli interessi coinvolti, pubblici e privati, tra tutti i diritti e le libertà in gioco (art. 5, par. 1), e sia basato su un consenso libero, specifico, informato e non ambiguo o su un'altra base legittima prevista dalla legge (art. 5, par. 2). I dati personali devono essere (art. 5, par. 4):

– trattati in modo equo e trasparente;
– raccolti per finalità esplicite, specifiche e legittime e non trattati in modo incompatibile con tali finalità; l'ulteriore trattamento per finalità di archiviazione nel pubblico interesse, per finalità di ricerca scientifica o storica o per finalità statistiche è, con le dovute garanzie, compatibile con tali scopi;

– adeguati, pertinenti e non eccedenti rispetto alle finalità per le quali vengono trattati;
– esatti e, se necessario, aggiornati;
– conservati in una forma che consenta l'identificazione degli interessati per un periodo di tempo non superiore a quello necessario alle finalità per le quali sono trattati.

La Convenzione 108+, inoltre, garantisce all'interessato i seguenti diritti (art. 9):
– il diritto a non essere sottoposto a una decisione che produca effetti significativi e sia basata esclusivamente su un trattamento automatizzato dei dati, senza che il suo punto di vista venga preso in considerazione;
– il diritto ad ottenere, su richiesta, a intervalli ragionevoli e senza ritardi o spese eccessive, la conferma del trattamento dei dati personali che lo riguardano, la comunicazione in forma intelligibile dei dati trattati, di tutte le informazioni disponibili sulla loro origine e sul periodo di conservazione, nonché ogni altra informazione che il titolare del trattamento è tenuto a fornire al fine di garantire la trasparenza del trattamento (art. 8, par. 1);
– il diritto di ottenere, su richiesta, la conoscenza della motivazione alla base della quale è stata presa una decisione per il trattamento dei dati, quando i risultati di tale decisione sono applicati alla sua persona;
– il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione, al trattamento di dati personali che lo riguardano, a meno che il titolare del trattamento non dimostri l'esistenza di motivi legittimi per il trattamento, che prevalgano sui suoi interessi o sui suoi diritti e libertà fondamentali;
– il diritto di ottenere, su richiesta, gratuitamente e senza ritardi eccessivi, la rettifica o la cancellazione dei dati se sono o sono stati trattati in violazione delle disposizioni della Convenzione;
– il diritto di disporre di un rimedio qualora i suoi diritti siano stati violati (art. 12);
– il diritto di beneficiare, a prescindere dalla sua nazionalità o residenza, dell'assistenza di un'autorità di controllo nell'esercizio dei suoi diritti (art. 15).

Il titolare del trattamento deve garantire questi diritti, adottare adeguate misure di sicurezza a protezione dei dati (art. 7), fornire informazioni sulle attività che intende svolgere (art. 8) e dimostrare di aver rispettato le regole della Convenzione (art. 10).

Questo quadro normativo ha uno scopo materiale e territoriale più ampio del GDPR; confrontando i due testi è possibile rilevare che i principi base per il trattamento sono essenzialmente equivalenti [Ukrow 2018, 242]. Con riferimento alle prerogative dell'interessato, la Convenzione non garantisce un ampio diritto alla cancellazione dei dati e un diritto alla portabilità, novità del GDPR. La definizione della portata degli altri diritti è più limitata rispetto al regolamento europeo. Tuttavia, nel 2018 sono state compiute alcune integrazioni ai principi che tengono conto delle esigenze di trasparenza e comprensibilità richieste dalle tecnologie digitali e in particolare dal fenomeno dei Big Data [vedi → Capitolo 13].

La Convenzione 108+, più flessibile e aperta all'interpretazione del GDPR, è stata definita il possibile futuro «global standard» in materia di protezione dei dati; il GDPR, invece, rimarrebbe il «gold standard» a cui fare riferimento [Mantelero 2020].

Il Privacy framework dell'Organisation for Economic Cooperation and Development [vedi → Capitolo 4] è un'altra fonte che ha svolto e svolge un ruolo a livello internazionale come modello per l'introduzione di regole in ambito di protezione dei dati personali. I suoi principi, cd. Fair Information Practices, hanno infatti influenzato la legislazione di molti ordinamenti giuridici, soprattutto oltreoceano [Solove, Schwartz 2021].

Con la risoluzione n. 69/166 del 2014 l'Assemblea Generale delle Nazioni Unite riconosceva l'importanza della tutela della privacy, sollecitando gli stati membri a definire misure a sua protezione, specialmente nel contesto digitale. Nel 2016, le Nazioni Unite hanno creato il gruppo di lavoro chiamato «UN Privacy Policy Group» per unire gli sforzi a protezione della privacy e dei dati a livello internazionale e creare uno «UN system-wide framework» nella materia[1]. Grazie al lavoro di questo gruppo nel 2018 sono stati formalmente adottati i «Principles on Personal Data Protection and Privacy» dalle UN System Organisations. Questi principi

1 Si v. il sito ufficiale del gruppo in https://www.unglobalpulse.org/policy/un-privacy-policy-group/.

si applicano ai dati personali, intesi come informazioni riferite o riferibili ad una persona fisica e sono così sintetizzabili[2]:
– liceità, intesa come la presenza di una valida base giuridica, e correttezza del trattamento;
– limitazione delle finalità, che deve essere specifica;
– proporzionalità e necessità, limitando i dati a quanto necessario per il conseguimento della finalità;
– limitazione alla conservazione dei dati a quanto necessario;
– esattezza dei dati, nel senso che devono essere veritieri e, quando necessario, aggiornati;
– riservatezza e sicurezza dei dati, grazie all'adozione di specifiche misure tecniche e organizzative;
– trasparenza del trattamento, fornendo adeguate informazioni;
– trasferimento dei dati presso terze parti previa appropriata protezione degli stessi;
– «accountability».

Al di là dell'esistenza di queste policy internazionali, la protezione effettiva dei dati personali rimane un compito dei singoli ordinamenti giuridici, caratterizzati dalle loro specifiche tradizioni [Custers et al. 2017].

Nei precedenti capitoli sono stati introdotti i quadri normativi europeo e statunitense. Pur consapevoli della semplificazione, è possibile affermare che queste giurisdizioni hanno seguito traiettorie differenti.

Negli Stati Uniti le garanzie per la protezione dei dati a livello legislativo sono più limitate e manca una normativa onnicomprensiva che regoli il settore privato [Bignami, Resta 2015, 236-238]. La legislazione statunitense, infatti, è frammentata e settoriale, spesso frutto di situazioni «emergenziali» e, alla luce delle caratteristiche di questo sistema giuridico, è suddivisa tra il livello federale e statale. La maggior parte delle regole si rivolge all'ambito pubblico per la tutela del privato nei suoi confronti (rapporto pubblico-privato, tra Stato/autorità e cittadino). Un ruolo fondamentale per la protezione della privacy è stato svolto dalla giurisprudenza e dall'affermarsi della tutela rimediale dei *privacy tort*. A livello costituzionale, nell'ordinamento statunitense non esiste un diritto

2 Si v. il testo completo dei principi in https://unsceb.org/principles-personal-data-protection-and-privacy-listing.

a protezione dell'*informational privacy* analogo a quello fondamentale alla protezione dei dati dell'UE [Schwartz, Peifer 2017, 132]. Non manca, comunque, *case law* che interpreta gli emendamenti del Bill of Rights per garantire la protezione delle informazioni personali.

Negli Stati Uniti non c'è un'autorità paragonabile ai garanti europei e degli Stati membri; ciò nonostante, la Federal Trade Commission svolge alcune attività in materia di privacy. In ogni caso, il punto di partenza delle regole è la libera circolazione delle informazioni, a meno che si applichi uno specifico limite. Tale approccio prende il punto di vista del mercato e della protezione del consumatore, ed è opposto a quello europeo, che si sviluppa dalla tutela dell'individuo e delle sue libertà e diritti fondamentali. Le differenze di protezione hanno un forte impatto sul regime di trasferimento transfrontaliero dei dati personali [vedi → Capitolo 6].

Queste stesse differenze sono anche l'esito della diversità di approccio tra le tradizioni giuridiche di civil law, più legate al dato positivo, e quelle di common law, in cui la giurisprudenza ha storicamente svolto un ruolo primario nella creazione del diritto. Tuttavia, le tradizionali diversità tra sistemi giuridici sono sempre più sfumate dalla circolazione dei modelli in un mondo globalizzato.

Nelle prossime sezioni verranno presentate le regole in materia di protezione di dati personali previste in due paesi di civil law, che fanno parte dell'UE, e quali Stati membri applicano il GDPR, e in altri due di common law. Senza pretesa di esaustività, saranno forniti i riferimenti alla normativa attualmente in vigore, segnalando gli aspetti peculiari di ciascun ordinamento.

5.2 Il diritto alla protezione dei dati in Italia

Il diritto alla protezione dei dati personali nell'ordinamento italiano è considerabile uno degli aspetti del generale diritto della personalità garantito dall'art. 2 della Cost., parimenti al diritto alla riservatezza [vedi → Capitolo 2]. A differenza di quest'ultimo, che è stato primariamente elaborato dalla giurisprudenza, esso è stato introdotto a livello legislativo a partire dalla l. 675/1996 «tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali», che ha trasposto la prima direttiva europea in materia, la Direttiva madre 95/46/CE.

In seguito, la legge n. 675 è stata abrogata dal d.lgs. 196/2003 (Codice Privacy), che ha creato un corpo organico di disposizioni, inserendo anche le regole relative ai trattamenti dei dati nel settore delle comunicazioni elettroniche per adempiere alla Direttiva 2002/58/CE [vedi → Capitolo 7]. L'art. 2 del Codice del 2003 specificava che la tutela veniva prevista con riferimento alla riservatezza, all'identità personale degli individui e al diritto alla protezione dei dati personali; in altre parole, il diritto alla riservatezza e alla protezione dei dati personali convivevano esplicitamente nel sistema di regole codicistico. Il Codice Privacy è attualmente in vigore con le modifiche apportate dal d.lgs. 10 agosto 2018, n. 101 per l'adeguamento della normativa nazionale alle disposizioni del GDPR.

A partire dalla data di applicazione del GDPR, la normativa sulla protezione dei dati personali in Italia è di fonte prevalentemente europea e solo limitatamente nazionale [Finocchiaro, 2019]. Infatti, la legge di delegazione europea n. 163 del 2017, che ha stabilito i criteri per l'adeguamento, precisava che il Governo avrebbe dovuto abrogare espressamente le disposizioni incompatibili con quelle contenute nel GDPR, modificare le previsioni limitatamente a quanto necessario per dare attuazione alle disposizioni non direttamente applicabili, coordinare le varie regole e adeguare il sistema sanzionatorio penale ed amministrativo (art. 13). La commissione incaricata per l'elaborazione dello schema di decreto ha utilizzato la tecnica normativa della novellazione, innovando profondamente il Codice per renderlo compatibile con il GDPR, senza richiederne la totale abrogazione. Ciò però ha avuto un impatto sull'organicità e leggibilità del suo testo [Finocchiaro 2019].

Non è possibile in questa sede analizzare tutte le norme ancora presenti nel Codice Privacy. È invece opportuno segnalare alcune disposizioni particolari che non trovano una corrispondenza nel diritto europeo.

Per quanto riguarda il consenso di un minore in relazione ai servizi della società dell'informazione, disciplinato dall'art. 8, par. 1, del GDPR, il Codice Privacy fissa a quattordici anni l'età per prestare lecitamente la propria volontà al trattamento (art. 2-*quinquies*). Si tratta, perciò, di una disposizione meno restrittiva rispetto a quella europea che prevede l'età di sedici anni, ma comunque consentita per la possibilità di deroga introdotta dallo stesso GDPR, purché non sia inferiore a tredici anni di età.

Il GDPR non si applica ai dati personali dei defunti (Cons. 27); tuttavia, il regolamento lascia agli Stati Membri la possibilità di prevedere regole

specifiche a protezione dei dati delle persone decedute. Il Codice Privacy del 2003 già prevedeva una disposizione sui dati personali delle persone defunte (art. 9, co. 3). A seguito dell'adeguamento al Regolamento il legislatore ha abrogato la precedente previsione e inserito una norma specifica all'art. 2-*terdecies*, rubricato «diritti riguardanti le persone decedute», il quale recita:

> 1. I diritti di cui agli articoli da 15 a 22 del Regolamento riferiti ai dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato, in qualità di suo mandatario, o per ragioni familiari meritevoli di protezione.
> 2. L'esercizio dei diritti di cui al comma 1 non è ammesso nei casi previsti dalla legge o quando, limitatamente all'offerta diretta di servizi della società dell'informazione, l'interessato lo ha espressamente vietato con dichiarazione scritta presentata al titolare del trattamento o a quest'ultimo comunicata.
> 3. La volontà dell'interessato di vietare l'esercizio dei diritti di cui al comma 1 deve risultare in modo non equivoco e deve essere specifica, libera e informata; il divieto può riguardare l'esercizio soltanto di alcuni dei diritti di cui al predetto comma.
> 4. L'interessato ha in ogni momento il diritto di revocare o modificare il divieto di cui ai commi 2 e 3.
> 5. In ogni caso, il divieto non può produrre effetti pregiudizievoli per l'esercizio da parte dei terzi dei diritti patrimoniali che derivano dalla morte dell'interessato nonché del diritto di difendere in giudizio i propri interessi.

Questa norma riconosce la possibilità di esercitare i diritti dell'interessato sui dati personali di una persona deceduta, ossia i diritti di accesso, rettifica e cancellazione dei dati personali, di limitazione al trattamento, di portabilità dei dati, di opposizione al trattamento e il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato (artt. 15-22 GDPR), per chi ha un interesse proprio o agisce a tutela dell'interessato, quale mandatario, o chi ha ragioni familiari meritevoli di protezione, salvi i casi in cui l'esercizio di uno o più diritti sia escluso dalla legge [Resta 2021].

L'interessato, durante la sua vita, può vietare l'esercizio di questi diritti con dichiarazione scritta da presentare al titolare del trattamento, ma il

divieto non può pregiudicare diritti patrimoniali di terzi che derivano dalla sua morte e i diritti dei terzi a difendere in giudizio i loro interessi. Se non vi è un divieto, perciò, i congiunti o gli eredi di una persona defunta potrebbero rivolgersi al titolare del trattamento sulla base di uno o più diritti e chiedere, ad esempio, l'accesso o la cancellazione dei dati personali, o opporsi al trattamento ancora pendente.

La disciplina dell'art. 2-*terdecies* consente una tutela e un esercizio *post mortem* del diritto alla protezione dei dati personali e non si limita ai familiari, ma introduce la figura del mandatario, che può essere incaricato dall'interessato mandante, quando è ancora in vita, a gestire i suoi interessi dopo la morte, come poter chiedere l'accesso a credenziali di un servizio digitale o poter cancellare un account di social network, affinché non sia più operativo. La possibilità di veto dell'interessato è un'espressione dell'autodeterminazione informativa dell'individuo [Resta 2019, 102]. Peraltro, le questioni relative alla successione nei rapporti digitali («digital inheritance») e alla tutela dei dati personali dei defunti sono tra gli argomenti più studiati e dibattuti degli ultimi anni [Resta 2019]. Anche la Francia, come si vedrà, ha da tempo introdotto una disciplina relativa ai dati dei defunti.

Inoltre, gli articoli 51 e 52 del Codice Privacy prevedono delle regole in merito al trattamento dei dati identificativi presenti in documenti processuali, quali sentenze, ordinanze, atti giudiziari e loro allegati, nel momento in cui vengono utilizzati per scopi di informazione giuridica. Il processo è di regola pubblico. Tuttavia, la possibile diffusione su Internet di documenti giudiziari in banche dati informative richiede delle limitazioni per salvaguardare i diritti degli interessati. Secondo i principi generali previsti dalla prima norma, e fatta salva la disciplina processuale relativa alla visione e al rilascio di estratti e di copie di atti e documenti, i dati personali identificativi delle questioni pendenti presso l'autorità giudiziaria sono resi accessibili a chi vi abbia interesse, anche mediante reti di comunicazione elettronica, come i siti internet della medesima autorità (art. 51, co. 1). Dovrà, quindi, essere allegato un interesse alla richiesta di accesso. Le sentenze e le altre decisioni già depositate nelle cancellerie sono rese accessibili anche attraverso il sistema informativo e il sito istituzionale dell'autorità giudiziaria, osservando i limiti previsti dall'art. 52 (art. 51, co. 2).

Questa norma disciplina i limiti per la diffusione del contenuto dei provvedimenti giurisdizionali per qualsiasi finalità, facendo salva la disciplina riguardante la redazione e il contenuto di sentenze e di altri provvedimenti giurisdizionali (compresi i lodi arbitrali, per il richiamo contenuto nel co. 6).

Se sono presenti motivi legittimi, l'interessato può chiedere, attraverso una richiesta depositata nella cancelleria o segreteria dell'ufficio del processo pendente e prima che sia definito il relativo grado di giudizio, che (art. 52, co. 1)

> sia apposta a cura della medesima cancelleria o segreteria, sull'originale della sentenza o del provvedimento, un'annotazione volta a precludere, in caso di riproduzione della sentenza o provvedimento in qualsiasi forma, l'indicazione delle generalità e di altri dati identificativi del medesimo interessato riportati sulla sentenza o provvedimento.

Si tratta, in concreto, di una richiesta di anonimizzazione della sua identità nella sentenza. La regola generale sarebbe, infatti, quella della pubblicità integrale di ogni provvedimento giurisdizionale (art. 52, co. 7). Se la richiesta è legittima, l'autorità provvede, senza ulteriori formalità, in calce alla sentenza tramite un decreto (art. 52, co. 2) e la cancelleria al deposito indicherà le generalità e gli identificativi da omettere in caso di diffusione con un timbro (art. 52, co. 3).

L'autorità giurisdizionale può anche disporre d'ufficio tale annotazione, a tutela dei diritti o della dignità degli interessati (art. 52, co. 2). Questo potere officioso di oscuramento terrà conto delle particolarità del caso giudiziario, che potrebbe riguardare il trattamento di dati sensibili.

I terzi che intendono diffondere una sentenza con annotazione dovranno omettere le generalità e i dati identificativi (art. 52, co. 4). È il caso delle banche dati giuridiche, come Foro Italiano (foro.it) o DeJure. In presenza di vittime minori di reato a sfondo sessuale, o di procedimenti relativi a rapporti di famiglia e stato delle persone, la diffusione del provvedimento deve omettere le generalità e altri dati identificativi. Tra gli interessati legittimati a tali richieste vi sono certamente le parti processuali e i testimoni [Resta 2014].

In caso di mancata anonimizzazione, l'interessato potrà rivolgersi all'amministrazione che gestisce il sito di divulgazione e presentare ricorso per la tutela risarcitoria, costituendo un'illecita diffusione di dati che dovevano essere oscurati per annotazione di un giudice.

Questa tutela protegge l'identità di persone coinvolte, per le più svariate ragioni, in un processo giudiziario. Si tratta di un'espressione non solo del diritto alla protezione dei dati, ma anche del rispetto alla vita privata. L'autorità opererà un bilanciamento tra la richiesta individuale e l'esigenza di pubblicità del contesto processuale.

Il Codice prevede poi regole specifiche per i trattamenti con finalità di ricerca scientifica (artt. 97- 110-*bis*) [vedi → Capitolo 16], nell'ambito del rapporto di lavoro (artt. 111-115) [vedi → Capitolo 9], per le comunicazioni elettroniche (artt. 121-132-*quater*) [vedi → Capitolo 7] e sui poteri e compiti del Garante per la protezione dei dati personali (artt. 153-160-*bis*).

Oltre alle regole ancora disciplinate nel Codice Privacy, il quadro normativo italiano in materia è completato dai provvedimenti e dalle pronunce del Garante, dai codici deontologici e di settore e dal d.lgs. 51/2018, che ha trasposto la Direttiva 2016/680, disciplinante i trattamenti svolti dall'autorità pubblica per le finalità di prevenzione, accertamento, repressione dei reati o tutela dell'ordine e della sicurezza pubblici [per questo settore, vedi → Capitolo 7].

Con riferimento ai codici deontologici e ai provvedimenti chiave dell'autorità garante si segnalano:

– le Regole deontologiche relative al trattamento dei dati personali nell'esercizio dell'attività giornalistica (Allegato 1 del Codice Privacy);
– le Regole deontologiche relative ai trattamenti di dati personali effettuati per svolgere investigazioni difensive o per fare valere o difendere un diritto in sede giudiziaria (Allegato 2 del Codice Privacy);
– le Regole deontologiche per il trattamento a fini di archiviazione nel pubblico interesse o per scopi di ricerca storica (Allegato 3 del Codice Privacy);
– le Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica effettuati nell'ambito del Sistema statistico nazionale (Allegato 4 del Codice Privacy);
– le Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica (Allegato 5 del Codice Privacy) [vedi → Capitolo 16];

– le Prescrizioni relative al trattamento di categorie particolari di dati nei rapporti di lavoro (aut. gen. n. 1/2016) [vedi → Capitolo 9];
– le Prescrizioni relative al trattamento di categorie particolari di dati da parte degli organismi di tipo associativo, delle fondazioni, delle chiese e associazioni o comunità religiose (aut. gen. n. 3/2016);
– le Prescrizioni relative al trattamento di categorie particolari di dati da parte degli investigatori privati (aut. gen. n. 6/2016);
– le Prescrizioni relative al trattamento dei dati genetici (aut. gen. n. 8/2016);
– le Prescrizioni relative al trattamento dei dati personali effettuato per scopi di ricerca scientifica (aut. gen. n. 9/2016) [vedi → Capitolo 16].

Le regole deontologiche sono dedicate a specifiche tipologie o contesti di trattamento e sono formalmente parte del Codice Privacy come suoi allegati. Le prescrizioni, invece, raccolgono disposizioni che prima del GDPR erano considerate autorizzazioni generali dell'autorità a determinate circostanze di trattamento e che a seguito del d.lgs. 101/2018 sono state integrate e modificate per adeguarle all'attuale quadro normativo. Gli operatori del diritto devono tenere conto di entrambe le tipologie di fonti per progettare e attuare attività di trattamento in modo compatibile con l'ordinamento giuridico italiano.

5.3 Il diritto alla protezione dei dati in Francia

L'ordinamento francese è stato uno dei primi a tutelare espressamente il diritto alla privacy nella sua legislazione nazionale [Custers et al. 2019]. Il diritto alla riservatezza (*vie privée*) trova riscontro nell'art. 9 del Code Civil, come modificato nel 1970, che stabilisce che:

> Chacun a droit au respect de sa vie privée.
>
> Les juges peuvent, sans préjudice de la réparation du dommage subi, prescrire toutes mesures, telles que séquestre, saisie et autres, propres à empêcher ou faire cesser une atteinte à l'intimité de la vie privée : ces mesures peuvent, s'il y a urgence, être ordonnées en référé.

Al diritto alla protezione dei dati personali è dedicata la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, una delle prime legislazioni in materia in tutto il mondo. In questa normativa è stata trasposta la Direttiva madre 95/46/CE.

La Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles e il Décret n° 2019-536 du 29 mai 2019 hanno, invece, recepito il GDPR modificando in gran parte la legge del 1978 [Tambou 2018]. Con riferimento ad alcune disposizioni particolari della normativa francese si può segnalare quanto segue.

L'art. 3 della Loi n° 78-17 disciplina l'ambito di applicazione territoriale. Dopo aver fatto salve le regole dell'art. 3 del GDPR [vedi → Capitolo 3], questa norma amplia l'applicazione delle regole interne a tutti i trattamenti di dati personali effettuati nell'ambito delle attività di uno stabilimento di un titolare o di un responsabile del trattamento sul territorio francese, indipendentemente dal fatto che il trattamento abbia luogo o meno in Francia. In aggiunta, le regole nazionali che prevedono regole ulteriori sulla base delle indicazioni del GDPR (es., art. 9, par. 4) si applicano a partire dal momento in cui l'interessato risiede in Francia, anche quando il titolare del trattamento non è stabilito in Francia. Ciò, tuttavia, non vale per i trattamenti di cui all'articolo 85, paragrafo 2, del Regolamento («libertà d'espressione e di informazione», inclusi i trattamenti a scopi giornalistici o di espressione accademica, artistica o letteraria) per i quali si considera lo stabilimento nell'UE.

Con riferimento all'età per prestare validamente il consenso in relazione ai servizi della società dell'informazione, la legge francese richiede quindici anni (art. 45). Come nel caso dell'Italia, si tratta di una disposizione meno restrittiva rispetto a quella dell'art. 8, par. 1, del GDPR, ma ugualmente legittima per la possibilità di deroga a livello nazionale.

La Loi n° 78-17 prevede, inoltre, regole specifiche e dettagliate per i trattamenti nel contesto sanitario (artt. 64-77), per quelli con finalità di archiviazione nell'interesse pubblico, ricerca scientifica, storica o statistica (artt. 78-79) e per l'ambito delle comunicazioni elettroniche (artt. 81-83, vedi → Capitolo 7).

Come anticipato nella precedente sezione, il GDPR non si applica ai dati personali dei defunti, ma inserisce la possibilità di stabilire regole specifiche a protezione dei dati delle persone decedute a livello nazio-

nale. L'articolo 85 della Loi n° 78-17 estingue i diritti dell'interessato con la sua morte, ma consente al medesimo soggetto di stabilire «direttive» generali o speciali riferite al trattamento dei dati personali dopo la sua morte [Resta 2019, 97-98]. Peraltro, la possibilità di dare direttive sui dati personali deve essere inserita nell'informativa rilasciata ai sensi degli artt. 13 e 14 del GDPR (art. 48).

Le direttive possono riguardare la conservazione, la comunicazione o la cancellazione dei dati personali. Per la validità delle direttive generali, l'interessato dovrà riferirsi all'insieme di tutti i dati personali e depositarle presso un ente certificato presso la CNIL, autorità di controllo francese, che provvederà a pubblicarle in un apposito registro.

Le direttive speciali, invece, si possono riferire a trattamenti particolari e potranno essere depositate presso il titolare coinvolto, previa espressione del consenso. Le condizioni generali di un contratto di un servizio, infatti, non potranno definire direttive per la gestione post-mortale dei dati senza il consenso specifico dell'interessato; in caso contrario, si avranno come non apposte.

Entrambe le tipologie di direttive sono revocabili in ogni momento. Nelle direttive generali l'interessato può indicare un soggetto di fiducia che risulterà responsabile della loro esecuzione. Questa persona avrà quindi il diritto, quando l'interessato sarà deceduto, di prendere conoscenza delle direttive e di richiederne l'attuazione a tutti i titolari del trattamento dei dati personali del *de cuius*. In mancanza di una tale designazione, gli eredi avranno il diritto di prendere conoscenza delle direttive alla morte dell'interessato e di richiederne l'esecuzione ai titolari del trattamento.

In assenza di direttive generali o speciali, gli eredi dell'interessato potranno esercitare i diritti previsti dagli artt. 15-22 GDPR, se intendono dare corso alla successione e i dati sono necessari alla liquidazione e ripartizione dell'eredità. Possono anche ricevere comunicazioni di beni digitali o dati simili a ricordi di famiglia (*digital inheritance*). Gli eredi potranno anche regolare gli effetti dell'evento morte sul rapporto negoziale di account del *de cuius* (ad es., con un social network), opponendosi al trattamento o facendo aggiornare i dati (ad. es., dichiarando la morte sul profilo, che rimarrà come una «pagina commemorativa»). In ogni caso, il prestatore di un servizio di comunicazione pubblica online deve informare l'utente, quale interessato, sulla possibile sorte dei dati personali alla

sua morte, e deve consentire di scegliere se comunicare o meno i suoi dati a un terzo da lui designato.

Questa norma fornisce una tutela completa per la gestione post-mortale dei dati personali. Non solo prevede la possibilità di determinare a chi potranno essere resi accessibili i dati, ma anche di richiederne l'immediata cancellazione. Viene attribuita particolare importanza al concetto di trasparenza, dovendo comunicare all'interessato, fin dall'inizio del trattamento, che ha una scelta sulla futura gestione dei suoi dati personali.

Come sottolineato da Resta, la normativa francese diverge da quella italiana perché la prima considera i diritti estinti, mentre la seconda li preserva [Resta 2019, 103]. La legge francese prevede un contenuto prevalentemente positivo, mentre quella italiana negativo. In entrambi i casi, tuttavia, la volontà dell'interessato deve essere determinata e chiara e non può essere desunta dalla sottoscrizione di clausole generali. L'art. 85 della Loi n° 78-17 offre, comunque, una tutela più ampia rispetto a quella dell'art. 2-*terdecies* del Codice Privacy.

A differenza della scelta compiuta in Italia, il legislatore francese ha inserito direttamente nella Loi n° 78-17 le norme di attuazione alla Direttiva 2016/680. I trattamenti svolti dall'autorità pubblica per le finalità di prevenzione, accertamento, repressione dei reati o tutela dell'ordine e della sicurezza pubblici sono infatti regolati dagli articoli 87-114.

Oltre alla Loi n° 78-17, si possono segnalare alcune normative speciali dedicate a particolari tipologie di trattamento o ad alcuni settori:

– la Loi n° 2004-575 du 21 juin 2004 «pour la confiance dans l'économie numérique» e la Loi n° 2004-669 du 9 juillet 2004 «relative aux communications électroniques et aux services de communication audiovisuelle», che hanno adottato la Direttiva europea 2002/58/CE sul trattamento dei dati personali nel contesto delle comunicazioni elettroniche [vedi → Capitolo 7];
– il «Code des postes et des communications électroniques» (Loi n° 2020-1508 du 3 déc. 2020), anch'esso contenente regole per la «protection de la vie privée des utilisateurs de réseaux et services de communications électroniques»;
– il «Code de la santé publique», che stabilisce altre regole per l'utilizzo dei dati personali relativi alla salute, quali la norma sull'accesso (art. L1435-6) e le disposizioni sull'utilizzo (artt. L1460-1–L1462-2).

L'autorità di controllo francese, la Commission nationale de l'informatique et des libertés o CNIL, svolge un ruolo prominente non solo nell'ordinamento francese, ma anche a livello europeo, pubblicando[3]:

– *lignes directrices*, ossia documenti che forniscono elementi di interpretazione dei testi legislativi nazionali ed europei, informando sulle procedure da seguire e sulle corrette regole da applicare. Tra queste si possono segnalare le «Lignes directrices "cookies et autres traceurs", che forniscono indicazioni sull'utilizzo di strumenti di tracciamento durante la navigazione online [vedi → Capitolo 7], e le «Lignes directrices sur les analyses d'impact relatives à la protection des données (AIPD) prévues par le Règlement Général sur la Protection des Données (RGPD)», riguardanti la valutazione di impatto dell'art. 35 del GDPR, a cui si può affiancare lo strumento tecnologico sviluppato dalla stessa autorità per consentire ai titolari del trattamento di elaborarla in modo chiaro ed efficace [vedi → Capitolo 3];
– *recommandations*, che non si considerano prescrittive, ma servono come guida pratica per implementare specifiche regole giuridiche, come nel caso delle «Recommandation - traitement et utilisation de données personnelles par la presse écrite ou audiovisuelle à des fins journalistiques ou rédactionnelles» per l'ambito giornalistico, o le «Recommandation - réutilisation de données personnelles d'archives publiques» sull'uso secondario di dati personali conservati in archivi pubblici. Le liste elettorali francesi sono pubbliche e il sistema di votazione prevede la possibilità di votare in modalità elettronica presso le sedi elettorali e a distanza. Vista la particolarità del sistema elettorale, la CNIL ha elaborato le «Recommandation - sécurité des systèmes de vote électronique» e le «Recommandation - systèmes de vote par correspondance électronique notamment via internet»;
– *référentiels et méthodologies de référence*, che possono essere considerate come regole di riferimento per consentire a un titolare del trattamento di conformarsi a una specifica operazione di trattamento dei dati, quali «pacchetti di conformità». Pur non essendo formalmen-

3 I documenti sono disponibili sul sito ufficiale dell'autorità in https://www.cnil.fr/fr/decisions/lignes-directrices-recommandations-CNIL.(per linee guida e raccomandazioni), https://www.cnil.fr/fr/autres-referentiels.(per référentiels) e https://www.cnil.fr/fr/les-referentiels-et-methodologies-de-reference-sante.(per il settore sanitario).

te vincolanti, indicano metodologie e pratiche che rendono le attività compatibili con la normativa vigente. Di particolare interesse sono il «Référentiel – protection de l'enfance», per i trattamenti di dati di minori, e il «Référentiel relatif aux traitements de données personnelles mis en oeuvre dans le cadre de la gestion locative», che si riferisce alla gestione dei dati raccolti per sottoscrivere contratti di locazione;
– *référentiels et méthodologies de référence santé*, ossia le regole di conformità per il settore sanitario, che in Francia richiede in molti casi di presentare una richiesta di autorizzazione alle operazioni di trattamento, dunque in via preventiva all'autorità di controllo. Se il titolare si conforma a tali metodologie, la richiesta risulta semplificata, anche in caso di finalità di ricerca scientifica con dati relativi alla salute [Bincoletto, Guarda 2021, 59-63].

Come per l'Italia, a seguito del GDPR la normativa francese sulla protezione dei dati personali è considerabile di fonte prevalentemente europea e solo limitatamente nazionale.

5.4 Il diritto alla protezione dei dati in Canada[4]

Il Canada è un sistema giuridico composto da dieci province e tre territori, uniti da un livello federale e caratterizzati da tre tradizioni giuridiche: civil law, common law e «aboriginal law»[5]. In breve, la prima tradizione è tipica della Provincia del Québec, unica che dispone di un Civil Code, e che ha subito la dominazione francese, diventando un sistema misto. Espressione di questa tradizione è anche il Criminal Code, applicato in tutto lo stato. La seconda è, invece, il frutto delle conquiste inglesi e può considerarsi la più diffusa, mentre la terza si riferisce a quanto tramandato da First Nations, Métis, Inuit e da altri gruppi indigeni, e da quanto stabilito nei trattati che ne regolano i diritti.

L'ordinamento canadese non prevede una norma che tutela esplicitamente il diritto a protezione dei dati a livello costituzionale, ma la privacy

4 Si ringrazia la Prof.ssa Federica Giovanella per la collaborazione e il confronto sul sistema giuridico canadese.

5 Per una breve descrizione si v. https://www.justice.gc.ca/eng/csj-sjc/just/03.html.

è, più in generale, garantita attraverso le Sezioni 7 e 8 del «Canadian Charter of Rights and Freedoms» del 1982 [Giovanella 2017, 144-147]. Queste norme sono considerate di rango costituzionale e si applicano con riferimento ai rapporti tra individuo e governo o istituzioni, prevedendo che:

> Everyone has the right to life, liberty and security of the person and the right not to be deprived thereof except in accordance with the principles of fundamental justice (Section 7, Life, liberty and security of person).
> Everyone has the right to be secure against unreasonable search or seizure (Section 8, Search or seizure).

Con il famoso caso *Hunter v. Southam* del 1984 la Corte Suprema Canadese ha infatti stabilito che:

> the Canadian Charter of Rights and Freedoms is a purposive document, the provisions of which must be subjected to a purposive analysis. Section 8 of the Charter guarantees a broad and general right to be secure from unreasonable searches and seizures which extends at least so far as to protect the right of privacy from unjustified state intrusion. Its purpose requires that unjustified searches be prevented.

Questa protezione è, come anticipato, limitata al rapporto pubblico-privato, non applicandosi per una violazione compiuta da un soggetto privato.

Le corti di common law hanno individuato tre distinte «zones of privacy» [si v. ad es., *Ruby v. Canada* [2000] 3 F.C. 589 (F.C.A.); Giovanella 2017, 145]:

– *territorial privacy*, a protezione della casa e del domicilio dall'invasione fisica altrui, ma anche di luoghi in cui il singolo ha un'aspettativa di riservatezza (si v. *R v. Jarvis*, 2019 S.C.C. 10, sugli studenti in classe);
– *personal or corporeal privacy*, che protegge il corpo e la sfera psichica dell'individuo da intrusioni materiali e immateriali, così come caratteristiche personali quali l'immagine, la fotografia, la voce e il nome;
– *informational privacy*, connessa al concetto di «personal information», ossia all'informazione che identifica una persona fisica.

Le prime due *zone* sono paragonabili al diritto alla riservatezza, mentre la terza dimensione al diritto alla protezione dei dati personali.

Con riferimento alla tutela dell'*informational privacy* da parte della giurisprudenza si può affermare che gli individui possono invocare la violazione sia della Section 7 che 8.

Nel caso *R. v. O'Connor* del 1995 un soggetto accusato di violenza sessuale lamentava che la raccolta di informazioni mediche e scolastiche sul suo conto fosse stata effettuata in violazione del suo diritto alla libertà (sez. 7, *R. v. O'Connor*, 1995 CanLII 51 (SCC), [1995] 4 SCR 411). Nella sua decisione la Corte Suprema ha indicato i criteri per bilanciare le aspettative del singolo con le esigenze del pubblico alla conoscenza dell'informazione, raccolta presso terzi. In particolare, è necessario definire e valutare:

– se le informazioni siano necessarie per l'accusato per consentire una difesa completa;
– il valore probatorio di tali informazioni;
– la natura e l'ampiezza della «reasonable expectation of privacy» del soggetto sulle stesse informazioni;
– se la produzione delle informazioni sia influenzata da pregiudizi discriminatori;
– il potenziale danno alla dignità, privacy o sicurezza della persona.

Questi elementi vanno bilanciati con l'interesse pubblico, che può prevalere quando prominente, come è avvenuto per O'Connor.

Il concetto di «ragionevole aspettativa della privacy» era già stato utilizzato nel caso *R. v. Plant* del 1993, che riguardava la raccolta di informazioni sul consumo di energia elettrica di un sospettato coltivatore di marijuana (*R. v. Plant*, 1993 CanLII 70 (SCC), [1993] 3 S.C.R. 281). Questi aveva lamentato la violazione della Section 8 perché la polizia era entrata nel suo appartamento dopo aver usato uno strumento per misurare l'energia consumata al suo interno. Era stato emesso un mandato, ma sulla base indiziaria di questa raccolta di informazioni. La Corte Suprema, negando la ragionevolezza nell'aspettativa di privacy sulle informazioni di specie, argomentava che i fattori per valutarne la sussistenza sarebbero:

– la tipologia di informazione;

– la natura della relazione fra la parte che rivela l'informazione e quella che la considera confidenziale;
– il luogo dove l'informazione è stata ottenuta e il modo per ottenerla;
– in presenza di un reato, la serietà del crimine sotto indagine.

Nella stessa decisione la Corte ha definito il concetto di «biographical core of personal information», quale nucleo informazionale che deve sempre rimanere segreto perché rivela dettagli intimi dell'individuo. La tutela di questo *core* deve essere garantita in una società democratica. L'interesse del singolo alla protezione delle sue informazioni veniva così definito: «a biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state».

Il caso *R. v. Tessling* del 2004 chiarisce che non tutte le informazioni rientrano nel *core*: i valori riferiti ad un edificio, nella specie il calore, non si possono considerare segreti (*R. v. Tessling* [2004] 3 S.C.R. 432 (S.C.C.)). Nel caso *R. v. Cole* del 2012 la medesima Corte argomentava che «the more personal and confidential the information, the more willing reasonable and informed Canadians will be to recognize the existence of a constitutionally protected privacy interest», sulla base della Section 8 del Charter (*R. v. Cole*, 2012 SCC 53 (CanLII), [2012] 3 SCR 34). Il *core*, perciò, sarà più facilmente riconosciuto se le informazioni riguardano aspetti particolarmente personali.

Nel 2014, la Corte Suprema ha inserito nel concetto di *informational privacy* non solo la protezione della segretezza e confidenzialità delle informazioni, ma anche del loro controllo, accesso e utilizzo e, in un contesto online, dell'anonimato (*R. v. Spencer*, 2014 SCC 43 (CanLII), [2014] 2 SCR 212). Il caso riguardava l'ottenimento di un indirizzo IP da parte della polizia per un sospetto accesso a file pedopornografici, senza un mandato. Ebbene, Mr. Spencer poteva avere una ragionevole aspettativa di privacy perché l'anonimato online, e così delle informazioni a disposizione dell'Internet Service Provider durante la navigazione, è una componente della protezione fornita dalla Section 8. In altre parole, «informational privacy includes at least three conceptually distinct although overlapping understandings of privacy: as secrecy, as control, and as anonymity».

In ogni caso, affinché sia riconosciuta la «reasonaable expectation of privacy» devono concorrere due elementi:
– la persona che rivendica un diritto alla privacy deve avere un'aspettativa soggettiva che sia oggettivamente ragionevole in base alle circostanze e
– l'aspettativa si basa su interessi legalmente riconosciuti dall'ordinamento in materia di privacy (*R. v. J.J.*, 2022 SCC 28 (CanLII)).

Dall'accesso ingiustificato ad un dispositivo elettronico, ad esempio, si presume che si avrà la raccolta di informazioni riservate, tutelate dalle Section 7 e 8 (si v. *R. v. Reeves*, 2018 SCC 56 (CanLII), [2018] 3 SCR 531, in cui l'accesso al computer del marito sospettato, con il solo consenso della moglie e senza mandato, veniva considerato illegittimo).

Il diritto all'*informational privacy* è protetto da legislazioni sia federali che provinciali, in molti casi dedicate a specifici settori[6].

A livello federale sono due le legislazioni principali. Il «Privacy Act» del 1985 concerne i trattamenti compiuti dal governo federale e da specifiche istituzioni pubbliche indicate nella «Schedule of Institutions». Il «Personal Information Protection and Electronic Documents Act» (PIPEDA) del 2001, applicativo dal 2004, si riferisce al settore privato e ai titolari che trattano «personal information» «in the course of for-profit, commercial activities across Canada», e anche alla tutela di «personal information of employees of federally-regulated businesses» (come banche, linee aeree e compagnie di telecomunicazione). Sono espressamente esclusi gli usi di natura personale (*domestic purposes*), con finalità giornalistica, artistica e letteraria, quelli a cui si applica il Privacy Act, e alcuni trattamenti legati al settore della giustizia e a quello amministrativo (art. 3).

A livello provinciale alcune normative dedicate al settore privato si devono applicare al posto del PIPEDA se prevedono norme «substantially similar»: il «Personal Information Protection Act» (PIPA Alberta), il «Personal Information Protection Act» (PIPA British Columbia) e l'«An Act Respecting the Protection of Personal Information in the Private Sector»

6 Si v. il summary dell'Office of Privacy Commissioner del Canada in https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/.

(Quebec Privacy Act, che si ispira al GDPR). Le Province di Ontario, New Brunswick, Nova Scotia and Newfoundland e Labrador hanno, invece, adottato legislazioni riferite al trattamento nel contesto sanitario.

La PIPEDA è basata sui Fair Information Practices dell'OECD e incorpora i principi del «Model Code for the Protection of Personal Information» sviluppato dalla «Canadian Standards Association» del 1996 [Solove, Schwartz 2021, 1295; Charnetski et al. 2001]. Si tratta di un testo organico che si applica in tutto lo stato, salvo eventuale normativa provinciale che deroghi alla sua applicazione, come anticipato.

Nella legislazione canadese la nozione di informazione personale è più restrittiva rispetto a quella di dato personale del GDPR perché l'informazione protetta è quella riferita ad un soggetto individuato e non anche quella che «potrebbe identificarlo», a meno che non ci sia una seria possibilità che tramite altre informazioni il titolare possa apprendere l'identità del soggetto (art. 2(1) PIPEDA, dove «personal information means information about an identifiable individual»).

Un'altra chiara differenza con l'ordinamento europeo è la mancata distinzione tra la definizione generale di informazione personale e informazioni particolari o sensibili [Giovanella 2017, 183]. Un'eccezione è l'inserimento del separato concetto di «personal health information» nel PIPEDA (art. 2(1)).

Il PIPEDA non utilizza il concetto di «base giuridica del trattamento», ma richiede il consenso dell'interessato per la raccolta, l'uso e la comunicazione delle informazioni, a meno che non vi sia un'autorizzazione esplicita nello stesso atto o si applichi un'eccezione (artt. 6 e 12). Questo sistema è stato definito un «individual-oriented consent-based mechanism» [Scassa 2020].

Affinché il consenso possa ritenersi valido, l'organizzazione che tratta le informazioni deve informare l'individuo sulle finalità della raccolta (art. 7 e 10). A differenza di quanto previsto dal GDPR, il PIPEDA inserisce alcune condizioni di validità di un consenso implicito (ad es., se le informazioni sono volontariamente fornite dal soggetto o l'individuo deve fornirle per la sottoscrizione di un contratto). Queste eccezioni sono tuttavia in parte simili ad alcune basi giuridiche degli artt. 6 e 9 GDPR. Il consenso è sempre revocabile (art. 9).

Un organizzazione può utilizzare le informazioni «only for purposes that a reasonable person would consider appropriate in the circumstan-

ces» e per quella finalità comunicata all'individuo al momento della raccolta o per quanto consentito dalla legge (art. 14).

L'individuo ha poi diritto all'accesso e alla rettifica delle informazioni in presenza di determinate circostanze (artt. 23 e 24). Tra le regole del PIPEDA è possibile riconoscere l'espressione dei principi di limitazione della finalità, confidenzialità e sicurezza, limitazione alla conservazione e accountability [Solove, Schwartz 2021, 1295].

Le norme del PIPEDA sono state considerate come un quadro di protezione adeguato per il trasferimento di dati tra UE e Canada da parte della Commissione Europea nel 2002 (C(2001) 4539) [sui trasferimenti, vedi → Capitolo 6].

A controllo della protezione di dati in Canada sono state istituite le seguenti autorità:

– Office of the Privacy Commissioner of Canada (OPC), che si occupa del rispetto delle regole federali[7] e i cui compiti e poteri sono definiti nel PIPEDA. Questa autorità non può imporre ordini o comminare sanzioni, perciò le investigazioni proseguono presso le corti federali;
– Office of the Information and Privacy Commissioner of Alberta;
– Office of the Information and Privacy Commissioner for British Columbia;
– Office of the Information and Privacy Commissioner of Ontario;
– Commission d'accès à l'information du Québec ;
– Ombudsman a livello locale, come commissario a cui rivolgersi quando non è stato istituito un Office.

Nel 2019, alla luce delle caratteristiche del quadro normativo vigente per la protezione delle informazioni personali e dei cambiamenti tecnologici degli ultimi anni l'istituzione federale Innovation, Science and Economic Development Canada (ISED) ha pubblicato il documento «Proposals to modernize the Personal Information Protection and Electronic Documents Act»[8].

Questa proposta contiene diverse modifiche al testo del PIPEDA che potrebbero proteggere maggiormente gli individui in un contesto digitale. Tra queste, si suggerisce di inserire dei nuovi requisiti per la traspa-

7 Il sito ufficiale dell'OPC è https://www.priv.gc.ca/en.

8 Il sito ufficiale dell'OPC è https://www.priv.gc.ca/en.

renza del trattamento, modificare il meccanismo basato sul consenso, fornendo alternative più efficaci e più eccezioni, e riconoscere un diritto ad essere informati sull'uso di processi decisionali automatizzati, sui fattori coinvolti nelle decisioni e, qualora esse abbiano un impatto sul singolo, sulla logica su cui si basano. Si propone, in aggiunta, l'inserimento di un diritto alla «data mobility», simile al diritto alla portabilità dei dati personali, di condizioni per l'uso secondario delle informazioni per finalità di ricerca e di aumentare i compiti e i poteri dell'OPC.

Tuttavia, non era chiaro quando una tale riforma potesse essere approvata dal governo federale. Secondo Scassa, nel processo di modernizzazione delle leggi canadesi sulla privacy il GDPR dovrebbe avere un impatto significativo; ciò contribuirebbe ad un cambiamento di prospettiva verso il riconoscimento della protezione dei dati come diritto fondamentale dell'ordinamento giuridico [Scassa 2020].

Successivamente, nel giugno 2022, il Minister of Innovation, Science and Industry ha proposto il «Bill C 27: Digital Charter Implementation Act 2022» allo scopo di introdurre tre nuove e diverse normative[9]:

– Consumer Privacy Protection Act (CPPA), che dovrebbe abrogare gran parte del PIPEDA, applicandosi al settore privato, e modificare altre legislazioni federali. Allo stato attuale non dovrebbe essere modificata la definizione di «personal information», ma dovrebbero essere garantite maggiori protezioni grazie all'introduzione di nuovi obblighi (come l'attuazione di un «privacy management program» e di «security safeguards»), il rafforzamento dei presupposti per il trattamento (ad es., nuove condizioni per la validità del consenso e nuove eccezioni alla sua raccolta), il riconoscimento di nuovi diritti (tra cui il menzionato diritto alla «data mobility»). Tale Act dovrebbe altresì aumentare i compiti e poteri dell'OPC, dal momento che verrebbe riconosciuto un «private right of action» per ottenere il risarcimento di danni patrimoniali e non patrimoniali in presenza di una violazione della normativa;
– Personal Information and Data Protection Tribunal Act (PIDPTA), che dovrebbe istituire una nuova corte con il potere di decidere sui reclami presentati ai sensi del CPPA;

9 A gennaio 2023 la proposta risulta nella fase di second reading presso l'House of Commons.

– Artificial Intelligence and Data Act (AIDA), che dovrebbe aggiornare la normativa sulla gestione dei dati per far fronte alle sfide poste dall'intelligenza artificiale, scopo condiviso dalla «Proposal for a Regulation of the European Parliament and of the Council laying down Harmonized Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending certain Union Legislative Act» della Commissione Europea del 2021 [vedi → Capitolo 13].

5.5 Il diritto alla protezione dei dati nel Regno Unito

Il Regno Unito è un paese di common law. Dal 1° gennaio 2021 ha cessato di essere uno Stato membro dell'UE. In questo ordinamento il diritto alla privacy è protetto sia dal *tort* «misuse of private information» che da alcuni *statute*, tra cui una normativa organica in materia di dati personali, il «Data Protection Act», in cui è stato inserito il cd. «UK General Data Protection Regulation» o «UK GDPR». Con la Brexit, infatti, parte della disciplina europea è stata mantenuta nel diritto inglese [Schwartz 2021].

In primo luogo, il *misuse of private information* si è affermato come *cause of action* autonoma rispetto al tradizionale *tort* «breach of confidence» nel 2004 nel caso *Campbell v. Mirror Group Newspapers Ltd* della House of Lord (*Campbell v. Mirror Group Newspapers Ltd* [2004] UKHL 22).

Nel 2001 il giornale «The Mirror» pubblicava un articolo intitolato «Naomi: I am a drug addict» con due fotografie della modella Naomi Campbell, di cui una ritratta all'uscita da un incontro ai narcotici anonimi. La modella si rivolgeva alla casa editrice del giornale per ritirare l'articolo e in risposta il giornale continuava a pubblicare sulla donna rivelando dettagli intimi della sua vita e creando una sorta di attacco mediatico personale. Ms. Campbell agiva dunque contro la casa editrice sulla base del *tort* «breach of confidence». La House of Lords esordiva statuendo che «in this country, unlike the United States of America, there is no overarching, all-embracing cause of action for ˝invasion of privacy˝». Secondo la Corte il caso di specie riguardava la divulgazione illecita di informazioni private, ma non era rintracciabile una *cause of action* specifica. Per tale tipologia di violazione si utilizzava generalmente il rimedio di «breach of confidence», che richiedeva la presenza di un «duty of confidence»

e così di un'informazione che avrebbe dovuto rimanere confidenziale. Tuttavia, alla luce dell'emersione di nuovi fenomeni di divulgazione di informazioni sulla vita privata di un individuo e dell'art. 8 della Cedu, che tutela la privacy a livello europeo e che è stato trasposto internamente dallo «Human Rights Act» del 1998, l'House of Lords ha definito per la prima volta il *tort* di *misuse of private information*, da invocarsi in caso di uso di informazioni private e pretesa di controllo sull'informazione da bilanciare con la libertà di espressione. La protezione delle informazioni private è un aspetto della *human autonomy* e *dignity*. La Corte così decise a favore di Ms. Campbell.

La Supreme Court of the United Kingdom ha chiarito che l'informazione è protetta contro l'uso illecito solo quando sussiste una «reasonable expectation of privacy» sulla stessa (si v. ad es. *Lloyd v. Google LLC* [2021] UKSC 50; *Bloomberg LP v. ZXC* [2022] UKSC 5). Per valutare la sussistenza di tale aspettativa, il giudice deve considerare:

– come è stata ottenuta l'informazione;
– quale sia il danno provato dalla divulgazione;
– se sussiste un interesse pubblico preminente all'utilizzo dell'informazione.

Per questa valutazione si deve adottare il punto di vista di una persona ragionevole di comune sensibilità, chiarendo come quest'ultima possa sentirsi se si trovasse nella stessa situazione e nelle medesime circostanze del soggetto che lamenta la violazione della sua privacy (*Murray v. Big Pictures (UK) Ltd* [2008] EWCA Civ 446). Una volta accertata la ragionevolezza dell'aspettativa, il giudice dovrà bilanciare l'interesse individuale con quello pubblico all'utilizzo dell'informazione. Il bilanciamento sarà compiuto caso per caso.

Questo approccio è più simile alla protezione della privacy nella dimensione della riservatezza, utilizzando il concetto statunitense di «reasonable expectation of privacy», non solo tra pubblico e privato, ma anche tra privati, rispetto alla tutela dei dati personali per come concepita dall'ordinamento europeo. Il diritto alla riservatezza viene introdotto grazie all'interpretazione dell'art. 8 della Cedu che, come anticipato, è stata incorporata nella legislazione inglese dallo Human Rights Act del 1998.

In ogni caso, al diritto alla protezione dei dati personali sono dedicati il «Data Protection Act», che contiene l'«UK GDPR», e i «Privacy and Electronic Communications Regulations» (PECR).

Il Data Protection Act (DPA) è stato emanato nel 1998 in attuazione della Direttiva madre 95/46/CE. È stato successivamente sostituito dal «Data Protection Act» del 2018 e nel gennaio 2021 quest'ultimo Act è stato emendato per adeguarlo all'uscita del Regno Unito dall'UE, con l'inserimento dell'«UK GDPR» nella Part 2.

L'«UK GDPR» è in realtà il GDPR come adottato a livello interno dallo «European Union Withdrawal Act» del 2018. Ad oggi il DPA è così composto da sette parti:

– Part 1 «Prelimirary» sull'ambito di applicazione, in cui si statuisce che ha ad oggetto il trattamento i dati personali (section 1), e dove si trovano le definizioni (section 3);
– Part 2 «General processing», ossia l'«UK GDPR»;
– Part 3 «Law enforcement processing», che ha trasposto la Direttiva 2016/680, disciplinante i trattamenti svolti dall'autorità pubblica per le finalità di prevenzione, accertamento, repressione dei reati o tutela dell'ordine e della sicurezza pubblici [sulla direttiva, vedi → Capitolo 7];
– Part 4 «Intelligence services processing», che si applica al trattamento di dati svolto da parte di un servizio di intelligence inglese ed in particolare dal Security Service, Secret Intelligence Service e dai Government Communications Headquarters;
– Part 5 «The Information Commissioner», che istituisce l'autorità predisposta per il controllo dei trattamenti di dati personali, ossia l'Information Commissioner's Office (ICO), regolandone i compiti e poteri;
– Part 6 «Enforcement», contenente le regole sui procedimenti investigativi e sanzionatori dell'ICO e, più in generale, sulla responsabilità per la violazione dell'Act e i rimedi giurisdizionali e amministrativi;
– Part 7 «Supplementary and final provision», in si trovano varie disposizioni di settore.

Per quanto riguarda alcune particolarità della normativa inglese, il DPA ha introdotto eccezioni al riconoscimento di diritti dell'interessato (schedule 2), come nel caso della «migration exception». I diritti, infatti, non sono riconosciuti nel contesto dei trattamenti che hanno finalità di mantenimento di un efficace controllo dell'immigrazione, o per l'indagi-

ne o l'individuazione di attività che potrebbero compromettere il mantenimento di un efficace controllo dell'immigrazione (schedule 2, 4(1)).

Altre eccezioni riguardano il contesto penale (schedule 2, 2), i privilegi del Parlamento e della Corona (schedule 2, 13-15), la tutela della libertà di espressione (schedule 2, Part 5), l'uso dei dati personali per finalità di ricerca, statistica o di archiviazione nel pubblico interesse (schedule 2, Part 6) o i dati sanitari, relativi ai lavoratori e ai minori (schedule 3).

Il DPA, inoltre, consente il trattamento di particolari categorie di dati personali per salvaguardare la sicurezza nazionale o per scopi di difesa (section 26). Si tratta, perciò, di una nuova eccezione, e così base giuridica, rispetto a quanto previsto dall'art. 9, par. 2, del GDPR. Nel 2021, l'ICO ha pubblicato delle linee guida su tale eccezione[10]. Secondo l'autorità è possibile utilizzare questa base giuridica se si può dimostrare che il rispetto del divieto al trattamento dei dati particolari in questione è incompatibile con la salvaguardia della sicurezza nazionale e quando il non riconoscimento dei diritti dell'interessato fa sì che le persone non possano trarre conclusioni dannose per la sicurezza nazionale.

L'«UK GDPR» fissa a tredici anni l'età per la validità del consenso di un minore ad un servizio della società dell'informazione. Il Regno Unito ha pertanto optato per l'età che il GDPR considera minima per prestare il consenso (art. 8, par. 1, GDPR). Il medesimo atto aggiunge agli elementi richiesti per elaborare il registro del trattamento dei dati del GDPR (art. 30) le misure di sicurezza richieste dal DPA. L'«UK GDPR» non contiene tutte le regole sulle autorità di controllo del GDPR, essendo l'ICO già regolato nel DPA e non essendo più tenuto il Regno Unito alla cooperazione tra autorità richiesta tra gli Stati Membri (artt. 60 e ss.).

Anche le norme sul trasferimento transfrontaliero divergono in parte, essendo ora il paese all'esterno dell'UE. Rimane comunque la possibilità che venga adottata una decisione di adeguatezza [vedi → Capitolo 6] che consideri legittimi i trasferimenti di dati personali da Regno Unito a UE, o viceversa. Il 28 giugno 2021 la Commissione ha pubblicato tale decisione rilevando che le norme sulla protezione dei dati nel Regno Unito rispecchiano in molti aspetti le norme applicabili nel diritto europeo (par.

10 Si v. le linee guida nel sito dell'ICO in https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/national-security-and-defence/.

16, C(2021) 4800 final) e concludendo che esse assicurano un livello di protezione adeguato. Questa decisione, comunque, non si applica ai dati trasferiti in materia di immigrazione alla luce delle restrizioni che il DPA prevede in tale contesto e della vaghezza delle regole.

Infine, i «Privacy and Electronic Communications Regulations» disciplinano il trattamento di dati personali nel contesto delle comunicazioni elettroniche, stabilendo regole per la gestione dei dati relativi al traffico, sulle chiamate con finalità commerciale e promozionali, e sui c.d. *cookie* [vedi → Capitolo 7].

CAPITOLO 6.
Il trasferimento internazionale di dati personali

Giorgia Bincoletto

6.1 Il trasferimento di dati personali all'estero

Nella società dell'informazione, caratterizzata dal c.d. «cyberspazio», e all'interno di un mondo globalizzato in cui opera una «data economy», i dati personali circolano al di là dei confini geografici degli ordinamenti giuridici.

Il trasferimento di dati da un paese in cui si è originato il trattamento ad uno diverso per conseguire una successiva finalità, o per adempiere alle finalità principali, implica inevitabilmente un cambiamento di regole applicabili.

Secondo Solove e Schwartz, le differenze di protezione tra i regimi giuridici in materia di *informational* privacy creano almeno due ordini di problemi [Solove, Schwartz 2021, 1259]:

– i diversi livelli di protezione dei dati personali possono ostacolare un flusso fluido ed efficiente di informazioni tra i vari paesi;
– quando i dati personali attraversano le frontiere, i paesi d'origine dipendono dal livello di protezione dei dati accordato dai paesi di destinazione.

Con riferimento al livello di protezione dei dati personali durante un trasferimento internazionale, si tenderà a confrontare l'intera disciplina dei diversi ordinamenti, dovendo al contempo considerare la situazione politica e democratica del paese finale in cui i dati personali vengono trasferiti. Si vedrà, infatti, come le decisioni della Corte di Giustizia sugli

accordi tra UE e Stati Uniti per il trasferimento di dati personali non siano fondate soltanto su argomentazioni strettamente giuridiche, ma anche su dati fattuali, tra cui il sistema di pervasiva sorveglianza che è operato oltreoceano dalle agenzie di *intelligence* e di cui si ha conoscenza fin dalle indiscrezioni di Edward Snowden.

Ebbene, nel 2013 l'ex impiegato di una società statunitense che lavorava per la National Security Agency rivelava la presenza del programma di sorveglianza di massa PRISM da parte delle agenzie federali [Caso 2021, 25, 238]. Da qui ha avuto origine lo scandalo «Datagate». Tutto il mondo scopriva che i servizi di intelligence degli Stati Uniti stavano trattando enormi quantità di dati personali non solo di cittadini lì residenti, ma anche, e soprattutto, di individui appartenenti ad altri paesi [Snowden 2019]. I dati venivano estratti dal web e trattati tramite sofisticati software per esigenze di sicurezza nazionale. Così, la protezione dei dati personali veniva inevitabilmente compromessa a favore di un sistema di controllo generalizzato ed indifferenziato di enorme portata.

Al di là di questo particolare scenario, il trasferimento internazionale di dati avviene quotidianamente per varie finalità, tra cui l'operatività di servizi digitali, come quelli cloud o di social network, i cui server sono abitualmente collocati in un luogo diverso rispetto a quello da cui l'utente accede ai dati personali, o per la risoluzione di controversie che coinvolgono più giurisdizioni, i cui fascicoli e così i dati giudiziari trattati devono essere trasmessi tra più corti nazionali o locali.

Nelle prossime sezioni si adotterà il punto di vista del diritto dell'Unione europea, si presenteranno le regole previste come condizioni per il trasferimento internazionale di dati e si analizzeranno i *leading case* della CGUE prima e dopo l'applicazione del GDPR.

6.2 Il trasferimento di dati personali verso paesi terzi o organizzazioni internazionali nel diritto europeo prima del GDPR

La Direttiva 95/46/CE ha introdotto per la prima volta un regime applicabile ai trasferimenti di dati personali al di fuori del territorio dell'allora Comunità europea, considerandoli un aspetto rilevante in quanto «necessari allo sviluppo degli scambi internazionali» (Cons. 56). In particolare, la Direttiva prevedeva all'art. 25 che un trasferimento di dati perso-

nali verso un paese terzo potesse aver luogo soltanto se questo paese garantiva «un livello di protezione adeguato» da valutarsi con riguardo a tutte le circostanze relative al trattamento, tra cui «la natura dei dati, le finalità del o dei trattamenti previsti, il paese d'origine e il paese di destinazione finale, le norme di diritto, generali o settoriali, vigenti nel paese terzo di cui trattasi, nonché le regole professionali e le misure di sicurezza *ivi* osservate».

Qualora il paese terzo non avesse garantito un livello di protezione adeguato, il trasferimento sarebbe stato vietato per applicazione della regola generale. Diversamente, la Commissione europea poteva adottare una «decisione di adeguatezza» e così rendere operativi i trasferimenti dei dati personali verso uno specifico paese, esonerando il titolare del trattamento dal compiere una valutazione sulle condizioni applicabili (art. 25, n. 6). In alternativa e in assenza di decisioni di adeguatezza, il trasferimento risultava consentito in presenza di una delle condizioni dell'art. 26, quali la necessità di trasferire i dati personali per l'esecuzione di un contratto o per la salvaguardia dell'interesse vitale della persona interessata.

La Direttiva non conteneva una nozione di trasferimento verso un paese terzo. La nozione è stata indirettamente chiarita dalla Corte di Giustizia con riferimento al caricamento di dati su Internet. Secondo l'interpretazione fornita dalla CGUE nella sentenza Bodil Lindqvist (C-101/01), non si considerava trasferimento l'inserimento di dati personali in una pagina Internet da parte di una persona fisica che si trovava in uno Stato membro, nonostante tali dati fossero resi accessibili ad un numero indefinito di persone che si trovavano in molteplici luoghi e in qualunque momento nel mondo, in quanto caricati sul sito di un *hosting provider* stabilito altrove. Ciò perché la previsione del divieto al trasferimento dei dati in un paese «inadeguato» avrebbe dovuto applicarsi in via generale per ogni caricamento, risultando a quel punto necessario un controllo preliminare ad ogni attività di circolazione di dati personali su Internet. Si poteva affermare, dunque, che un trasferimento richiedeva una trasmissione di dati personali nel contesto di un'attività di trattamento e per una determinata finalità. In concreto, il trasferimento necessitava di un atto positivo del titolare o del responsabile del trattamento, e non una mera e passiva messa a disposizione da parte dell'interessato o di altro sog-

getto. Tale nozione, peraltro, non si riferiva soltanto al primo passaggio di dati, ma anche a tutte le comunicazioni successive.

Nel 2000, la Commissione ha autorizzato il trasferimento di dati dall'allora Comunità europea agli Stati Uniti, laddove le organizzazioni a cui venivano trasmessi i dati si fossero conformate ai «principi dell'approdo sicuro in materia di riservatezza», ossia ai «Safe Harbor Privacy Principles» (Decisione 520/2000/CE). Le condizioni del trasferimento venivano considerate adeguate dalla Commissione alla luce delle informazioni ricevute dal Dipartimento del commercio degli Stati Uniti. Un'organizzazione statunitense che voleva ricevere dati personali da un'altra stabilita nella Comunità poteva registrarsi per la qualificazione di «approdo sicuro» nel sito dedicato, mantenendo l'impegno a rispettare i principi descritti nell'Allegato I della Decisione (notifica, scelta, trasferimento successivo, sicurezza, integrità dei dati, accesso, garanzie d'applicazione). In caso di violazione, la Federal Trade Commission e il Department of Transportation avrebbero potuto esaminare le denunce degli interessati ed emettere provvedimenti inibitori verso le società statunitensi.

Il sistema era quindi basato su un regime di volontarietà e auto-certificazione dei titolari, responsabili e destinatari del trattamento dei dati. L'adeguatezza del singolo destinatario risultava presunta, se questi dichiarava di adottare i principi del Safe Harbor. Questi principi dovevano essere rispettati per fornire una tutela adeguata ai dati personali e dovevano essere sempre applicati, a meno che non si verificassero alcune eccezioni, come la necessità di soddisfare esigenze di sicurezza nazionali, per interesse pubblico di una particolare autorità o per l'amministrazione della giustizia. In questi casi, quindi, i dati personali venivano trasmessi ad autorità pubbliche e potevano non essere trattati con una protezione adeguata secondo la Direttiva.

Oltre alla decisione di adeguatezza, nel 2010 la Commissione ha adottato la decisione 2010/87/UE relativa alle clausole contrattuali tipo, che consentiva il trasferimento di dati personali sulla base di specifiche condizioni da sottoscrivere tra il titolare del trattamento e l'organizzazione destinataria. Questo meccanismo autorizzava, perciò, i trasferimenti di dati in presenza di specifiche garanzie contrattuali adottate sullo schema di quelle indicate dalla Commissione.

Gli scambi di dati tra Europa e Stati Uniti avvenivano per la maggior parte sulla base della decisione di adeguatezza «Safe Harbor» e, così, del

regime di auto-certificazione dei titolari del trattamento. A seguito delle rivelazioni di Snowden, iniziarono vari sospetti sul livello di protezione garantito sui dati all'interno dell'ordinamento statunitense.

Il 25 giugno 2013, il giovane austriaco Maximillian Schrems[1] ha presentato un reclamo presso il Commissario irlandese, quale autorità di controllo preposta alla protezione dei dati personali in Irlanda, chiedendo di vietare a Facebook Ireland di trasferire i suoi dati verso gli Stati Uniti perché questo paese non forniva la protezione adeguata richiesta dalla Direttiva. Facebook, oltre ad avere la sede legale nella Silicon Valley, aveva (e ha tutt'oggi) uno stabilimento in Irlanda, e trasferiva i dati raccolti dal social network sui server collocati nel territorio degli Stati Uniti. Per tale ragione, Schrems si è rivolto all'autorità irlandese.

In questa denuncia Schrems sosteneva che gli Stati Uniti non offrivano una protezione sufficiente ai dati personali conservati all'interno dell'ordinamento, anche considerando le attività dei servizi di intelligence, e in particolare quelle della National Security Agency.

Il Commissario irlandese tuttavia rigettava il reclamo, considerandosi non competente a decidere sulla questione, anche per la presenza della decisione di adeguatezza della Commissione europea 520/2000/CE che legittimava i trasferimenti di dati verso gli Stati Uniti, e sottolineando la mancanza di prove concrete sull'accesso dell'NSA ai dati personali dei cittadini europei (ricorrente compreso).

Schrems presentava poi ricorso presso la High Court (Corte d'Appello) irlandese. Questa riconosceva l'esistenza di «un serio dubbio» sul fatto che vi fosse un livello di protezione adeguato nell'ordinamento statunitense, visto l'accesso «massivo e indifferenziato» da parte delle agenzie di intelligence ai dati dei social network, che poteva considerarsi contrario ai principi del diritto irlandese a protezione dei dati e della vita privata degli individui. La Corte decideva comunque di presentare un rinvio pregiudiziale alla Corte di Giustizia dell'Unione Europea per risolvere le seguenti due questioni:

1 Si può segnalare che prima della vicenda giudiziaria Schrems aveva effettuato un soggiorno di studio alla Santa Clara University in cui aveva incontrato un legale di Facebook ed iniziato ad interessarsi attivamente alle problematiche relative alla protezione dei dati e alla loro gestione da parte del sempre più utilizzato social network.

> 1) Se, nel decidere in merito a una denuncia presentata a un'autorità indipendente investita per legge delle funzioni di gestione e di applicazione della legislazione sulla protezione dei dati, secondo cui i dati personali sono trasferiti a un paese terzo (nel caso di specie, gli Stati Uniti d'America) il cui diritto e la cui prassi si sostiene non prevedano adeguate tutele per i soggetti interessati, tale autorità sia assolutamente vincolata dalla constatazione in senso contrario dell'Unione contenuta nella decisione 2000/520, tenuto conto degli articoli 7, 8 e 47 della Carta, nonostante le disposizioni dell'articolo 25, paragrafo 6, della direttiva 95/46.
> 2) Oppure, in alternativa, se detta autorità possa e/o debba condurre una propria indagine sulla questione alla luce degli sviluppi verificatisi nel frattempo, successivamente alla prima pubblicazione della decisione 2000/520.

Con queste la Corte chiedeva, quindi, se l'autorità nazionale preposta alla protezione dei dati personali (come la Commissione irlandese) fosse vincolata alla decisione di adeguatezza della Commissione, sulla base dell'art. 25 della Direttiva, o se potesse condurre un'autonoma indagine sul livello di protezione del paese terzo, riferendosi alla domanda dell'interessato che volta per volta veniva chiamata a risolvere, anche alla luce dei principi e diritti della Carta dei diritti fondamentali dell'Unione Europea.

Con la causa C-362/14 *Maximillian Schrems v. Data Protection Commissioner*, la CGEU ha deciso su tali questioni, invalidando la decisione di adeguatezza della Commissione europea c.d. «Safe Harbor».

Le argomentazioni della Corte di Giustizia possono essere così riassunte. Una decisione di adeguatezza della Commissione è soggetta alla conformità con i Trattati, i principi generali del diritto europeo e i diritti fondamentali, così come con tutti gli altri atti adottati dalle istituzioni europee. La Corte ha invece competenza esclusiva a dichiarare l'invalidità di un atto di diritto dell'UE, dal momento che un'autorità nazionale non ha questa competenza. Se quest'ultima fosse investita di una domanda relativa alla protezione dei dati personali da parte di un interessato, essa dovrebbe esaminare diligentemente tale domanda per adempiere correttamente ai suoi doveri, e qualora rilevasse un'incompatibilità con i principi di diritto europeo, dovrebbe promuovere un rinvio pregiudiziale presso i giudizi della sua nazione.

Il termine «adeguato» livello di tutela richiesto per legittimare i trasferimenti di dati personali si riferisce alla necessità che la protezione fornita nel paese destinatario sia «sostanzialmente equivalente» a quella garantita all'interno dell'Unione europea (si v. il par. 74 della sentenza).

La decisione 520/2000, basata su un sistema di auto-certificazione, consente la disapplicazione dei principi «Safe Harbor» per esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia e ciò rende possibili le ingerenze da parte delle autorità di intelligence americane, senza che vi siano specifiche tutele giuridiche, distinzioni o limitazioni a seconda dell'obiettivo perseguito dalle stesse e in mancanza di un criterio oggettivo per l'accesso ai dati.

Una normativa che consente alle autorità pubbliche di accedere in modo generalizzato ai dati personali degli individui pregiudica il contenuto essenziale del diritto alla protezione dei dati e alla tutela della vita privata (artt. 7 e 8 della Carta di Nizza). Nell'adottare la decisione 520/2000 la Commissione non ha affermato che gli Stati Uniti garantiscono «effettivamente» un livello di protezione adeguato in considerazione della «legislazione nazionale o dei loro impegni internazionali» (si v. il par. 97 della sentenza); perciò, in assenza di tale analisi, la decisione di adeguatezza è da considerarsi invalida.

Infine, una decisione della Commissione non osta a che l'autorità di controllo nazionale esamini la domanda dell'interessato che faccia valere il fatto che il diritto e la prassi del paese di destinazione dei dati non garantiscono un livello di protezione adeguato. L'autorità di controllo può condurre un'indagine specifica, anche attribuendo rilievo agli sviluppi successivi all'adozione di una decisione.

La decisione 520/2000 venne così annullata dalla CGUE nel 2015. A seguito di questa sentenza, oggi conosciuta come «Schrems I», la High Court annullò la decisione della Commissione irlandese che iniziò un'indagine sui meccanismi di trasferimento dei dati personali operati da Facebook Ireland a Facebook Inc. negli Stati Uniti. La Commissione europea, dal canto suo, avviò un procedimento per l'emanazione di una nuova decisione di adeguatezza per i trasferimenti di dati personali verso questo ordinamento giuridico.

Dall'indagine del Commissario irlandese emergeva che Facebook aveva già modificato la base giuridica per il trasferimento dei dati, scegliendo la sottoscrizione di clausole contrattuali tipo, al posto dell'adesione

ai meccanismi di decisione di adeguatezza. A questo punto, l'autorità di controllo richiedeva a Schrems di riformulare la sua denuncia.

Nel dicembre 2015 Schrems ripresentava al Commissario irlandese la richiesta di vietare il trasferimento dei suoi dati personali da Facebook Ireland a Facebook Inc. sulla base del fatto che la società continuava a mettere a disposizione i dati alle autorità statunitensi, seppur con un diverso meccanismo. Per poter decidere, nel 2016, il Commissario adiva direttamente la High Court irlandese perché si rivolgesse alla CGUE con un nuovo rinvio pregiudiziale.

Nel frattempo, la Decisione 2016/1250, c.d. «Privacy Shield» – «Scudo per la privacy», veniva adottata dalla Commissione europea, dopo una valutazione della normativa degli Stati Uniti e a seguito dell'impegno da parte del governo statunitense a creare un meccanismo di vigilanza sulle ingerenze delle autorità pubbliche per motivi di sicurezza nazionale (cd. Mediatore dello scudo). I due principali strumenti giuridici per consentire il sistema di vigilanza delle agenzie erano l'Executive Order 12333 del Presidente degli Stati Uniti e la Presidential Policy Directive 28, mentre l'art. 702 del Foreign Intelligence Surveillance Act (FISA) autorizzava specifici programmi di sorveglianza a livello federale, tra cui PRISM, già oggetto delle rivelazioni di Snowden. Il FISA prevedeva dei mezzi per i cittadini stranieri per contestare la sorveglianza illecita. Il livello di protezione assicurato negli Stati Uniti veniva così considerato «adeguato» dall'art. 1 della Decisione 2016/1250.

Il nuovo regime per il trasferimento consisteva in un sistema di accreditamento delle società statunitensi aderenti ai principi dello scudo. Un registro riportava le organizzazioni a cui era possibile trasferire i dati personali. Le eccezioni alla protezione dei dati per motivi di sicurezza nazionale venivano riproposte nella nuova decisione, ma risultavano limitate dal controllo operato dal Mediatore dello scudo sulla concreta finalità perseguita dall'accesso.

Nel 2017 la High Court proponeva un nuovo rinvio pregiudiziale alla CGUE con undici, molto complesse, questioni. La causa C-311/18, *Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems*, verteva sull'interpretazione degli articoli 25 e 26 della Direttiva, e sull'interpretazione e validità di due decisioni della Commissione europea: la Decisione 2010/87/UE relativa alle clausole contrattuali tipo e la Decisione di esecuzione 2016/1250 sull'adeguatezza della protezione

offerta dal regime dello scudo UE-USA per la privacy. Tuttavia, nelle more del giudizio, identificato con il nome «Schrems II», la Direttiva 95/46/CE veniva abrogata dal GDPR, che aveva difatti modificato le regole sul trasferimento internazionale di dati. Dal momento che la Corte ha deciso alla luce del nuovo Regolamento e non delle norme della Direttiva (si v. par. 79 della sentenza), è così necessario presentare il nuovo regime per il trasferimento dei dati applicabile dal 25 maggio 2018 e, solo in seguito, analizzare l'importante pronuncia.

6.3 Il trasferimento di dati personali verso paesi terzi o organizzazioni internazionali nel diritto europeo dopo il GDPR

L'art. 44 del GDPR apre il Capo V dedicato alle regole sul trasferimento di dati personali al di fuori dell'Unione europea e dello Spazio Economico Europeo (oltre all'UE, Norvegia, Liechtenstein, Islanda) verso un paese terzo o un'organizzazione internazionale. Ai sensi di questa norma i dati personali non possono essere trasferiti a meno che non si rispettino le condizioni previste dal Capo V, in modo da assicurare che il livello di protezione dei dati garantito dal GDPR non sia pregiudicato. Sul punto, come anticipato, assume primaria importanza un'analisi comparata tra le garanzie previste dai diversi ordinamenti giuridici coinvolti in concreto nelle attività di trattamento.

Come specificato dal Considerando 102, gli Stati membri hanno la possibilità di concludere accordi internazionali che implicano il trasferimento di dati personali verso paesi terzi o organizzazioni internazionali; tuttavia, questi accordi non potranno incidere su quanto previsto dal GDPR o dal diritto dell'UE e dovranno includere un adeguato livello di protezione per i diritti fondamentali degli interessati. Il concetto chiave è, dunque, e ancora una volta, l'adeguatezza delle tutele fornite nel paese in cui è stabilito il soggetto destinatario dei dati personali.

In aggiunta alla necessità di una base giuridica, il GDPR prevede altre regole sul trasferimento dei dati. L'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo deve infatti essere comunicata all'interessato attraverso l'informativa (artt. 13 e 14 GDPR), seguendo le modalità di trasparenza e chiarezza prescritte dalla normativa (art. 12 GDPR). Si ricorda che questo documento è tra i più conosciuti e

diffusi in materia di privacy e deve essere elaborato dal titolare del trattamento indicando diversi elementi a seconda che i dati siano raccolti presso l'interessato (art. 13 del GDPR) o presso terzi (art. 14 del GDPR), utilizzando un linguaggio semplice e chiaro e scegliendo una forma concisa, trasparente, intellegibile e facilmente accessibile (art. 12 del GDPR). L'interessato ha anche diritto ad essere informato sulle garanzie applicate al trasferimento, quale forma del suo generale diritto di accesso (art. 15, par. 2 GDPR).

Nemmeno nel GDPR è prevista una definizione di trasferimento di dati, che può comunque intendersi come un'attività di trattamento che consiste nella comunicazione o messa a disposizione di dati personali da un titolare o responsabile del trattamento soggetto al GDPR (si v. gli ambiti di applicazione materiale e territoriale agli artt. 2 e 3 GDPR, [vedi → Capitolo 3]) ad un responsabile del trattamento o altro titolare o soggetto terzo ricevente che sono stabiliti in un paese terzo o un'organizzazione internazionale.

L'attività di trasferimento può avvenire solo in presenza di precise condizioni. Le basi giuridiche per tale trasferimento sono regolate dagli artt. 45-49 del GDPR e possono essere divise in tre gruppi: la decisione di adeguatezza (art. 45 GDPR), le garanzie adeguate (artt. 46-48 GDPR), le deroghe in specifiche situazioni (art. 49 GDPR).

La prima base giuridica per un trasferimento è la presenza di una decisione di adeguatezza della Commissione europea, che esclude la necessità di autorizzazioni specifiche per il titolare o il responsabile, vista la previa analisi sull'adeguato livello di protezione compiuto dall'autorità sulla base dei seguenti elementi (art. 45, par. 2):

> a) lo stato di diritto, il rispetto dei diritti umani e delle libertà fondamentali, la pertinente legislazione generale e settoriale (anche in materia di sicurezza pubblica, difesa, sicurezza nazionale, diritto penale e accesso delle autorità pubbliche ai dati personali), così come l'attuazione di tale legislazione, le norme in materia di protezione dei dati, le norme professionali e le misure di sicurezza, comprese le norme per il trasferimento successivo dei dati personali verso un altro paese terzo o un'altra organizzazione internazionale osservate nel paese o dall'organizzazione internazionale in questione, la giurisprudenza nonché i diritti effettivi e azionabili degli interessati e un ricorso effettivo in sede amministrativa e giudiziaria per gli interessati i cui dati personali sono oggetto di trasferimento;

> b) l'esistenza e l'effettivo funzionamento di una o più autorità di controllo indipendenti nel paese terzo o cui è soggetta un'organizzazione internazionale, con competenza per garantire e controllare il rispetto delle norme in materia di protezione dei dati, comprensiva di adeguati poteri di esecuzione, per assistere e fornire consulenza agli interessati in merito all'esercizio dei loro diritti e cooperare con le autorità di controllo degli Stati membri; e
> c) gli impegni internazionali assunti dal paese terzo o dall'organizzazione internazionale in questione o altri obblighi derivanti da convenzioni o strumenti giuridicamente vincolanti come pure dalla loro partecipazione a sistemi multilaterali o regionali, in particolare in relazione alla protezione dei dati personali.

La decisione di adeguatezza della Commissione è, in ogni caso, soltanto uno dei possibili meccanismi di trasferimento dei dati e per essere adottata richiede il parere del Comitato europeo per la protezione dei dati (EDPB) e deve seguire la procedura prevista dall'art. 45, paragrafi 3-9. La sua adozione, comunque, facilita i titolari del trattamento, che non devono trovare altre condizioni, ma comunque adottare le misure a protezione dei dati richieste dal Regolamento (artt. 24-36 GDPR). Il GDPR peraltro richiede un'attività di monitoraggio, almeno ogni quattro anni, per verificare periodicamente il livello di protezione del paese terzo.

Attualmente sono in vigore le decisioni di adeguatezza riguardanti i seguenti stati: Andorra; Argentina; Australia; Canada (soltanto per i trattamenti soggetti al PIPEDA); Giappone; Guernsey; Isola di Man; Isole Faroe; Israele; Jersey; Nuova Zelanda; Regno Unito (soltanto per l'adeguamento al GDPR e alla Direttiva 2016/680); Repubblica di Korea; Svizzera; Uruguay.

In mancanza di una decisione, il trasferimento di dati personali può avvenire in presenza di una di queste garanzie adeguate:

- la sottoscrizione di uno strumento giuridicamente vincolante e avente efficacia esecutiva tra autorità pubbliche o organismi pubblici che trasmettono dati personali (art. 46, par. 2, lett. a), GDPR);
- la sottoscrizione di norme vincolanti d'impresa (art. 46, par. 2, lett. b), GDPR), disciplinate nel dettaglio dall'art. 47 GDPR che richiede l'approvazione da parte di un'autorità di controllo;
- la presenza e applicazione delle clausole tipo di protezione dei dati, adottate dalla Commissione ai sensi dell'art. 93, par. 2 GDPR e quindi

dell'art. 5 del Reg. 182/2011 sulle competenze di esecuzione attribuite a quest'autorità (art. 46, par. 2, lett. c), GDPR);
– la presenza e applicazione delle clausole tipo di protezione dei dati, adottate da un'autorità di controllo nazionale e poi approvate dalla Commissione secondo la procedura d'esame dell'art. 5 del Reg. 182/2011 (art. 46, par. 2, lett. d), GDPR);
– la presenza e applicazione di un codice di condotta, approvato secondo le regole del GDPR (art. 40), unitamente all'impegno vincolante ed esecutivo del titolare o del responsabile del trattamento ad applicare le garanzie adeguate nel paese terzo, anche con riferimento ai diritti degli interessati (art. 46, par. 2, lett. e), GDPR);
– la presenza e applicazione di un meccanismo di certificazione, approvato secondo le regole del GDPR (art. 42), unitamente all'impegno vincolante ed esigibile del titolare o del responsabile del trattamento ad applicare le garanzie adeguate nel paese terzo, anche con riferimento ai diritti degli interessati (art. 46, par. 2, lett. f), GDPR);
– la sottoscrizione di clausole contrattuali tra il titolare del trattamento o il responsabile del trattamento e il titolare del trattamento, il responsabile del trattamento o il destinatario dei dati personali nel paese terzo o nell'organizzazione internazionale (art. 46, par. 3, lett. a), GDPR);
– la presenza di disposizioni inseribili in accordi amministrativi tra autorità pubbliche o organismi pubblici che comprendono diritti effettivi e azionabili per gli interessati (art. 46, par. 3, lett. b), GDPR).

In mancanza di una decisione della Commissione e di una delle garanzie adeguate appena descritte, il trasferimento dei dati personali può avvenire sulla base di una di queste deroghe previste dall'art. 49 GDPR:
– l'interessato ha esplicitamente prestato il consenso al trasferimento proposto, dopo essere stato informato dei possibili rischi dovuti alla mancanza di altri meccanismi di trasferimento;
– il trasferimento risulta necessario per l'esecuzione di un contratto concluso tra l'interessato e il titolare del trattamento ovvero per l'esecuzione di misure precontrattuali adottate su istanza dell'interessato;
– il trasferimento è necessario per la conclusione o l'esecuzione di un contratto stipulato tra il titolare del trattamento e un'altra persona fisica o giuridica a favore dell'interessato;

– il trasferimento è necessario per importanti motivi di interesse pubblico;
– il trasferimento risulta necessario per accertare, esercitare o difendere un diritto in sede giudiziaria;
– il trasferimento è necessario per tutelare gli interessi vitali dell'interessato o di altre persone, nei casi in cui l'interessato si trovasse nell'incapacità fisica o giuridica di prestare il proprio consenso;
– il trasferimento è effettuato «a partire da un registro che, a norma del diritto dell'Unione o degli Stati membri, mira a fornire informazioni al pubblico e può esser consultato tanto dal pubblico in generale quanto da chiunque sia in grado di dimostrare un legittimo interesse, solo a condizione che sussistano i requisiti per la consultazione previsti dal diritto dell'Unione o degli Stati membri».

Il GDPR ha, dunque, aumentato le possibili condizioni per i trasferimenti di dati. Ciò nonostante, la decisione di adeguatezza rimane il meccanismo a cui ci si affida nella maggior parte dei casi. L'altro meccanismo frequentemente utilizzato è la clausola contrattuale tipo di protezione dei dati, che, come visto, può essere definita dalla Commissione o dall'autorità di controllo nazionale.

Nella sentenza «Schrems II» la Corte di Giustizia si è trovata a decidere sull'operatività di entrambi questi strumenti.

Come anticipato, la causa C-311/18 contiene undici questioni pregiudiziali. La decisione della Corte può essere riassunta come segue. Con la prima questione la CGUE indaga se il Regolamento si applica ad un trasferimento di dati personali effettuato da un operatore economico stabilito in uno Stato membro verso un altro operatore stabilito in un paese terzo nel caso in cui durante o in seguito a tale trasferimento i dati personali sono trattati dalle autorità del suddetto paese terzo a fini di sicurezza pubblica, di difesa e di sicurezza dello Stato (si v. par. 80 e ss. della sentenza). Ciò avviene, ad esempio, nel caso in cui l'autorità di intelligence chieda l'accesso a Facebook per finalità di sicurezza nazionale. Secondo la Corte, la possibilità che i dati personali siano trattati a questi fini da parte delle autorità del paese terzo non esclude il trattamento principale dall'ambito di applicazione territoriale e materiale del GDPR, perché non vi sono eccezioni applicabili in senso opposto.

Le successive tre questioni (seconda, terza e quarta) riguardano la definizione del livello di protezione richiesto dall'articolo 46 del GDPR per le clausole tipo di protezione dei dati e, in particolare, il chiarimento sugli elementi da prendere in considerazione per determinare se il livello di protezione è concretamente garantito nel contesto di un trasferimento di dati personali (si v. par. 90 e ss.). Sul punto, i giudici di Lussemburgo hanno ribadito che il paese terzo non deve prevedere un livello di protezione identico, ma «sostanzialmente equivalente» a quello europeo che è fornito dal Regolamento e dalla Carta di Nizza. In presenza di un trasferimento basato su clausole contrattuali tipo, la valutazione di adeguatezza deve considerare sia il contenuto delle clausole convenute tra il titolare del trattamento o il responsabile del trattamento stabiliti nell'Unione e il destinatario del trasferimento stabilito nel paese terzo, sia gli elementi rilevanti del sistema giuridico di destinazione, ossia gli stessi elementi che la Commissione deve valutare quando procede all'elaborazione di una decisione di adeguatezza (art. 45, par. 2).

La Corte ha esaminato, poi, l'ottava questione che si riferisce alla possibilità per un'autorità di controllo di sospendere o vietare un trasferimento di dati personali verso un paese terzo effettuato sulla base di clausole tipo di protezione dei dati adottate dalla Commissione, qualora la medesima autorità ritenga che tali clausole non sono o non possono essere rispettate nel paese terzo e che la protezione dei dati non può essere garantita (si v. par. 106 e ss. della decisione). Dopo aver analizzato i poteri delle autorità di controllo ai sensi dell'art. 58 del GDPR [vedi → Capitolo 10], la Corte ha risposto affermativamente all'ottava questione, chiarendo che in presenza di una decisione di adeguatezza per un paese terzo, solo la stessa Corte può dichiararne l'invalidità, come peraltro già stabilito nella precedente sentenza «Schrems I».

Le questioni numero sette e undici sono dedicate alla validità della Decisione 2010/87/UE relativa alle clausole contrattuali tipo, dal momento che l'utilizzo di questo strumento non vincola le autorità del paese terzo, ma solo le parti che le hanno sottoscritte (si v. par. 122 e ss.). Ebbene, la Corte non ha rilevato nessun elemento per inficiare la validità di tale decisione: in ogni caso il titolare del trattamento e il soggetto destinatario devono di volta in volta verificare il livello di protezione garantito nel paese terzo prescelto per non incorrere in una violazione della normativa.

Con riferimento alla quarta, quinta, nona e decima questione, è stato richiesto alla Corte di valutare la validità della decisione «Privacy Shield» e dei suoi meccanismi interni, compreso le possibili deroghe ai principi per esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia, e il Mediatore dello scudo (si v. dal par. 150 della sentenza).

La Corte ha chiarito che la comunicazione di dati personali a un terzo, quale autorità pubblica, è una forma di ingerenza nei diritti fondamentali alla protezione della vita privata e familiare (art. 7 della Carta di Nizza) e alla protezione dei dati (art. 8 della Carta) «indipendentemente dall'uso ulteriore delle informazioni» (par. 171 della sentenza). Questi diritti non sono assoluti, possono essere limitati. Tuttavia, da un'analisi dell'art. 702 del FISA, che autorizza programmi di sorveglianza, è emerso che il diritto statunitense non prevede limitazioni all'autorizzazione per l'attuazione della sorveglianza, né garanzie per i cittadini stranieri potenzialmente soggetti a tali programmi. Questa norma, secondo la Corte, non è idonea a garantire un livello di tutela sostanzialmente equivalente (par. 181 della sentenza). Nemmeno la Presidential Policy Directive 28 e l'Executive Order 12333 sono idonei perché non comprendono: un controllo giudiziario all'accesso ai dati, una limitazione alla quantità di informazioni strettamente necessarie alla finalità, alcuna possibilità per il singolo interessato di avvalersi di rimedi giuridici, come un ricorso. Il sistema di sorveglianza risulta massivo. Il Mediatore è designato dal Segretario di Stato e ciò ha posto un dubbio sulla sua indipendenza rispetto al potere esecutivo, tanto più che non è prevista una possibilità per sanzionare i servizi segreti non adempienti alle sue decisioni.

Alla luce di tali argomentazioni la Corte ha invalidato la Decisione «Privacy Shield» in quanto contraria ai requisiti dell'art. 45 GDPR e degli artt. 7 e 8 della Carta di Nizza.

Ancora una volta la Corte di Giustizia ha ricoperto un ruolo fondamentale nell'ambito della protezione dei dati personali con un impatto a livello internazionale, invalidando la decisione di adeguatezza con gli Stati Uniti, paese in cui sono stabilite le principali *Big Tech*.

A seguito della sentenza «Schrems II» del 2020 non è stato concesso un «grace period» ai titolari del trattamento, i quali hanno dovuto modificare la base giuridica per le attività di trasferimento verso gli Stati Uniti scegliendo una garanzia adeguata dell'art. 46 del GDPR.

La Commissione ha successivamente adottato la Decisione di esecuzione (UE) 2021/914 sulle clausole contrattuali tipo, fornendo quattro moduli di condizioni applicabili a seconda di quale soggetto effettui il trasferimento (da titolare a titolare, da titolare a responsabile, da responsabile a responsabile, da responsabile a titolare).

Il 18 giugno 2021 l'EDPB ha anche fornito delle Raccomandazioni relative alle misure che integrano gli strumenti di trasferimento per la responsabilizzazione di chi compie il trasferimento dei dati e garantire un livello di protezione adeguata. Secondo questa autorità le garanzie europee rappresentano uno «standard di riferimento per valutare l'ingerenza che le misure di sorveglianza di paesi terzi comportano nel contesto dei trasferimenti internazionali di dati». I «passi» fondamentali della roadmap suggerita dal Board per effettuare un «Data Transfer Impact Assessment» - DTIA sono:

– conoscere il trasferimento, analizzando e mappando le attività di trattamento;
– individuare gli strumenti di trasferimento su cui fare affidamento tra quelli previsti dal GDPR;
– valutare se il meccanismo scelto sia efficace alla luce delle concrete circostanze del trattamento, considerando sia gli elementi di diritto che le prassi vigenti nel paese terzo; in particolare, deve essere posta attenzione ai requisiti interni per la comunicazione di dati personali ad autorità pubbliche, siano agenzie di sicurezza nazionale o altre autorità, ai mezzi di ricorso azionabili contro l'accesso illegale ai dati personali, alle norme in materia di diritti e libertà fondamentali;
– adottare misure supplementari a protezione dei dati personali per prevenire il rischio che norme e prassi del paese terzo pregiudichino le garanzie contrattuali sottoscritte tra soggetto esportatore e importatore dei dati. Le misure possono avere natura contrattuale, tecnica o organizzativa;
– adempiere a passaggi procedurali;
– rivalutare il livello di protezione a intervalli appropriati.

Le autorità europee stanno progressivamente rilasciando varie raccomandazioni e linee guida per l'operatività del trasferimento internazionale di dati. Il 14 giugno 2022 l'EDPB ha pubblicato la prima versione delle Linee Guida 07/2022 sui meccanismi di certificazione quali mec-

canismi per il trasferimento. In questo documento l'autorità ha fornito importanti indicazioni sui criteri di accreditamento ed esempi di misure supplementari che possono essere implementate a maggiore sicurezza del trattamento.

L'autorità di controllo francese, la Commission Nationale de l'Informatique et des Libertés, ha reso disponibile nel suo sito una mappa interattiva[2] che indica il livello di protezione che un paese accorda ai dati personali secondo le seguenti categorie: «EU or EEA Member country»; «adequate country», «partially adequate country», paesi in cui è presente una «independent authority and law(s)», paesi in cui esiste una «data protection law(s)», paesi che hanno «no specific rule». Questa mappatura può supportare i titolari e responsabili del trattamento nella complessa valutazione sulle norme e prassi applicabili nel paese terzo e così nell'adeguatezza dell'attività di trasferimento di dati personali.

Da ultimo, nell'ottobre del 2022, il Presidente degli Stati Uniti Biden ha firmato l'Executive Order «Enhancing Safeguards for United States Signals Intelligence Activities» per implementare nella legislazione statunitense quanto statuito dalla CGUE nel caso Schrems II sulla necessaria limitazione all'accesso ai dati personali da parte dei servizi di intelligence. Questo Executive Order mira a limitare l'accesso a quanto necessario e proporzionato per proteggere la sicurezza nazionale e istituire un meccanismo di ricorso indipendente e imparziale per gli interessati. Su questa base, la Commissione europea ha preparato nel dicembre 2022 un progetto di decisione di adeguatezza denominato EU-U.S. Data Privacy Framework e avviato la procedura di adozione tra Unione europea e Stati Uniti. A gennaio 2023 questo progetto è stato presentato all'EDPB e attende un suo primo avvallo tramite una dedicata Opinion, prima di essere approvato da un comitato di rappresentanti degli Stati Membri e infine definitivamente adottato da parte della Commissione[3].

2 Si v. https://www.cnil.fr/en/data-protection-around-the-world.

3 Si segnala che, nelle more di pubblicazione, l'EDPB ha pubblicato l'Opinion 5/2023 del 28 febbraio 2023 suggerendo alla Commissione varie questioni giuridiche per aumentare le salvaguardie previste a tutela dei dati personali. Si v. https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-52023-european-commission-draft-implementing_it.

6.4 Casi 6-1, 6-2, 6-3

Caso 6-1

La società francese Alfa mira ad espandere i suoi servizi in Sud America ed in particolare in Argentina e in Brasile, dove colloca alcuni server per conservare i dati personali raccolti all'interno dello Spazio Economico Europeo. Alla luce dei possibili rischi, Alfa si rivolge al legale di fiducia per comprendere quali siano le regole giuridiche applicabili alle sue attività di trattamento e ai futuri trasferimenti di dati.
Quali norme o documenti di soft-law devono essere considerati?
È necessario distinguere le condizioni per le diverse destinazioni?
Quali meccanismi di trasferimento dei dati sono individuabili?

Caso 6-2

Il professore universitario Tizio intende caricare i dati degli esami scritti dei suoi studenti nel cloud della società Beta come strumento di backup. Nel sito di Beta si specifica che le sue piattaforme cloud sono stabilite al di fuori dello Spazio Economico Europeo, nel Regno Unito, ma nell'informativa privacy del servizio nulla viene specificato sulla presenza di un trasferimento di dati personali in siti terzi. Tizio, a questo punto, decide di chiedere consiglio al DPO della sua università per capire se possa continuare ad utilizzare il servizio cloud senza porre a rischio i dati personali raccolti.
Quali previsioni normative e documenti di soft-law devono essere tenuti conto dal DPO nell'elaborare la sua risposta?

Caso 6-3

Nel 2019 l'università italiana Gamma ha concluso un accordo con l'università statunitense Delta per lo scambio di visite di docenti e ricercatori, lo scambio di studenti e assegnisti di ricerca e per altre forme di collaborazione, come lo sviluppo di progetti di ricerca. Durante la pandemia, nel 2020, la Corte di Giustizia ha invalidato la decisione cd. Privacy Shield e Gamma si è vista costretta a contattare gli uffici di Delta per definire una nuova base giuridica per il trasferimento dei dati personali dei soggetti coinvolti nell'attività di collaborazione.
Quali norme o documenti di soft-law devono essere considerati?
Quali meccanismi di trasferimento dei dati sono individuabili?

CAPITOLO 7.
Le disposizioni relative alle comunicazioni elettroniche e al trattamento dei dati in ambito di prevenzione, investigazione e repressione dei reati

Giorgia Bincoletto

7.1 Le ulteriori regole a protezione dei dati personali nel diritto europeo

Il GDPR stabilisce le regole generali in materia di protezione di dati personali. Tuttavia, il quadro europeo a loro tutela non si esaurisce a questo regolamento. Sono, infatti, previste norme speciali in settori chiave o con riferimento ad alcune particolari tipologie di trattamento, ossia:

– la Direttiva 2002/58/CE relativa alla protezione dei dati personali e della vita privata nel contesto delle comunicazioni elettroniche, a tutela delle informazioni raccolte dalle apparecchiature e dai servizi di comunicazione, quali dati sul traffico e sull'ubicazione dell'utente, e anche della riservatezza o «vita privata elettronica» garantita dall'art. 7 della Carta di Nizza;
– la Direttiva 2016/680, che è stata approvata nel pacchetto di misure per la protezione dei dati adottato nel 2016 assieme al GDPR, e che si applica ai trattamenti di dati personali effettuati dalle autorità competenti ai fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, così come per la salvaguardia contro le minacce alla sicurezza pubblica e per la prevenzione delle stesse;
– il Regolamento 2018/1725 che stabilisce le norme applicabili al trattamento dei dati personali da parte delle istituzioni, degli organi e degli

organismi dell'UE e che istituisce il Garante Europeo della protezione dei dati.

Mentre quest'ultima disciplina è in linea con quanto già descritto sul GDPR [vedi → Capitolo 3] – il Regolamento 1725 riporta, infatti, gran parte del suo testo – e riguarda la creazione di un'autorità europea di controllo i cui compiti verranno descritti nel Capitolo 10, le due Direttive richiedono specifici approfondimenti che verranno svolti nelle prossime sezioni.

7.2 La normativa europea in materia di comunicazioni elettroniche

La Direttiva 2002/58/CE, anche denominata direttiva *e-privacy*, disciplina il trattamento dei dati personali e protegge il diritto alla vita privata nel settore delle comunicazioni elettroniche. Questo settore normativo è attualmente oggetto di una proposta di regolamento della Commissione Europea (COM (2017)10) che intende uniformare le regole a livello europeo, allinearle agli standard di protezione del pacchetto di protezione dei dati del 2016, ossia del GDPR e della Direttiva 2016/680, considerando al contempo sia la strategia europea per il Mercato Unico Digitale, in cui le reti di telecomunicazione svolgono un ruolo rilevante, sia gli sviluppi tecnologici intercorsi negli ultimi anni [si pensi al c.d. *Internet of Things,* vedi → Capitolo 14].

A gennaio 2023, il procedimento legislativo ordinario risulta nella fase di discussione presso il Consiglio dell'Unione europea. Si dedicherà, pertanto, ampio spazio alle regole ancora applicative, fornendo al contempo alcuni riferimenti alla proposta di regolamento nella sua prima versione elaborata dalla Commissione nel 2017.

La Direttiva e le sue implementazioni nazionali derogano alle regole generali del GDPR secondo il principio di specialità. Tuttavia, secondo alcuni, questo rapporto di specialità non sarebbe più giustificato dallo stato attuale dell'evoluzione tecnologica, che vedrebbe i sistemi digitali fortemente interconnessi [Poddighe 2021a, 1422]. Una rete di comunicazione elettronica potrebbe difatti essere connessa ad altre soluzioni tecnologiche, il cui trattamento dati sarebbe soggetto al GDPR.

Al contempo, la speciale regolazione dell'ambito delle comunicazioni elettroniche risponde sia all'esigenza di tutelare i dati personali, a cui il GDPR è dedicato, sia di garantire il diritto al rispetto della vita privata e della segretezza della corrispondenza, anche in una dimensione digitale, previsto dall'art. 7 della Carta di Nizza e da alcune costituzioni degli Stati membri. Sul punto si possono segnalare, a titolo esemplificativo, l'art. 15 della Costituzione Italiana, l'art. 181 della Constitutión Española, l'art. 11 della Constitution du Grand Duche de Luxembourg o l'art. 12 della Constitution of the Republic of Lithuania, previsioni che inseriscono la tutela della riservatezza della corrispondenza a livello di diritto fondamentali del rispettivo ordinamento giuridico nazionale. I dati raccolti nel corso di una comunicazione elettronica possono rivelare abitudini di consumo, informazioni su orari di connessione, durata delle comunicazioni e qualità delle chiamate [Poddighe 2021b, 1433].

In aggiunta, i rischi di «malware», «phishing» o «spamming» e di ricezione di comunicazioni indesiderate sono tipici del contesto delle comunicazioni elettroniche e richiedono specifiche garanzie e misure a loro prevenzione, ulteriori rispetto a quelle previste per la generalità dei trattamenti di dati personali. L'etimologia della parola *spam* deriva dalla marca americana di carne in scatola *Spiced Pork And haM*. Nel 1972, la BBC trasmise una scenetta comica del gruppo Monty Python in cui due clienti chiedevano ad una cameriera cosa fosse possibile ordinare. La cameriera proponeva diversi piatti, ma tutti con la carne *spam*. Un gruppo di clienti vestiti da vichinghi intonava una canzone ripetendo insistentemente la parola *spam* fino ad impedire ai due clienti e alla cameriera di sentirsi («Spam, Spam, Spam, Spam… Lovely Spam! Wonderful Spam!»). Ciò probabilmente per sottolineare l'eccessiva produzione e consumazione di carne in scatola di quegli anni. La ripetizione insistente e martellante della parola *spam* nel video ha fatto sì che il fenomeno di invio massivo e non richiesto di comunicazioni promozionali nelle nuove caselle di posta elettronica degli anni Ottanta, privo di termine che lo identificasse, le fosse associato per analogia [Poddighe 2021c, 1480].

Lo spamming si riferisce pertanto al fenomeno di invio di messaggi di posta elettronica o di newsletter senza il consenso del destinatario e in modo indiscriminato, solitamente per scopi promozionali, pubblicitari, o di vendita diretta. In molti casi i mittenti dei messaggi sono indirizzi anonimi, privi di indicazione o non corrispondenti alla realtà e il destina-

tario riceve molte comunicazioni in un breve lasso di tempo. Il phishing, invece, è da considerarsi una tipologia di truffa che utilizza messaggi ingannevoli da indirizzi apparentemente reali, come quello di una banca o di una società di credito, per indurre il ricevente a cliccare su un link che rinvia ad una pagina in cui inserire dati personali, quali i dati di una carta, per sottrarli a fini illeciti. Il malware è un software dannoso, come un virus, un trojan o uno spyware, programmato per infettare un dispositivo, ed è molto spesso diffuso con messaggi di phishing o di altre forme di comunicazione elettronica[1].

L'ambito di operatività della Direttiva è limitato ai servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche (art. 3). Il trattamento di dati personali tramite reti private è pertanto soggetto alle norme generali del GDPR.

Il riferimento ad una «comunicazione» richiede poi che si tratti di una trasmissione bidirezionale tra soggetti determinati o determinabili. La Direttiva 2018/1972, che istituisce il Codice europeo delle comunicazioni elettroniche, definisce i servizi di comunicazione elettronica come:

> i servizi forniti di norma a pagamento su reti di comunicazioni elettroniche, che comprendono, con l'eccezione dei servizi che forniscono contenuti trasmessi utilizzando reti e servizi di comunicazione elettronica o che esercitano un controllo editoriale su tali contenuti, i tipi di servizi seguenti: a) «servizio di accesso a internet» quale definito all'articolo 2, secondo comma, punto 2), del regolamento (UE) 2015/2120; b) «servizio di comunicazione interpersonale»; c) servizi consistenti esclusivamente o prevalentemente nella trasmissione di segnali come i servizi di trasmissione utilizzati per la fornitura di servizi da macchina a macchina e per la diffusione circolare radiotelevisiva.

I servizi telefonici, di posta elettronica e di accesso ad Internet, come nel caso del Wi-Fi, rientrano tipicamente tra i servizi di comunicazione soggetti alla disciplina *e-privacy*. Oltre a questi servizi, un altro ambito in cui quest'ultima è applicativa è l'utilizzo di *cookie*, ossia

1 Per approfondimenti tecnici su *spamming*, *phishing* e *malware*, si v. la pagina della Polizia Postale in https://www.commissariatodips.it/index.html.

> file che il fornitore di un sito Internet installa nel computer dell'utente di tale sito e ai quali il fornitore può nuovamente accedere durante una nuova visita del sito da parte dell'utente, per facilitare la navigazione in Internet o transazioni oppure al fine di ottenere informazioni sul comportamento dell'utente,

come spiegato dalla Corte di Giustizia nella causa C-673/17, di cui presto si dirà.

Con riferimento agli obblighi previsti dalla Direttiva, i fornitori dei servizi di comunicazione elettronica devono assicurare che le reti abbiano un livello di sicurezza adeguato ai rischi (art. 4), impedendo l'accesso ai dati da parte di persone non autorizzate e adottando misure per prevenire la loro distruzione, perdita o danneggiamento.

La riservatezza delle comunicazioni non deve essere pregiudicata da forme di ascolto, captazione, memorizzazione, intercettazione o sorveglianza dei dati relativi al traffico, ossia di tutti i dati necessari per la trasmissione di una comunicazione o della sua fatturazione (art. 2, lett. b)). Gli Stati Membri hanno vietato queste tipologie di interferenze nella sfera giuridica dell'utente richiedendo per la loro operatività un suo preventivo consenso o una base legale che le autorizzi (art. 5). L'utilizzo di software spia e *web bug* richiede perciò il consenso legittimante dell'utente [Bonzagni 2019]. Ciò non pregiudica, tuttavia, la memorizzazione tecnica necessaria per l'operatività della comunicazione o per l'archiviazione di transazioni, di per sé legittimate anche senza il consenso dell'interessato.

Quando i dati del traffico non sono più necessari ai fini della trasmissione di una comunicazione, essi devono essere cancellati o anonimizzati, a meno che non siano indispensabili per finalità di fatturazione, di commercializzazione di altri servizi, o di gestione del traffico (art. 6).

Il fornitore del servizio di comunicazione deve consentire all'utente di impedire la presentazione dell'identificazione della linea chiamante, mediante una funzione semplice e accessibile gratuitamente (art. 8). Dovrebbe quindi essere possibile mascherare l'identificabilità della chiamata come fosse un «numero sconosciuto» o un «numero privato». Da un punto di vista tecnico si tratta del processo di mascheramento del *calling*

line identifier dell'utente chiamante, che impedisce anche la funzione di *call return*[2].

Oltre ai dati relativi al traffico della comunicazione, i fornitori non dovrebbero trattare dati relativi all'ubicazione dell'utente, come la posizione geografica del punto di rete al momento della comunicazione, a meno che tali dati non siano anonimizzati o che sia stato prestato un preventivo consenso al loro trattamento (art. 9). Questo consenso potrà essere ritirato in qualsiasi momento e anche in via temporanea per specifiche comunicazioni. In ogni caso, tale attività di trattamento deve essere limitata a quanto necessario per la fornitura del servizio di comunicazione, non può perciò perseguire altre finalità (ad es. tracciare congiuntamente gli spostamenti degli utenti iscritti in una data località).

In aggiunta, l'interessato dovrebbe essere preventivamente informato dell'inserimento dei suoi riferimenti in un elenco cartaceo o elettronico pubblico degli abbonati al servizio di comunicazione (art. 12).

L'art. 13 della Direttiva, infine, disciplina un particolare aspetto delle comunicazioni elettroniche che è stato necessario regolare per la sua diffusione e importanza da un punto di vista fattuale: il fenomeno delle comunicazioni indesiderate (*spamming*) o di marketing diretto.

Una pratica commerciale molto utilizzata, come anticipato, è l'invio di comunicazioni a fine promozionale attraverso sistemi di chiamata, di messaggistica o di posta elettronica, in modo automatizzato, ossia senza l'intervento di un operatore. Ai sensi di questa previsione normativa l'uso di sistemi automatizzati di chiamata senza intervento di un operatore per finalità di commercializzazione diretta, attraverso il fax o la posta elettronica dell'interessato, è consentito soltanto sulla base di un suo preliminare ed espresso consenso. Nel contesto di una vendita di un prodotto o un servizio in cui si trattino dati personali e il cui trattamento è soggetto alla generale disciplina a protezione dei dati, è possibile richiedere il consenso all'utilizzo dell'indirizzo di posta elettronica a fini di commercializzazione diretta di altri prodotti o servizi che si considerino analoghi, a condizione che l'interessato sia informato in modo chiaro e distinto di tale trattamento al momento della raccolta di tale indirizzo

2 In ambito italiano si v. ad es. le specifiche tecniche pubblicate dal Ministero dello Sviluppo Economico in https://atc.mise.gov.it/index.php/tecnologie-delle-comunicazioni/servizi/specifiche-tecniche.

e che sia fornita la possibilità di opporsi. La normativa nazionale deve necessariamente prevedere la base giuridica del consenso per le comunicazioni indesiderate a scopo di commercializzazione diretta. L'art. 13 vieta peraltro «la prassi di inviare messaggi di posta elettronica a scopi di commercializzazione diretta camuffando o celando l'identità del mittente da parte del quale la comunicazione è effettuata, o senza fornire un indirizzo valido cui il destinatario possa inviare una richiesta di cessazione di tali comunicazioni».

Alcune norme della Direttiva sono state oggetto di interpretazione da parte della Corte di Giustizia. Nel 2006 questa normativa veniva modificata dall'ulteriore Direttiva 2006/24/CE «riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione», c.d. «Data Retention Directive», che consentiva appunto la conservazione dei dati delle comunicazioni, come data, ora e durata, per un periodo da 6 mesi a 2 anni e per finalità di sicurezza nazionale, sicurezza e difesa pubblica e prevenzione, ricerca, accertamento di reati. L'art. 15 della Direttiva *e-privacy* lasciava quindi agli Stati Membri la possibilità di adottare misure restrittive nazionali per tali finalità, come per la prevenzione del terrorismo.

Nella famosa causa Digital Rights Ireland Ltd. (C-293/12), la Corte di Giustizia ha riunito più ricorsi pregiudiziali riguardanti l'interpretazione di misure nazionali relative al periodo di conservazione dei dati e della stessa Direttiva. Il tempo di conservazione e le modalità di accesso ai dati previste dalle leggi nazionali apparivano come ingiustificate interferenze con il diritto alla protezione alla vita privata e alla protezione dei dati personali. Con tale decisione la Corte ha invalidato la Direttiva 2006/24/CE perché essa non prevedeva precisi limiti, condizioni e garanzie per la possibile ingerenza nei diritti fondamentali causata dalle previsioni di *data retention*, suscettibili quindi di abuso da parte delle autorità pubbliche e di accesso illecito anche dai fornitori dei servizi.

Nella causa Tele2 Sverige AB (C-203/15) la medesima corte ha poi ritenuto compatibile con il diritto europeo una norma nazionale che consentiva, per finalità di lotta contro la criminalità, «una conservazione generalizzata e indifferenziata dell'insieme dei dati relativi al traffico e dei dati relativi all'ubicazione di tutti gli abbonati e utenti iscritti riguardante tutti i mezzi di comunicazione elettronica», ma tale norma, per essere

compatibile con l'art. 15 della Direttiva *e-privacy* e con il diritto europeo doveva limitare l'accesso ai dati alle finalità di lotta contro la criminalità grave e sottoporlo ad un controllo preventivo da parte di un giudice o di un'autorità amministrativa indipendente, conservando i dati all'interno dell'Unione.

Nella causa di rinvio pregiudiziale C-673/17, *Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV v. Planet49 GmbH*, la Corte di Giustizia ha interpretato gli articoli 2 e 5 della Direttiva per escludere che un consenso sia validamente espresso «quando l'archiviazione di informazioni o l'accesso a informazioni già archiviate nell'apparecchiatura terminale dell'utente di un sito Internet attraverso cookie sono autorizzati mediante una casella di spunta preselezionata che l'utente deve deselezionare al fine di negare il proprio consenso». In altre parole, la selezione automatica e preventiva di una casella dovrà sempre essere a favore dell'utente (minor raccolta di informazioni e minor tracciamento) e non a vantaggio del fornitore del servizio. È così necessario un consenso attivo dell'utente perché la preselezione è insufficiente a dimostrare la sua consapevolezza e volontà nell'accettare forme di tracciamento. Nella medesima pronuncia la Corte ha chiarito che tra le informazioni da comunicare sui *cookie* dovranno essere inserite il periodo di attività del tracciamento e la possibilità o meno per i terzi soggetti di avere accesso ai file salvati nei dispositivi dell'utente.

Le norme della Direttiva sono state implementate nel diritto nazionale degli Stati Membri.

In Francia, sono state trasposte con la Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique et 10 e la Loi n° 2004-669 du 9 juillet 2004 relative aux communications électroniques et aux services de communication audiovisuelle, che hanno anche previsto specifiche disposizioni nella Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

In seguito, ulteriori specificazioni sono state inserite nella Section 3 del Code des postes et des communications électroniques (Loi n° 2020-1508 du 3 déc. 2020), dedicata alla «protection de la vie privée des utilisateurs de réseaux et services de communications électroniques» (artt. L34-1-L34-6). L'art. L 34-5 richiede che il consenso per le comunicazioni a fini promozionali (art. 13 della Direttiva) sia l'espressione di una volontà

libera, specifica e informata con cui una persona accetta che i dati personali che la riguardano possano essere utilizzati per finalità di marketing diretto. A seguito del GDPR, l'Ordonnance n°2018-1125 du 12 décembre 2018 ha apportato delle modifiche alla Loi 78-17. Attualmente gli articoli di riferimento in questa legge sono i numeri 81, 82 e 83. La base giuridica per il trattamento è il «consentement» dell'interessato, a meno che non sia necessario trattare i dati per necessità tecnica o per fornire un servizio richiesto dall'utente (art. 82, trasposizione dell'art. 5 della Direttiva).

In caso di violazione dei dati personali, il fornitore del servizio di comunicazione deve notificare l'accaduto alla Commission Nationale de l'Informatique et des Libertés, l'autorità di controllo francese (art. 83). Nel 2020, questa autorità ha sanzionato Amazon Europe Core, stabilita in Lussemburgo, per 35 milioni di euro alla luce della violazione dell'art. 82 della Loi 78-17, per non aver correttamente informato, in maniera chiara e completa, e richiesto il consenso agli utenti per l'utilizzo di *cookie* sul sito www.amazon.fr (Délibération SAN-2020-013 du 7 décembre 2020)[3]. L'autorità si è considerata territorialmente competente perché la vicenda riguardava file scaricati su dispositivi di utenti residenti in Francia e richiedeva l'applicazione della disciplina *e-privacy*, che rimane ancora in gran parte nazionale.

Con riferimento proprio ai *cookie*, nel 2019 la CNIL ha adottato delle dettagliate linee guida, poi validate dal Conseil d'État con la Délibération n° 2020-092 du 17 septembre 2020 «portant adoption d'une recommandation proposant des modalités pratiques de mise en conformité en cas de recours aux cookies et autres traceurs»[4]. Nelle raccomandazioni si specifica che se il fornitore del servizio decidesse di adottare una «cookie wall» per le scelte dell'utente sui *cookies* da acconsentire (come si sta verificando di frequente), l'informazione fornita dovrebbe indicare chiaramente le conseguenze delle sue scelte e in particolare l'impossibilità di accesso al contenuto o al servizio in assenza di consenso.

---

3 Il testo della decisione è disponibile in https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000042635729.

4 Si v. il testo delle linee guida in https://www.cnil.fr/fr/cookies-et-autres-traceurs/regles/cookies/lignes-directrices-modificatives-et-recommandation.e della decisione del Conseil d'État in https://www.conseil-etat.fr/fr/arianeweb/CE/decision/2020-06-19/434684.

In Italia, il Titolo X del Codice Privacy, agli artt. 121-134, fornisce regole specifiche per i trattamenti di dati personali connessi alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazioni, comprese le reti che forniscono servizi di raccolta e identificazione. Queste norme sono state modificate dal d.lgs. 101/2018 di adeguamento nazionale al GDPR per allineare la terminologia e aggiornare i requisiti di sicurezza.

Si segnala, in particolare, quanto previsto dall'art. 122, che si applica ai *cookie* e agli altri strumenti di tracciamento:

> 1. L'archiviazione delle informazioni nell'apparecchio terminale di un contraente o di un utente o l'accesso a informazioni già archiviate sono consentiti unicamente a condizione che il contraente o l'utente abbia espresso il proprio consenso dopo essere stato informato con modalità semplificate. Ciò non vieta l'eventuale archiviazione tecnica o l'accesso alle informazioni già archiviate se finalizzati unicamente ad effettuare la trasmissione di una comunicazione su una rete di comunicazione elettronica, o nella misura strettamente necessaria al fornitore di un servizio della società dell'informazione esplicitamente richiesto dal contraente o dall'utente a erogare tale servizio. Ai fini della determinazione delle modalità semplificate di cui al primo periodo il Garante tiene anche conto delle proposte formulate dalle associazioni maggiormente rappresentative a livello nazionale dei consumatori e delle categorie economiche coinvolte, anche allo scopo di garantire l'utilizzo di metodologie che assicurino l'effettiva consapevolezza del contraente o dell'utente.
> 2. Ai fini dell'espressione del consenso di cui al comma 1, possono essere utilizzate specifiche configurazioni di programmi informatici o di dispositivi che siano di facile e chiara utilizzabilità per il contraente o l'utente.
> 2-bis. Salvo quanto previsto dal comma 1, è vietato l'uso di una rete di comunicazione elettronica per accedere a informazioni archiviate nell'apparecchio terminale di un contraente o di un utente, per archiviare informazioni o per monitorare le operazioni dell'utente.

Questa previsione subordina il trattamento di informazioni contenute nel terminale dell'utente o del contraente - visto che questi soggetti possono non coincidere - al loro consenso esplicito a seguito di informativa o alla necessità tecnica dell'uso, rendendo esplicito al co. 2-*bis* un divieto

generale di utilizzo della rete di comunicazione elettronica per accedere a quanto archiviato durante la trasmissione nel sistema dell'interessato [Poddighe 2021b]. Il consenso può essere richiesto con modalità semplificate e anche attraverso meccanismi informatici facilmente utilizzabili.

Si evidenzia che la presa visione della *cookie policy* e il consenso alla tipologia di *cookie* sono richiesti da ogni sito Internet al momento iniziale dell'accesso alla loro pagina. Ciò dovrebbe valere anche per le applicazioni che si collegano alla rete. Secondo l'interpretazione del Garante per la protezione dei dati personali l'art. 122 del Codice richiede che i *cookie* di profilazione di un utente utilizzati in un'applicazione che tratta dati personali sulla base del GDPR, nella specie «Tik Tok», devono essere soggetti al consenso esplicito dell'interessato, applicandosi per questo aspetto la normativa *e-privacy* perché vengono archiviate informazioni nei dispositivi degli utenti. Nel caso di specie il Garante ha ritenuto che

> l'attività di somministrazione di pubblicità commerciale «personalizzata», da parte di TikTok agli utenti maggiorenni, attraverso attività di profilazione dei loro comportamenti all'interno del social network, almeno nella misura in cui risulti basata, come espressamente riferito dalla società, sulle c.d. «informazioni raccolte automaticamente» e archiviate sul dispositivo degli utenti non possa basarsi giuridicamente sull'interesse legittimo ponendosi tale attività in contrasto con l'art. 5, par. 3 della Direttiva *e-privacy* e l'art. 122 del Codice[5].

Nel medesimo servizio di social network potrebbero quindi doversi applicare sia la Direttiva 2002/58 e le previsioni del Codice Privacy, che il GDPR per tutte le altre attività di trattamento che non riguardano comunicazioni elettroniche e archiviazioni di informazioni nel dispositivo dell'utente.

L'art. 130 del Codice Privacy è dedicato alle comunicazioni indesiderate e in adeguamento all'art. 13 della Direttiva prevede il preventivo consenso quale legittimazione del trattamento delle informazioni con sistemi automatizzati di chiamata o di comunicazione di chiamata senza operatore per l'invio di pubblicità, per vendita diretta, per il compimento di ricerche di mercato o di comunicazioni commerciali. Questa

5 Si v. il provvedimento del 7 luglio 2022 in https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9788429.

previsione normativa, inoltre, vieta l'uso di compositori telefonici per la ricerca automatica di numeri e così tutela l'utente abbonato ad un servizio dall'invasività della pubblicità che può arrivare da moltissime fonti [Poddighe 2021c, 1481].

Tuttavia, il trattamento di dati per finalità di invio di materiale pubblicitario, vendita diretta, compimento di ricerche di mercato o di comunicazione commerciale è consentito nei confronti degli utenti che non si sono iscritti al registro pubblico delle opposizioni (art. 130, co. 3-*bis*). È disponibile online, infatti, un registro che consente l'iscrizione in via telematica ad una lista di soggetti che si oppongono alla ricezione di chiamate tramite telefono e di posta pubblicitaria cartacea[6]. È lecito inviare comunicazioni di vendita diretta sull'indirizzo di posta elettronica fornito da un interessato per la vendita di un prodotto e un servizio, senza il suo preventivo consenso, se il servizio è analogo a quello oggetto di quanto venduto (art. 130, co.4). Al momento della vendita, comunque, il soggetto deve essere informato della possibilità di opporsi. Rimane, tuttavia, non definito cosa si intenda per «servizio analogo».

Nel 2021, il Garante Privacy ha pubblicato le «Linee guida cookie e altri strumenti di tracciamento»[7]. In questo documento i *cookie* vengono classificati secondo due macrocategorie:

– i *cookie tecnici*, utilizzati al solo fine di «effettuare la trasmissione di una comunicazione su una rete di comunicazione elettronica, o nella misura strettamente necessaria al fornitore di un servizio della società dell'informazione esplicitamente richiesto dal contraente o dall'utente a erogare tale servizio» (cfr. art. 122, co. 1 del Codice);
– i *cookie di profilazione*, utilizzati per ricondurre a soggetti determinati, identificati o identificabili, specifiche azioni o schemi comportamentali ricorrenti nell'uso delle funzionalità offerte (pattern) al fine del raggruppamento dei diversi profili all'interno di cluster omogenei di diversa ampiezza, in modo che sia possibile al titolare, tra l'altro, anche modulare la fornitura del servizio in modo sempre più personalizzato al di là di quanto strettamente necessario all'erogazione del servizio,

6 L'attuale indirizzo del registro è reperibile in https://www.registrodelleopposizioni.it/.

7 Si v. le linee guida in https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9677876.

nonché inviare messaggi pubblicitari mirati, cioè in linea con le preferenze manifestate dall'utente nell'ambito della navigazione in rete.

Per l'utilizzo dei *cookie* è in ogni caso richiesta la somministrazione di un'apposita informativa. I *cookie* tecnici o «essenziali» non richiedono un preventivo consenso, mentre tutti gli altri sì.

Il Garante ha fornito alcune indicazioni sulle modalità della sua raccolta che avviene frequentemente tramite la tecnica dello *scrolling*, ossia del semplice scorrimento verso il basso della pagina, o della *cookie wall*, ossia il meccanismo vincolante (cd. «take it or leave it») che obbliga l'utente, senza alternativa, ad acconsentire alla ricezione di strumenti di tracciamento, pena l'impossibilità di accedere alla pagina.

Come peraltro già indicato dall'EDPB nel Parere n. 5 del 2020[8], il mero scorrimento non equivale ad espressione del consenso, ma potrà essere utilizzato congiuntamente ad altri elementi che garantiscano l'espressione di una volontà consapevole da parte dell'utente. Sul meccanismo della *cookie wall*, invece, l'autorità nazionale ha specificato che si tratta di una modalità illecita, salvo venga consentito un alternativo accesso ad un servizio equivalente a quello della pagina in questione (par. 6.1). Il banner di richiesta del consenso limita la c.d. *user experience* del sito e può essere riproposto quando mutano significativamente le condizioni del trattamento, ove non sia possibile verificare l'avvenuta memorizzazione del tracciamento o se siano trascorsi sei mesi dalla prima raccolta (par. 6.2).

Il Garante ha altresì richiamato l'importanza dell'adozione dei principi di *data protection by design* e *by default* nella costruzione del meccanismo di acquisizione del consenso (par. 7). A ciò consegue che, *by design* e *by default*, nessuno strumento di tracciamento che non sia tecnico può essere utilizzato al primo accesso dell'utente ad una pagina, prima della visualizzazione del banner per il suo consenso. Chiudendo il banner senza prestare consensi, il sito dovrebbe utilizzare solo elementi essenziali.

Per quanto riguarda i cd. *cookies analytic*, ossia degli strumenti che misurano il numero di utenti del sito, la loro localizzazione e altre ca-

8 Si v. le linee guida dell'EDPB sul consenso in https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_it.

ratteristiche della loro navigazione, e che sono spesso forniti da «terze parti», quali terzi soggetti che prestano questo specifico servizio, come Google con la funzione Google Analytics, l'autorità italiana ha richiesto la minimizzazione del loro utilizzo come *cookie* tecnici e ha indicato vari e dettagliati requisiti operativi (par. 7.2). In ogni caso, l'informativa dovrà distinguere tra diverse categorie di *cookie* (par. 8). Si segnala peraltro che sulla funzionalità di analisi del sito e Google Analytics il Garante è nuovamente intervenuto il 23 giugno 2022, affermando che un sito web che usa questo servizio viola la normativa a protezione dei dati personali perché comporta un trasferimento di informazioni negli Stati Uniti, senza adeguate garanzie di protezione[9] [sui meccanismi di trasferimento e il particolare caso statunitense, vedi → Capitolo 6].

La Direttiva ha tracciato le linee chiave per la regolamentazione del contesto delle comunicazioni elettroniche, ma la disciplina prevista dagli Stati membri non è uniforme e risulta complesso mappare gli obblighi esistenti per i fornitori dei servizi che operano in più paesi. Il Regolamento *e-privacy* si applicherà, invece direttamente negli ordinamenti nazionali, uniformando il livello di protezione nel settore delle comunicazioni elettroniche, come già avvenuto per la generalità degli altri trattamenti con il GDPR.

Considerando l'attuale proposta, il regolamento disciplinerà «il trattamento di dati delle comunicazioni elettroniche effettuato in relazione alla fornitura e alla fruizione dei servizi di comunicazione elettronica e alle informazioni connesse alle apparecchiature terminali degli utenti finali» (art. 2, par. 1), ampliando lo scopo materiale della normativa ai servizi offerti a utenti finali stabiliti nell'UE (art. 3, par. 1, lett. a)) e anche ai metadati trattati nel servizio.

Il concetto di «dati delle comunicazioni elettroniche» comprenderà sia il contenuto delle comunicazioni (testo, voce, immagini e suono) sia i metadati, ossia le informazioni necessarie per trasmettere, distribuire o scambiare il contenuto, in cui si ricomprendono i dati di localizzazione, la data, l'ora, la durata e il tipo di comunicazione (art. 4, par. 3, lett. a), b) e c)).

9 Si v. uno dei provvedimenti adottati in questo senso in https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9782890.

L'art. 5 dell'attuale versione del regolamento vieterà tutte le interferenze non giustificate sui dati delle comunicazioni elettroniche, tra cui l'ascolto, la registrazione, la conservazione, il monitoraggio, la scansione o altri tipi di intercettazione, e la sorveglianza di dati e metadati, proteggendone la riservatezza.

Il trattamento dei dati da parte dei fornitori di reti e servizi di comunicazione elettronica sarà legittimato quando necessario per la trasmissione della comunicazione, durante la sua durata, e in seguito per il mantenimento o il ripristino della sicurezza delle reti e del servizio (art. 6, par. 1). I metadati, invece, potranno essere trattati dai fornitori dei servizi se necessario per garantire la loro qualità, per la fatturazione o il calcolo del pagamento di interconnessione, il rilevamento o arresto di un uso fraudolento o abusivo del servizio o sulla base del consenso dell'utente qualora riferito ad uno specifico fine (art. 6, par. 2). Gli stessi fornitori potranno trattare il contenuto delle comunicazioni solo sulla base del consenso dell'utente finale per l'erogazione di uno specifico servizio, oppure per una pluralità di fini se tutti gli utenti coinvolti hanno prestato il consenso ed è stata consultata l'autorità di controllo (art. 6, par. 3). La proposta, perciò, differenzia le basi giuridiche a seconda dell'oggetto del trattamento (dati, metadati o loro contenuto). Quando non più necessarie, le informazioni dovranno essere cancellate o anonimizzate (art. 6).

Con riferimento alle informazioni conservate nell'apparecchiatura dell'utente, come nel caso dei *cookie* o di altre tecnologie di tracciamento, è stabilito un generale divieto al loro utilizzo a meno che ciò non sia necessario per consentire la trasmissione della comunicazione, se sia autorizzato dal consenso dell'utente finale, se sia necessario per l'erogazione di un servizio richiesto dallo stesso utente o per «misurare il pubblico del web» (art. 8, par. 1). Verranno altresì posti dei limiti alla raccolta delle informazioni emesse dall'apparecchiatura terminale per consentirne la connessione a un altro dispositivo o a un'apparecchiatura di rete (art. 8, par. 2). Una particolare novità è che le comunicazioni all'utente potranno essere fornite in combinazione a icone standardizzate per dare un quadro d'insieme «in modo facilmente visibile, intelligibile e chiaramente leggibile» (art. 8, par. 3). Ciò è simile a quanto indicato all'art. 12, par. 7, del GDPR per l'informativa privacy da rilasciare ai sensi degli artt. 13 e 14.

Inoltre, il concetto di consenso verrà parificato a quello del GDPR (art. 9), verranno ampliati i diritti relativi alla presentazione e restrizione dell'identificazione della linea chiamante e collegata (art. 12), fissando al contempo delle restrizioni (art. 13) e la possibilità di bloccare le chiamate (art. 14). Eventuali elenchi pubblici di utenze dovranno raccogliere il consenso degli interessati per essere creati (art. 15).

Il lungo articolo 16 della proposta è dedicato alla nuova disciplina delle comunicazioni indesiderate. Tali tipologie di comunicazioni potranno essere inviate ad utenti finali che hanno espresso il consenso o a utenti che hanno fornito le coordinate di posta elettronica nel contesto di una vendita di un prodotto o di un servizio a cui si applica il GDPR e a cui si intende vendere un prodotto o servizio analogo, sempreché venga «offerta in modo chiaro e distinto la possibilità di opporsi gratuitamente e agevolmente a tale uso». Questo diritto di obiezione è applicabile al momento della raccolta del dato e in ogni occasione di invio di un messaggio. Durante la comunicazione di commercializzazione diretta l'operatore dovrà presentare l'identità della linea o un codice o prefisso specifico che chiarisca l'origine della chiamata a fini commerciali.

Le autorità di controllo previste dal GDPR [vedi → Capitolo 10] saranno responsabili di monitorare l'applicazione del Regolamento *e-privacy* (art. 18) e il sistema di responsabilità, diritto al risarcimento e sanzioni amministrative sarà allineato a quello del regolamento generale con l'ammontare definito dall'art. 23 della proposta [vedi → Capitolo 11].

Sulla proposta sono stati rilasciati pareri dell'EDPS, del Consiglio Europeo e dell'EDPB, che hanno indicato varie possibili modifiche all'attuale impianto, pur ritenendosi favorevoli a quanto elaborato dalla Commissione [Bonzagni 2019].

7.3 La normativa in materia di trattamenti per finalità di prevenzione, investigazione e repressione di reati

I trattamenti di dati personali per fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali rientrano nell'ambito di applicazione della Direttiva 2016/680 - *Law Enforcement Directive*. La disciplina europea ha abrogato la decisione quadro 2008/977/GAI in ambito di cooperazione giudiziaria e di polizia in mate-

ria penale e non si applica alle attività di trattamento che l'UE esercita in questo settore per sua competenza ai sensi dell'art. 16, par. 2, del TFUE.

La scelta dello strumento di armonizzazione e non uniformazione è stata criticata dalle autorità garanti europee, ma è dovuta al rispetto delle peculiarità che ciascun ordinamento nazionale assume nella materia penale [Resta F. 2021, 1200].

La Direttiva, come precedentemente illustrato per il contesto *e-privacy*, ha natura di *lex specialis* rispetto al GDPR.

Le regole in materia di trattamenti di dati in ambito penale a fini anticrimine e di sicurezza mirano a bilanciare le esigenze investigative e di cooperazione giudiziaria con la salvaguardia del diritto fondamentale alla protezione dei dati [Bomprezzi 2019]. Il fine è contribuire alla realizzazione di uno spazio di libertà, sicurezza e giustizia (Cons. 2 della Dir. 2016/680) e di adeguare la precedente normativa ai cambiamenti tecnologici intervenuti nel settore penale e di polizia (Cons. 3).

L'ambito di applicazione materiale della Direttiva è limitato ai trattamenti di dati effettuati dalle autorità pubbliche competenti a svolgere le specifiche e tipiche finalità di:

– prevenzione di reati;
– indagine di reati;
– accertamento di reati;
– perseguimento di reati;
– esecuzione di sanzioni penali, incluse la salvaguardia e la prevenzione di minacce alla sicurezza pubblica.

Queste autorità, quali le forze di polizia, ricoprono il ruolo di titolari del trattamento e devono adeguarsi ai principi generali di trattamento già definiti dal GDPR (art. 4, che riprende i principi dell'art. 5 GDPR). Una volta raccolti per una delle sopra indicate finalità, i dati personali non possono essere utilizzati per altro scopo se non in presenza di una base legale definita dal diritto europeo o nazionale.

Nel trasporre la Direttiva nel diritto interno gli Stati membri hanno dovuto definire un termine per la conservazione dei dati (art. 5) e distinguere i requisiti a seconda che il trattamento riguardi (art. 6):

> a) le persone per le quali vi sono fondati motivi di ritenere che abbiano commesso o stiano per commettere un reato;

b) le persone condannate per un reato;
c) le vittime di reato o le persone che alcuni fatti autorizzano a considerare potenziali vittime di reato, e
d) altre parti rispetto a un reato, quali le persone che potrebbero essere chiamate a testimoniare nel corso di indagini su reati o di procedimenti penali conseguenti, le persone che possono fornire informazioni su reati o le persone in contatto o collegate alle persone di cui alle lettere a) e b).

Tale necessità non riguarda solo le categorie degli interessati, ma anche la tipologia di dati personali. Gli Stati Membri, infatti, hanno dovuto disporre che i dati fondati sui fatti siano differenziati da quelli sulle valutazioni personali (art. 7).

Il trattamento di tutti questi dati sarà lecito soltanto per necessità di esecuzione di un compito per il quale l'autorità pubblica è competente (art. 8) o in presenza di particolari condizioni legali (art. 9). Qualora i dati rientrino nella definizione di particolare categoria di dato del GDPR, come i dati relativi alla salute o all'origine razziale o etnica, il trattamento sarà lecito se autorizzato da una disposizione legislativa europea o nazionale, se necessario per salvaguardare un interesse vitale dell'interessato o di un'altra persona fisica o se l'attività riguarda dati resi manifestamente pubblici dallo stesso interessato (art. 10).

L'utilizzo di processi decisionali automatizzati per il trattamento dei dati, come nel caso di strumenti di profilazione, che comportino effetti giuridici negativi per l'interessato o incidano significativamente nella sua sfera personale è vietato, a meno che non sia autorizzato dal diritto statale, il quale prevederà garanzie e il diritto ad un intervento umano (art. 11).

Con riferimento ai diritti degli interessati, la Direttiva prevede:

– il diritto ad essere informati sulle modalità e caratteristiche del trattamento (artt. 12 e 13);
– il diritto di accesso (art. 14), che potrà essere limitato a livello legislativo dagli Stati membri per esigenze di non compromissione delle finalità di prevenzione, indagine, accertamento e perseguimento di reati o per l'esecuzione di sanzioni penali, così come per proteggere la sicurezza pubblica e nazionale o altri diritti e libertà di diversi interessati (art. 15);

– i diritti di rettifica e cancellazione dei dati e di limitazione del trattamento, che possono però essere limitati per l'esecuzione delle medesime finalità (art. 16).

Tra gli obblighi delle autorità pubbliche come titolari del trattamento rientrano l'implementazione di misure protettive del diritto alla protezione dei dati fin dalla progettazione e per impostazione predefinita (art. 20), l'adozione di un registro delle attività di trattamento (art. 24) e di una valutazione di impatto (DPIA) (art. 27) e l'implementazione di misure di sicurezza (art. 29).

In caso di ricorso a servizi esterni, quali società che utilizzano tecnologie di intercettazione, dovrà essere sottoscritta la nomina a responsabile del trattamento e così applicate le garanzie di adeguatezza e protezione (art. 22). È possibile affermare, in generale, che i requisiti sono simili a quelli previsti nel GDPR.

La Direttiva è stata implementata nel diritto nazionale degli Stati membri. Commentando la normativa alcuni studiosi hanno specificato che la trasposizione nazionale ha creato un quadro molto frammentato di protezione [Sajfert, Quintel 2017].

In Italia, la Direttiva è stata attuata dal d.lgs. 18 maggio 2018, n. 51, entrato in vigore il giorno 8 giugno 2018, che può considerarsi un *corpus* normativo autonomo rispetto al Codice Privacy, disciplinante i trattamenti svolti dall'autorità di pubblica sicurezza per le finalità tassative di prevenzione, accertamento, repressione dei reati o tutela dell'ordine e della sicurezza pubblici [Resta 2021]. Si segnala infatti che l'art. 2 *octies* del Codice Privacy in materia di trattamento di dati relativi a condanne penali e reati pur riferendosi a dati giudiziari non si applica nel caso di attività effettuate da autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, ma riguarda l'implementazione degli artt. 10 e 23 del GDPR [Errani 2021 e Errani 2019].

In Francia, invece, la legge di adeguamento alla Direttiva ha direttamente modificato la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, inserendo il Titre III che agli artt. 87-114 prevede la normativa nazionale che le autorità pubbliche devono rispettare.

L'uso di tecnologie digitali nel contesto di polizia e sicurezza è molto frequente. Si pensi all'installazione di videocamere o di sistemi di intercettazione. Nel 2022, l'EDPB ha pubblicato le Guidelines 05/2022 «on the use of facial recognition technology in the area of law enforcement»[10]. Le tecnologie di riconoscimento facciale sono, infatti, sistemi particolarmente invasivi del diritto alla protezione dei dati e alla protezione della vita privata perché trattano dati biometrici e, se conservanti in grande quantità (Big Data), possono creare fenomeni di massima sorveglianza in nome della prevenzione dei rischi per la sicurezza pubblica [sul tema vedi → Capitolo 18]. Queste tecnologie sono utilizzate per verificare l'identità di un soggetto, rispetto a quanto dichiarato, o per identificarlo in un gruppo, in un database o in una specifica area geografica, e si basano su sistemi probabilistici (v. sez. 2 delle Linee Guida). L'autorità europea ha fornito indicazioni giuridiche e tecniche su tali strumenti e anche esempi pratici di scenari di trattamento (v. Annex I, II, III).

7.4 Casi 7-1, 7-2

Caso 7-1

L'applicazione Alfa, sviluppata dalla società Beta stabilita in Francia, offre un servizio di social network e dating per interagire e incontrare nuove persone con gli stessi gusti cinematografici e letterari. Attraverso l'applicazione Beta raccoglie vari dati degli utenti, inclusi indirizzi di posta elettronica e numeri di telefono, per fornire suggerimenti sulle nuove uscite editoriali. Tra le sue attività è inclusa infatti la promozione di prodotti che possono essere noleggiati o comprati presso terze società. Beta fornisce un'informativa privacy allo scaricamento dell'applicazione e richiede un unico e preventivo consenso per il trattamento dei dati.
In cosa consistono le attività di trattamento dei dati personali?
Quale normativa si applica a queste attività?
Qual è la base giuridica applicabile e la finalità del trattamento di ciascuna attività?
Quali sono i principali obblighi di Beta?

10 Si v. il documento in https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-052022-use-facial-recognition_it.

Caso 7-2

L'agente italiano di polizia Tizio sta svolgendo un'indagine sulla sparizione di alcuni minori, quando decide di usare un software per confrontare i volti di minori scomparsi con le immagine memorizzate dal sistema di sorveglianza (CCTV) della città Gamma, verificandone gli spostamenti e cercando eventuali sospettati in loro presenza.
In cosa consistono le attività di trattamento dei dati personali?
Quale normativa si applica a queste attività?
Qual è la base giuridica applicabile e la finalità del trattamento di ciascuna attività?
Quali sono i principali obblighi del titolare del trattamento?

CAPITOLO 8.
Il diritto all'oblio: tra diritto ad essere dimenticati e diritto alla cancellazione dei dati

Giorgia Bincoletto

8.1 Le dimensioni del diritto all'oblio

Nell'ordinamento europeo ed italiano l'espressione «diritto all'oblio» si può riferire ad alcune particolari accezioni del diritto alla riservatezza e del diritto alla protezione dei dati personali, ossia al:

- «diritto ad essere dimenticati», quale dimensione del diritto alla riservatezza riconosciuta a livello giurisprudenziale per non lasciare un soggetto indeterminatamente esposto a possibili danni alla sua personalità in caso di reiterata divulgazione di una notizia o di informazioni riferite al suo passato non più di interesse pubblico preminente;
- «diritto alla deindicizzazione», quale dimensione del diritto alla protezione dei dati personali, elaborata dalla Corte di Giustizia dell'Unione Europea per la prima volta nel famoso caso *Google Spain* nel 2014 e riferita alla possibilità di deindicizzare i risultati prodotti dall'algoritmo di un motore di ricerca;
- il «diritto alla cancellazione», quale dimensione del diritto alla protezione dei dati personali, positivizzato dal GDPR all'art. 17 per poter cancellare i dati personali il cui trattamento non trova più un legittimo fondamento.

Questo capitolo si concentrerà su ciascun aspetto, assumendo per il primo la prospettiva dell'ordinamento italiano e per gli altri due quella

del diritto europeo a protezione dei dati personali, effettuando al contempo brevi raffronti con il sistema statunitense.

8.2 Il diritto ad essere dimenticati

Come anticipato, il «diritto ad essere dimenticati» o diritto all'oblio è considerato uno dei possibili aspetti del diritto alla protezione della vita privata degli individui e può essere definito come il diritto a non veder ripubblicate e diffuse notizie legittimamente pubblicate in passato [Caso 2021, 200].

La formula «diritto all'oblio» è stata elaborata dalla giurisprudenza francese («droit a l'oubli») negli anni Sessanta per tutelare il singolo dalla nuova divulgazione di vicende in passato di dominio pubblico (si v. ad es., la sentenza TGI seine, 4 oct. 1965, JCP 1966 II, 14482, obs. Lyon-Caen). La tutela veniva ricondotta direttamente alla protezione della vita privata prevista dall'art. 9 del Code Civil.

In Italia, il diritto ad essere dimenticati trova fondamento nell'art. 2 della Cost., quale aspetto del generale diritto della personalità, e deve essere posto in bilanciamento con il diritto di cronaca tutelato dall'art. 21 della Carta. L'interesse del singolo al riserbo può infatti essere bilanciato con l'interesse della collettività alla conoscenza delle notizie, quale declinazione della libertà di manifestazione del pensiero e di informazione.

Seppur il diritto all'oblio sia una specificazione del diritto alla riservatezza, esso assume peculiarità differenti. Mentre il diritto alla riservatezza è volto ad ostacolare la diffusione e pubblicazione all'esterno di notizie, situazioni, vicende personali e familiari che non hanno per i terzi un interesse socialmente apprezzabile, il diritto ad essere dimenticati aspira ad evitare la ripubblicazione di fatti in passato diffusi sulla base di un tale interesse, ma non più presente o non più preponderante rispetto alla protezione del riserbo, dell'onore e della reputazione del singolo.

Dunque la riservatezza protegge l'aspirazione alla non rappresentazione all'esterno di sé dall'origine delle vicende, mentre l'oblio aspira all'eliminazione di una passata rappresentazione oggi riprodotta e ingiustamente lesiva della personalità dell'individuo. In questo senso, il diritto all'oblio è connesso anche al diritto all'identità personale, di elaborazio-

ne giurisprudenziale, che tutela l'individuo ad essere rappresentato secondo la sua vera identità, ossia a non vedere alterato il suo patrimonio intellettuale, ideologico, etico, professionale presente nel suo tessuto sociale di riferimento (Cass. 22 giugno 1985, n. 3769, caso Veronesi).

Per il diritto ad essere dimenticati gioca un ruolo fondamentale il decorso del tempo. Trascorso un certo periodo, l'interesse del pubblico alla conoscenza dei fatti del passato viene meno. Perciò, se in un primo momento la riservatezza, la protezione dell'onore e della reputazione potevano cedere nel bilanciamento con il diritto di cronaca e all'esigenza di divulgazione di un'informazione, con il passare del tempo questi diritti tenderanno a prevalere.

Come anticipato [vedi → Capitolo 2], secondo la Corte di Cassazione la divulgazione di notizie lesive del diritto alla riservatezza deve considerarsi lecita espressione del diritto di cronaca, non comportando responsabilità civile, quando ricorrano le tre condizioni di i) verità oggettiva dei fatti esposti, ii) interesse pubblico alla conoscenza (c.d. pertinenza), e iii) correttezza formale della forma espositiva (c.d. continenza) [Pardolesi 1984]. Il giornalista dovrebbe quindi controllare l'attendibilità della fonte e rispettare la verità della vicenda in modo obiettivo. La valutazione di meritevolezza della pretesa di riserbo del soggetto è stata ancorata a questi criteri fin dal Decalogo del Giornalista del 1984 (Cass. 18 ottobre 1984, n. 5259).

L'accezione del diritto all'oblio come diritto ad essere dimenticati è stata riconosciuta per la prima volta dalla giurisprudenza italiana in un caso del 1998 riguardante la pubblicazione di una notizia relativa all'incriminazione di un soggetto, avvenuta sei anni prima, e archiviata con l'esclusione di tale soggetto dai fatti di reato contestati, ma, ciò nonostante, resa nota dalla stampa molti anni dopo (Cass. 9 aprile 1998, n. 3679). In particolare, nel 1990 il settimanale «Avvenimenti» pubblicò un articolo dal titolo «Duecento giorni a Palermo: perché la mafia ha ucciso» inserendo Mario Rendo tra gli episodi, malgrado l'avvenuta archiviazione delle vicende a suo carico, che comunque erano state oggetto di stampa in passato, prima della sua esclusione di responsabilità. Rendo lamentò quindi una violazione del suo diritto alla riservatezza, chiedendo il risarcimento del danno subito. Nel 1998 la Corte di Cassazione ha così aggiunto una nuova condizione ai criteri per il bilanciamento tra il diritto di cronaca e l'invasione nella sfera personale del singolo: l'attualità della

notizia. La divulgazione dopo un consistente lasso di tempo di una notizia in passato legittimamente pubblicata non è lecita se non coperta da un attuale interesse pubblico preponderante. Da tale rilievo la Corte ha riconosciuto il diritto all'oblio quale legittimo interesse a non restare indeterminatamente esposti ai danni ulteriori che una reiterata pubblicazione di una notizia legittimamente divulgata in passato arreca all'onore e alla reputazione, a meno che non vi siano eventi sopravvenuti che la rendano attuale e così di interesse pubblico per la collettività.

A partire da questa sentenza la giurisprudenza italiana ha più volte deciso su questioni riguardanti il bilanciamento tra interesse alla riservatezza, all'onore e alla reputazione nella dimensione del diritto all'oblio, e il diritto di cronaca, critica e satira, quali declinazioni della libertà di manifestare liberamente il pensiero e dell'interesse della collettività all'informazione. Il limite temporale che determina l'insorgenza del diritto ad essere dimenticati non è fisso e dovrà essere determinato dal giudice caso per caso, così come per la sussistenza dell'interesse pubblico attuale alla conoscenza delle vicende.

La Corte di Cassazione con la sentenza 5 aprile 2012, n. 5525 ha affrontato la questione della pubblicazione di un articolo del passato nell'archivio web di un giornale, che inevitabilmente si intreccia con la normativa a protezione dei dati personali. Al di là di tale aspetto, la corte ha chiarito che un fatto di cronaca può assumere rilevanza quale fatto storico e che ciò può giustificare la conservazione della notizia in un archivio, anche diverso da quello originale e persino in versione digitale. La pretesa del singolo, perciò, non potrebbe trovare soddisfazione se la vicenda personale o familiare è di interesse storico, che può o dovrebbe non essere dimenticato. I fatti riguardavano la pubblicazione di una vicenda giudiziaria riguardante un politico, prima arrestato e poi dopo anni assolto, all'interno dell'archivio online del Corriere della Sera. Secondo la Corte, la vicenda può essere legittimamente conservata e resa accessibile al pubblico tramite un archivio storico, ma dovrà essere contestualizzata, integrata e aggiornata per tutelare la personalità del soggetto coinvolto ed evitare illegittime ingerenze nella sua vita privata attuale. Ciò crea inevitabilmente un obbligo deontologico gravoso in capo al giornalista e all'editore, che consiste nell'impegno costante e complesso di aggiornamento delle notizie. In aggiunta, questa pronuncia ha riconosciuto il diritto a richiedere l'integrazione di una notizia affinché sia rappresenta-

tiva dell'identità e della corretta e completa rappresentazione dell'individuo [Ratti 2019]. Questa dimensione del diritto all'oblio è particolarmente rilevante nel contesto digitale.

Nel 2019 le Sezioni Unite della Corte di Cassazione hanno stabilito che dopo un lunghissimo lasso di tempo la ripubblicazione di una notizia può rispondere non tanto all'esercizio del diritto di cronaca, quanto a quello di rievocazione storica (Cass., sez. un., 22 luglio 2019, n. 19681). La vicenda riguardava la divulgazione di un articolo riguardante diciannove omicidi avvenuti nel passato e sui quali l'opinione pubblica locale si era a lungo dedicata. Una di queste notizie si riferiva a un individuo che aveva ucciso la moglie ventisette anni prima, che aveva scontato la pena e si era reinserito nella società in una diversa città e con un nuovo lavoro. Il soggetto, a seguito della ripubblicazione della vicenda in una rubrica di cronaca nera, lamentò una violazione del suo diritto all'oblio, e l'insorgenza di un grave disagio psicologico che la pubblicazione della notizia aveva arrecato. La Cassazione ha chiarito che il trascorrere del tempo impone l'aggiornamento della notizia, che altrimenti risulterebbe «non vera» e che il bilanciamento tra l'interesse del singolo ad essere dimenticato e del pubblico alla memoria di fatti a suo tempo legittimamente divulgati, presuppone un complesso giudizio nel quale assumono rilievo:
– la notorietà dell'interessato;
– il suo coinvolgimento nella vita pubblica;
– il contributo ad un dibattito di interesse generale della notizia;
– l'oggetto della notizia;
– la forma della pubblicazione;
– il tempo trascorso dal momento in cui i fatti si sono effettivamente verificati alla nuova divulgazione.

Il problema giuridico di questa decisione riguarda un caso connesso alla diffusione di una notizia a mezzo giornalistico molti anni dopo la prima pubblicazione e, quindi, sembrerebbe relativo ad un tradizionale bilanciamento tra il diritto di cronaca e il diritto all'oblio, inteso come diritto ad essere dimenticati. Le Sezioni Unite hanno chiarito, tuttavia, che quando un giornalista ripubblica dopo un lungo periodo di tempo una notizia sta esercitando il diritto alla rievocazione storica o storiografica dei fatti e non il diritto di cronaca.

La storia non è cronaca e non trova, perciò, applicazione la tutela costituzionale prevista dall'art. 21 della Costituzione. La ripubblicazione, se consiste in una rievocazione, deve avvenire in forma anonima perché non vi è un interesse pubblico alla conoscenza dell'identità dei soggetti legati alla vicenda, a meno che non vi siano fatti sopravvenuti che mutino tali presupposti. L'attore non era una persona nota e il suo percorso di reinserimento lo aveva riabilitato nella società. Il giudice ha dunque stabilito questo principio di diritto:

> In tema di rapporti tra il diritto alla riservatezza (nella sua particolare connotazione del c.d. diritto all'oblio) e il diritto alla rievocazione storica di fatti e vicende concernenti eventi del passato, il giudice di merito – ferma restando la libertà della scelta editoriale in ordine a tale rievocazione, che è espressione della libertà di stampa e di informazione protetta e garantita dall'art. 21 Cost. – ha il compito di valutare l'interesse pubblico, concreto ed attuale alla menzione degli elementi identificativi delle persone che di quei fatti e di quelle vicende furono protagonisti. Tale menzione deve ritenersi lecita solo nell'ipotesi in cui si riferisca a personaggi che destino nel momento presente l'interesse della collettività, sia per ragioni di notorietà che per il ruolo pubblico rivestito; in caso contrario, prevale il diritto degli interessati alla riservatezza rispetto ad avvenimenti del passato che li feriscano nella dignità e nell'onore e dei quali si sia ormai spenta la memoria collettiva (nella specie, un omicidio avvenuto ventisette anni prima, il cui responsabile aveva scontato la relativa pena detentiva, reinserendosi poi positivamente nel contesto sociale).

Il diritto all'oblio può, perciò essere posto in bilanciamento con il diritto alla rievocazione storica e l'esigenza di riserbo dell'individuo non può ostacolare la ripubblicazione della notizia se, al contempo, si garantisce l'anonimato di chi è coinvolto nella vicenda.

Riportare fatti del passato potrebbe rispondere ad un interesse a non dimenticare eventi storici di una data comunità, ma non implica necessariamente il ricordo di chi era coinvolto in tali situazioni. L'anonimizzazione dell'identità è in questo senso la prima soluzione da adottare. Al contempo, è opportuno segnalare che la determinazione del *quantum* temporale idoneo a generare la pretesa di oblio è un aspetto chiave; difatti, se le informazioni si riferissero a vicende giudiziarie lontane, ma

non ancora definite, si rischierebbe di «scivolare inopinatamente verso la prevalenza del segreto e dell'anonimato nel quadro dell'attività giurisdizionale», a cui alcune pronunce sembrano condurre [Palmieri 2022a].

Con l'ordinanza n. 25481 del 30 agosto 2022 la Corte di Cassazione ha nuovamente affrontato un caso relativo ad un archivio nel sito web di un'agenzia di stampa. Nonostante un articolo con una notizia del passato fosse stato rimosso, l'attore ha chiesto il riconoscimento dei danni subiti nel periodo intercorso tra il momento in cui era maturato il diritto all'oblio e la cancellazione, sul presupposto dell'obbligo di rimozione della notizia, anche prima dell'attivazione del soggetto. La Suprema Corte ha rinviato varie questioni alla pubblica udienza della prima sezione civile, che dovrà tra i vari aspetti chiarire se sia esigibile un obbligo generalizzato di controllo sull'attualità dell'informazione ricavabile da una consultazione online [Palmieri 2022b].

Nella tradizione giuridica europea ed italiana il diritto all'oblio è considerato uno dei diritti della personalità [Alpa, Resta 2019, 482]. Da una breve comparazione con l'ordinamento statunitense emerge che tale categoria dogmatica non è traducibile nei sistemi di common law, in cui la tutela della persona è azionata tramite i vari *torts*, quali rimedi azionabili in presenza di particolari condizioni. Secondo la dottrina giuridica statunitense, il diritto ad essere dimenticati non potrebbe trovare applicazione negli Stati Uniti poiché contrasterebbe con il Primo Emendamento che tutela la libertà di espressione quale uno dei più importanti principi costituzionali e non troverebbe supporto nell'attuale ordinamento giuridico [Solove 2021, 157 e Nicola, Pollicino 2020].

Un famoso caso deciso dalla United States Court of Appeals for the Second Circuit nel 1940 (*Sidis v. FR Pub. Corporation*, 113 F.2d 806 (2d Cir. 1940)) ha chiarito i confini del diritto alla privacy con riferimento all'interferenza sulla vita privata di un soggetto famoso in passato, ma successivamente ritiratosi dai riflettori. Nel 1910 William James Sidis era considerato un bambino prodigio per aver tenuto una conferenza ad illustri matematici sul tema dei corpi quadridimensionali, alla sola età di undici anni, e successivamente essersi laureato ad Harvard a sedici. A seguito della pressante attenzione mediatica, Sidis decise di ritirarsi a vita privata e condurre una vita normale. Nel 1937 il giornale The New Yorker pubblicò prima un breve schizzo fotografico e una vignetta ironica sull'ex bambino prodigio e poi un articolo dal titolo «April fool» descrivendo il

crollo psicologico causato dalla popolarità durante l'infanzia, raccontando l'attuale condizione di impiegato e riferendo vari dettagli sulla vita privata di Sidis, incluse le condizioni del suo alloggio. A seguito di tali pubblicazioni Sidis citò in giudizio la società proprietaria del giornale per violazione della sua privacy, ma i giudici rigettarono il suo ricorso, così esprimendosi:

> (…) we are not yet disposed to afford to all of the intimate details of private life an absolute immunity from the prying of the press. Everyone will agree that at some point the public interest in obtaining information becomes dominant over the individual's desire for privacy. Warren and Brandeis were willing to lift the veil somewhat in the case of public officers. We would go further, though we are not yet prepared to say how far. At least we would permit limited scrutiny of the «private» life of any person who has achieved, or has had thrust upon him, the questionable and indefinable status of a «public figure».

Sidis è stato considerato un tipico *paradox of American privacy* dal momento che la grandissima esposizione mediatica del caso ne ha impedito ogni dimenticanza [Barbas 2012]. In aggiunta, questo precedente è stato utilizzato per giustificare l'invasione nella vita privata dei singoli da parte del giornalismo investigativo negli anni Cinquanta e Sessanta, proprio sulla base di un interesse pubblico alla notizia, seppur limitato a lieve curiosità [Barbas 2012, 65].

Negli Stati Uniti un soggetto pubblico non avrebbe, dunque, diritto ad essere dimenticato poiché l'interesse a conoscere i dettagli della sua vita da parte del pubblico, e così della stampa, tutelato dal Primo Emendamento, prevarrebbe sull'aspirazione all'intimità del singolo. Soltanto in presenza dei presupposti di una diffamazione, si potrebbe tutelare la riservatezza a svantaggio dell'interesse pubblico e della libertà di parola [Antani 2015, 1187].

Il privacy *tort* che protegge da una *false light in public eye* potrebbe essere utilizzato in caso di nuova divulgazione di notizie lesive della reputazione dell'individuo. Non mancano del tutto, infatti, casi in cui le corti hanno eccezionalmente tutelato il singolo sulla base di tale *cause of action* o del *public disclosure tort* a protezione della sua privacy in caso di invasione da parte dei media [Solove 2021, 156 ss.].

Nell'era digitale le notizie sono sempre più riportate nelle versioni online dei quotidiani e ciò ha comportato l'emergere di una nuova forma di diritto all'oblio, il diritto alla deindicizzazione, che è stato prima riconosciuto a livello europeo ed è oggi pienamente applicato anche a livello nazionale (si v. Cass., ord. 19 maggio 2020, n. 9147 e ord. 30 agosto 2022, n. 25481).

8.3 Il diritto alla deindicizzazione

Con le modifiche tecnologiche dell'era digitale il diritto all'oblio ha assunto l'ulteriore e diversa accezione di domanda di deindicizzazione (*right to delisting*) di pagine web dai motori di ricerca. Come è stato riportato, questa dimensione riguarda il diritto a non essere trovato online o al c.d. ridimensionamento della visibilità telematica [Ricci 2019]. Si tratta, in particolare, di un aspetto del diritto alla protezione dei dati personali, i quali possono, in presenza di alcune circostanze, essere sottratti alla conoscenza generalizzata a cui i motori di ricerca consentono l'accesso. Questo diritto è nato sulla scia della previsione dell'art. 12 lett. b) della Direttiva 95/46/CE che consentiva la cancellazione dei dati personali in presenza di alcune circostanze.

Nel contesto digitale una volta che un'informazione è online, il soggetto alla quale essa si riferisce potrebbe essere indeterminatamente esposto alla memoria di tale vicenda perché grazie ad Internet i ricordi sono liberamente disponibili nel cyberspazio, probabilmente anche per sempre (o fino a che la pagina non viene archiviata). La reputazione del singolo potrebbe essere irrimediabilmente macchiata per un errore del passato. Ciò è esacerbato dall'utilizzo dei motori di ricerca che consentono, tramite l'elenco dei risultati, l'accesso ad un'indefinita quantità di informazioni previo inserimento di parole chiave.

La nuova declinazione del diritto all'oblio è stata elaborata per la prima volta dalla CGUE nel 2014 nel famoso caso di *Mario Costeja González v. Google Spain e Google Inc*. (C-131/12). Il signor Costeja aveva presentato un reclamo contro Google e il quotidiano «La Vanguardia» presso l'Agencia de Protección de Datos (AEPD), l'autorità di controllo spagnola, rilevando che nel momento in cui si digitava il suo nome nel motore di ricerca Google search comparivano alcuni link verso due pagine dell'archi-

vio online del quotidiano del 1988, sulle quali figurava un annuncio sulla vendita all'asta di immobili per un pignoramento legato alla riscossione coattiva di redditi previdenziali che lo aveva coinvolto. Il reclamante lamentava un danno morale (reputazionale) per la presenza di tali risultati e chiedeva, da un lato, la rimozione delle pagine da parte del quotidiano e, dall'altro, di eliminare o occultare i dati personali che comparivano tra i risultati della ricerca per impedire il riferimento ai link dell'archivio del giornale. Il reclamo veniva respinto dall'AEPD per la prima richiesta, accogliendo, invece, la seconda. Google ricorreva in giudizio contro la decisione e il giudice spagnolo (*Audiencia Nacional*) procedeva con un rinvio alla CGUE con varie questioni pregiudiziali. Tra queste, per quanto riguarda il diritto all'oblio, si chiedeva:

> Se si debba ritenere che i diritti di cancellazione e congelamento dei dati, disciplinati dall'articolo 12, lettera b), e il diritto di opposizione al loro trattamento, regolato dall'articolo 14, [primo comma,] lettera a), della direttiva [95/46], implichino che l'interessato può rivolgersi ai motori di ricerca per impedire l'indicizzazione delle informazioni riguardanti la sua persona pubblicate su pagine web di terzi, facendo valere la propria volontà che tali informazioni non siano conosciute dagli utenti di Internet, ove egli reputi che la loro divulgazione possa arrecargli pregiudizio o desideri che tali informazioni siano dimenticate, anche quando si tratti di informazioni pubblicate da terzi lecitamente.

La Corte ha risposto positivamente sulla base di alcune argomentazioni. Innanzitutto, le attività di Google sono considerabili un trattamento di dati che si svolge all'interno dell'UE per lo stabilimento presente in Spagna e a cui si applica la normativa europea in materia di protezione dei dati personali (questioni 1 e 2). I giudici hanno poi rilevato che un trattamento di dati personali può divenire con il tempo illecito perché i dati non sono più necessari in rapporto alla finalità per la quale siano stati raccolti e trattati. Pertanto, i risultati ottenuti da una ricerca compiuta con un nome possono riportare a pagine web non più pertinenti, inadeguate, non veritiere, o eccessive rispetto alle finalità. Il giudice di merito deve, in concreto, verificare se l'interessato abbia diritto a eliminare il collegamento tra sé e l'informazione riguardante la sua persona all'interno dell'elenco di risultati che appare a seguito di una ricerca effettuata

a partire dal suo nome nel motore di ricerca, e se subisca un pregiudizio per la presenza di collegamenti.

La possibilità di deindicizzazione, ossia di eliminazione del collegamento, sarebbe basata sugli articoli 7 e 8 della Carta di Nizza, che (quali diritti fondamentali) possono prevalere, afferma la Corte, «in linea di principio, non soltanto sull'interesse economico del gestore del motore di ricerca, ma anche sull'interesse» del pubblico «a trovare l'informazione suddetta in occasione di una ricerca concernente il nome di questa persona». Un limite rimarrebbe nei confronti di persone che ricoprono un ruolo pubblico, a cui è ricollegabile un interesse preponderante collettivo ad avere accesso alle informazioni sul loro conto.

Nel merito, la Corte ha sottolineato che se non sussiste un interesse pubblico preponderante alla visualizzazione nell'elenco di risultati di link verso pagine degli archivi online di un quotidiano su notizie di molti anni prima, il soggetto vanterà un diritto a che tali informazioni non siano più collegate al suo nome attraverso i risultati della ricerca, anche sulla base delle regole della Direttiva. Infatti, la questione pregiudiziale è stata conclusa dalla CGUE con questo principio di diritto:

> Gli articoli 12, lettera b), e 14, primo comma, lettera a), della direttiva 95/46 devono essere interpretati nel senso che, nel valutare i presupposti di applicazione di tali disposizioni, si deve verificare in particolare se l'interessato abbia diritto a che l'informazione in questione riguardante la sua persona non venga più, allo stato attuale, collegata al suo nome da un elenco di risultati che appare a seguito di una ricerca effettuata a partire dal suo nome, senza per questo che la constatazione di un diritto siffatto presupponga che l'inclusione dell'informazione in questione in tale elenco arrechi un pregiudizio a detto interessato. Dato che l'interessato può, sulla scorta dei suoi diritti fondamentali derivanti dagli articoli 7 e 8 della Carta, chiedere che l'informazione in questione non venga più messa a disposizione del grande pubblico in virtù della sua inclusione in un siffatto elenco di risultati, i diritti fondamentali di cui sopra prevalgono, in linea di principio, non soltanto sull'interesse economico del gestore del motore di ricerca, ma anche sull'interesse di tale pubblico ad accedere all'informazione suddetta in occasione di una ricerca concernente il nome di questa persona. Tuttavia, così non sarebbe qualora risultasse, per ragioni particolari, come il ruolo ricoperto da tale persona nella vita pubblica, che l'ingerenza nei suoi diritti fondamentali è giustificata dall'interesse prepon-

derante del pubblico suddetto ad avere accesso, in virtù dell'inclusione summenzionata, all'informazione di cui trattasi.

Anche in questa seconda accezione del diritto all'oblio giocano ruoli chiave l'attualità dell'interesse pubblico alla notizia, il trascorrere del tempo e il necessario bilanciamento tra interessi contrapposti. I commentatori hanno rilevato che «l'anelito all'oblio (sui dati) prevale (quasi) sempre e impone al gestore del motore di ricerca, se allertato, di intervenire per correggere il proprio sistema di indicizzazione», anche in assenza di vero pregiudizio, perché la valutazione è compiuta da tale soggetto e non dal giudice sulla base di una diretta richiesta dell'interessato [Palmieri, Pardolesi 2014, 318].

L'obbligo a carico del motore di ricerca (*duty to delisting*) che la sentenza Google Spain ha creato non è attributo al quotidiano, che potrà mantenere la notizia nell'archivio. Come hanno evidenziato Palmieri e Pardolesi, «la notizia è illecita nelle mani, meglio nei link di Google, inoppugnabile nell'archivio del giornale, per chi si dia la pena di recuperarla»; da ciò deriverebbe una «minaccia allargata di cancellazione per inattualità del dato censito, pur se legittimamente presente in rete» [Palmieri, Pardolesi 2014, 322].

Può peraltro essere sottolineato un evidente paradosso: colui che voleva essere dimenticato dal motore di ricerca sarà a lungo (se non per sempre) ricordato in letteratura come primo caso in materia di de-indicizzazione.

A seguito di questa importante pronuncia sono state promosse moltissime richieste di cancellazione dei collegamenti ai risultati di ricerca e Google, come altri motori, hanno creato appositi format online per inviarle. Ciò ha comportato l'inaccessibilità ad informazioni che non essendo più recuperabili attraverso un motore di ricerca risultavano praticamente oscurate, in assenza di chiari criteri di bilanciamento tra il diritto alla riservatezza e la libertà di informazione [Giovanella 2022].

Quattro ricorsi per mancata deindicizzazione hanno portato nel 2019 ad una nuova decisione della Corte di Giustizia in materia di esercizio dell'oblio e motori di ricerca in presenza di particolari categorie di dati personali (C-136/17, *GC e a. v. Commission nationale de l'informatique et des libertés*). Questi ricorsi erano stati proposti presso la CNIL, l'autorità di controllo francese, e riguardavano attività di trattamento di dati

politici, religiosi o relativi alla vita sessuale per i quali la Direttiva 95/46/CE disponeva il divieto di raccolta o dati giudiziari il cui trattamento doveva sottostare al controllo dell'autorità pubblica [Pardolesi 2017]. Ciò nonostante, i dati erano presenti nel web e ricollegabili agli interessati grazie ai risultati ottenuti su *Google search*. Gli interessati presentavano separatamente ricorso alla CNIL che tuttavia archiviava i procedimenti, non ritenendo Google il soggetto tenuto a cancellare i collegamenti. Venivano, quindi, proposti dei ricorsi giurisdizionali e il giudice francese riuniva le cause, procedendo al rinvio pregiudiziale alla Corte di Giustizia per determinare se i divieti e le restrizioni riguardanti il trattamento di categorie particolari di dati personali si applicassero anche ad un gestore di un motore di ricerca nell'ambito delle sue responsabilità, competenze e possibilità. Nel 2019 la Corte di Giustizia ha risposto affermativamente: il motore di ricerca, quale responsabile del trattamento, in occasione della richiesta di deindicizzazione deve verificare l'illiceità del trattamento di particolari categorie di dati, accogliendo l'istanza dell'interessato, a meno che non si applichi un'eccezione al divieto o alla restrizione che renda il trattamento legittimo. La decisione sulla richiesta di deindicizzazione dovrà tenere conto:

– della gravità dell'ingerenza nei diritti fondamentali della persona interessata al rispetto della vita privata e alla protezione dei dati personali;
– dei motivi di interesse pubblico rilevante alla presenza del link nel web;
– della necessità di proteggere la libertà di informazione degli utenti di Internet potenzialmente interessati ad avere accesso a tale pagina web.

Nello stesso anno, la Corte di Giustizia ha deciso su un ulteriore rinvio pregiudiziale di un giudice francese riguardante la portata territoriale dell'obbligo di deindicizzazione (C-507/17, *Google LLC v. Commission nationale de l'informatique et des libertés*). La vicenda ha origine da una richiesta di un interessato che a seguito della mancata deindicizzazione presentava ricorso alla CNIL. L'autorità condannava Google a rimuovere il link dall'elenco di risultati visualizzati in esito alle ricerche effettuate a partire dal nome dell'interessato, e ciò su tutte le estensioni del nome di dominio del suo motore di ricerca. Google contestava tale portata della cancellazione, intendendo limitarla all'estensione utilizzabile nel luogo

di residenza degli interessati. A seguito della mancata applicazione della diffida a cancellare, la CNIL condannava Google al pagamento di una sanzione di 100.000,00 euro. A questo punto, Google promuoveva ricorso al Conseil d'État, che rinviava alla Corte di Giustizia per decidere sulle seguenti questioni pregiudiziali:

> 1) Se il «diritto alla deindicizzazione», come sancito dalla [Corte] nella sentenza del 13 maggio 2014, [Google Spain e Google (C-131/12, EU:C:2014:317),] sulla base delle disposizioni di cui all'articolo 12, lettera b), e all'articolo 14, [primo comma,] lettera a), della direttiva [95/46], debba essere interpretato nel senso che il gestore di un motore di ricerca, nel dare seguito a una richiesta di deindicizzazione, è tenuto ad eseguire tale deindicizzazione su tutti i nomi di dominio del suo motore, affinché i link controversi non appaiano più – indipendentemente dal luogo a partire dal quale viene effettuata la ricerca avviata sul nome del richiedente – e ciò anche al di fuori dell'ambito di applicazione territoriale della direttiva [95/46].
> 2) In caso di risposta negativa alla prima questione, se il «diritto alla deindicizzazione», come sancito dalla [Corte] nella summenzionata sentenza, debba essere interpretato nel senso che il gestore di un motore di ricerca, nel dare seguito a una richiesta di deindicizzazione, sia tenuto solamente a sopprimere i link controversi che appaiono in esito a una ricerca effettuata a partire dal nome del richiedente sul nome di dominio corrispondente allo Stato in cui si ritiene sia stata effettuata la domanda o, più in generale, sui nomi di dominio del motore di ricerca corrispondenti alle estensioni nazionali di tale motore per tutti gli Stati membri (…).
> 3) Inoltre se, a complemento degli obblighi richiamati [nella seconda questione], il «diritto alla deindicizzazione», come sancito dalla [Corte] nella summenzionata sentenza, debba essere interpretato nel senso che il gestore di un motore di ricerca, quando accoglie una richiesta di deindicizzazione, è tenuto a sopprimere, con la cosiddetta tecnica del «blocco geografico», a partire da un indirizzo IP che si ritiene localizzato nello Stato di residenza del beneficiario del «diritto alla deindicizzazione», i risultati controversi delle ricerche effettuate a partire dal nome di quest'ultimo, o persino, più in generale, a partire da un indirizzo IP che si ritiene localizzato in uno degli Stati membri assoggettati alla direttiva [95/46], e ciò indipendentemente dal nome di dominio utilizzato dall'utente di Internet che effettua la ricerca.

Si tratta, perciò, della necessità di comprendere se l'obbligo di deindicizzazione sia limitato alla versione nazionale del motore di ricerca o a tutte le sue estensioni nel mondo, al di là della geolocalizzazione della richiesta dell'interessato. La Corte di Giustizia non si limita a considerare le regole della Direttiva, ma utilizza anche quelle del GDPR che è stato approvato nelle more del procedimento.

In primo luogo, la Corte richiama quanto stabilito nel caso Google Spain. Il gestore del motore di ricerca è considerabile titolare del trattamento dei dati personali a cui fornisce i collegamenti. In assenza di una base giuridica, anche il suo trattamento può risultare illecito. L'elenco di link in cui sono presenti dati sensibili potrebbe, infatti, considerarsi un trattamento non conforme alle regole dell'ordinamento giuridico. Solo la deindicizzazione da tutte le versioni del motore di ricerca sembrerebbe soddisfare l'aspirazione di oblio del singolo in un mondo globalizzato e all'interno di Internet. Da ciò deriverebbe, tuttavia, una portata extraterritoriale della normativa europea a protezione dei dati personali. Le questioni pregiudiziali sono state così definite un «groviglio di vipere» alla luce della loro complessità [Pardolesi 2017].

In breve, i giudici di Lussemburgo hanno rilevato che non tutti gli Stati terzi hanno riconosciuto il diritto alla deindicizzazione o comunque ne prevedono una portata differente. Secondo la Corte non esiste nemmeno nell'Unione un obbligo di effettuare la deindicizzazione su tutte le versioni del motore di ricerca, quanto piuttosto:

> […] nelle versioni di tale motore corrispondenti a tutti gli Stati membri, e ciò, se necessario, in combinazione con misure che, tenendo nel contempo conto delle prescrizioni di legge, permettono effettivamente di impedire agli utenti di Internet, che effettuano una ricerca sulla base del nome dell'interessato a partire da uno degli Stati membri, di avere accesso, attraverso l'elenco dei risultati visualizzato in seguito a tale ricerca, ai link oggetto di tale domanda, o quantomeno di scoraggiare seriamente tali utenti.

In ogni caso, il gestore del motore di ricerca dovrà operare un bilanciamento tra interesse del singolo a protezione dei dati personali e alla riservatezza, nella dimensione dell'oblio, e di interesse pubblico al reperimento della notizia nel web, di libertà di manifestazione del pensiero e di diritto ad essere informati. È stato peraltro segnalato che da un *obiter*

dictum di una recente sentenza della Corte di Giustizia emergerebbe un diritto alla re-indicizzazione (*right to relisting*) quale diritto all'adeguamento della lista dei risultati all'attuale posizione giuridica dell'interessato, che risulterebbe una soluzione migliore e più equa della deindicizzazione [Giovanella 2022].

Occorre, inoltre, segnalare che l'obbligo alla deindicizzazione potrebbe essere imposto anche all'editore del giornale online se l'articolo è rimasto a lungo tempo sulla sua pagina in violazione dell'onore e della reputazione dell'individuo e a seguito di una decisione giudiziale di responsabilità e condanna. Con riferimento a tale questione, nella sentenza Biancardi del 2021 la Corte di Strasburgo ha stabilito che il direttore di una testata giornalistica online possa essere ritenuto responsabile per la tardiva deindicizzazione di un articolo pubblicato, in quanto tale pretesa, quando esito di una pronuncia giudiziale, non viola l'art. 10 Cedu sulla libertà di espressione dal momento che il bilanciamento dei diritti e delle libertà fondamentali è stato operato dal giudice interno (Cedu, 25 novembre 2021, no. 77419/16, *Alessandro Biancardi v. Italia*).

All'esercizio del diritto alla deindicizzazione risulta una cancellazione di dati personali. La cancellazione rappresenta la terza dimensione del diritto all'oblio, inserita nel diritto europeo dalla Direttiva 95/46/CE e potenziata dal GDPR.

8.4 Il diritto alla cancellazione dei dati

Il diritto a protezione dei dati personali attribuisce all'interessato il diritto al controllo sulle informazioni che lo riguardano e la normativa europea, fin dalla Direttiva 95/46/CE, ha previsto degli specifici diritti per avere accesso, modificare o persino cancellare i dati in presenza di determinati presupposti. Nel GDPR la norma di riferimento è l'art. 17, rubricato «diritto alla cancellazione (diritto all'oblio)», che recita:

> 1. L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti:

a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
b) l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento;
c) l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2;
d) i dati personali sono stati trattati illecitamente;
e) i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento;
f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1.
2. 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.
3. I paragrafi 1 e 2 non si applicano nella misura in cui il trattamento sia necessario:
a) per l'esercizio del diritto alla libertà di espressione e di informazione;
b) per l'adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
c) per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'articolo 9, paragrafo 2, lettere h) e i), e dell'articolo 9, paragrafo 3;
d) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1, nella misura in cui il diritto di cui al paragrafo 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento; o

> e) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Questa norma consente all'interessato di ottenere la cancellazione dei dati personali da parte del titolare del trattamento nei casi elencati dal primo paragrafo. Tutte le tipologie di titolari del trattamento sono soggetti all'art. 17 e non solo i motori di ricerca, come nel caso del diritto alla deindicizzazione.

Nella rubrica dell'art. 17 è presente sia il termine cancellazione, che oblio. Ciò è dovuto al fatto che nelle varie raccomandazioni precedenti al Regolamento si fosse fatto riferimento alla necessità di introdurre un formale «diritto all'oblio» [Ricci 2019]. In realtà, il diritto alla cancellazione rimane una autonoma pretesa dell'interessato da cui deriva in concreto la perdita di informazioni che saranno così dimenticate.

Come anticipato, l'art. 17 non rappresenta una assoluta novità del GDPR poiché già la Direttiva 95/46/CE prevedeva alcune circostanze per poter presentare tale richiesta (art. 12, lett. b)) all'interno delle regole sul diritto all'accesso. Il Regolamento ha ampliato i motivi per i quali è possibile esercitare la pretesa, ma ha una portata limitata all'esaurimento della finalità di raccolta dei dati, a casi di contrarietà alle regole generali del trattamento, di revoca del consenso, dell'esercizio del diritto di opposizione, dell'obbligo di legge e del trattamento illecito di dati di minori in presenza di un servizio della società dell'informazione [Ricci 2019].

Il secondo paragrafo dell'art. 17 prevede anche un obbligo del titolare del trattamento a comunicare ai destinatari dei dati personali dell'avvenuta cancellazione, implicando, indirettamente, che questi ultimi provvedano a cancellare i dati ricevuti. Tale previsione risulta di complessa attuazione poiché è difficile risalire a tutti gli altri titolari del trattamento che hanno avuto accesso ai dati pubblicati dal primo soggetto.

Il terzo paragrafo dell'art. 17 inserisce molte eccezioni all'applicazione della cancellazione, tra cui la presenza di interessi pubblici e di tutela della libertà di espressione e informazione. Sarà il titolare del trattamento a verificare di volta in volta se la richiesta dell'interessato sia non accoglibile sulla base di ragioni che rendano le sue attività necessarie.

Peraltro, l'art. 85 del GDPR richiede agli Stati membri di conciliare la protezione dei dati personali con il diritto alla libertà di espressione e di

informazione, anche declinato in ambito giornalistico, accademico, artistico o letterario. Questa libertà rimane un aspetto del bilanciamento del diritto all'oblio anche nel caso della cancellazione di dati personali. Per effettuare tale bilanciamento è stato chiarito che l'interesse dell'interessato di regola supera interessi economici del titolare, ma potrebbe essere limitato da interessi pubblici alla conoscenza del dato a seconda della natura dell'informazione, della sua sensibilità, dal ruolo che il soggetto ricopre nella società [Kranenborg 2020, 480].

Nelle Linee Guida 5/2019 l'EDPS ha coordinato le previsioni dell'art. 17 con l'esercizio del diritto alla deindicizzazione nei confronti dei motori di ricerca[11]. In caso di cancellazione del mero link di collegamento da parte del motore di ricerca, il dato presente nel sito della notizia non viene cancellato. Tuttavia, secondo l'EDPS, ciò non esclude che una completa cancellazione possa diventare necessaria in presenza di alcuni presupposti. Ad esempio, alla richiesta di deindicizzazione potrebbe conseguire una totale eliminazione del dato se:

– l'informazione è stata rimossa da un registro pubblico;
– il link ad una pagina di una società contiene contatti di soggetti che non lavorano più presso la stessa;
– l'informazione è stata pubblica per anni sulla base di un obbligo legale e rimane online oltre il termine della sua efficacia;
– l'informazione consiste in espressioni di odio, calunnia, diffamazione come stabilito da un giudice.

Con il termine «cancellazione» si può intendere sia la distruzione che l'anonimizzazione dei dati. Come si vedrà [vedi → Capitolo 12], quest'ultima attività richiede che non sia più possibile, con ragionevole certezza e assunzione del rischio da parte del titolare, re-identificare i dati personali.

Il diritto alla cancellazione è uno dei più efficaci strumenti dell'interessato per controllare i suoi dati, evitando che siano conservati in assenza di una valida giustificazione. Questo diritto è anche riconosciuto dall'art. 9(e) dell'attuale versione della Convenzione 108 e fa, perciò, parte de-

11 Si v. le Linee Guida in https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-52019-criteria-right-be-forgotten-search-engines_en.

gli strumenti internazionali a protezione dei dati personali [Kranenborg 2020, 478].

Il diritto alla cancellazione, come quello alla deindicizzazione, infine, non è ad oggi riconosciuto nell'ordinamento statunitense [Pfenninger 2021]. L'American Law Institute sul punto ha sottolineato che [Solove, Schwartz 2022, 23]:

> this interest is highly controversial on this side of the Atlantic, and has only begun to find its way into U.S. law. The leading example here is the CCPA, which contains a highly qualified right to deletion. All and all, we did not think that the timing was right to propose an American "right to be forgotten". The ALI advises that Principles "should be written in the voice of the ALI." In our view, there was not yet enough agreement among the ALI membership on this topic for us to speak for this organization on it.

8.5 Casi 8-1, 8-2, 8-3

Caso 8-1

Tizio, ex-terrorista degli anni di piombo, ha scontato la sua pena detentiva e si è reinserito nella società. Dopo vent'anni dalla vicenda per la quale Tizio era stato condannato, la testata giornalistica Alfa pubblica un articolo nel quale viene accostata l'identità di Tizio con il ritrovamento di armi in un luogo non lontano alla sua abitazione e viene ripercorsa tutta la sua storia processuale e personale. A seguito della pubblicazione Tizio soffre di un profondo turbamento psicologico e subisce anche alcuni danni relazionali e a livello lavorativo. Tizio decide quindi di rivolgersi al suo legale di fiducia, chiedendo se sia possibile rimuovere l'articolo e ottenere il risarcimento del danno.
Quale o quali dimensioni del diritto all'oblio sono richiamabili nel presente caso?
Quali sono le norme applicabili?
Quali diritti sono da porre in bilanciamento?

Caso 8-2

Il giornale online Beta pubblica l'articolo «Truffa Asl per fornitura di protesi, patteggia otto mesi», riferendosi ad una vicenda in cui è coinvolto

Caio, amministratore unico di una società di rappresentanza di dispositivi medicali. La notizia viene conservata nell'archivio online della testata. Dopo due anni, Caio si rivolge a Google Italia per rimuovere il link alla pagina dell'archivio di Beta. Google rifiuta la richiesta di Caio, che decide quindi di chiedere al suo legale di fiducia come possa agire per tutelare la sua pretesa.
Quale o quali dimensioni del diritto all'oblio sono richiamabili nel presente caso?
Quali sono le norme applicabili?
Quali diritti sono da porre in bilanciamento?

Caso 8-3

Il giornale locale Gamma pubblica una notizia sulle cattive condizioni di salute del Sindaco, alludendo alla grave malattia di cui sarebbe affetto, grazie ad alcune interviste a cittadini e al suo medico di base. Il Sindaco, imbarazzato dalla questione, non lascia commenti né richiede rettifiche o modifiche a quanto divulgato. Dopo un anno dalla pubblicazione, in periodo di elezioni, il Sindaco, perfettamente sano e in forma, scopre che tale articolo viene ripubblicato sulla pagina Facebook del giornale e ne intende richiedere la cancellazione.
Quale o quali dimensioni del diritto all'oblio sono richiamabili nel presente caso?
Quali sono le norme applicabili?
Quali diritti sono da porre in bilanciamento?

CAPITOLO 9.
La privacy nel contesto lavorativo

Paolo Guarda

9.1 Premessa: il quadro giuridico di riferimento

Nel contesto lavorativo la raccolta di dati personali rappresenta un'attività indispensabile. Il rispetto della privacy nei luoghi dove si svolge l'attività lavorativa rappresenta, quindi, un elemento imprescindibile al fine di realizzare e tutelare la libertà e dignità del lavoratore.

La privacy nei luoghi di lavoro trova la propria disciplina nell'insieme di norme che regolano i punti di incontro tra la libertà del datore di lavoro di verificare il buon andamento dell'azienda e il diritto del lavoratore a vedere tutelata la propria riservatezza [Turco 2019].

Già la Direttiva 95/46/CE prevedeva all'art. 8, par. 2, lett. b) una regolamentazione *ad hoc* che era stata, poi, recepita in modi diversi nei vari Stati membri dell'UE. L'art. 88 del GDPR ha cercato di garantire la continuità delle regole ed è volto a favorire una comune interpretazione di queste a livello nazionale e da parte delle autorità competenti [Ciucciovino 2021 e Van Eecke, Simkus 2020]. Anche il GDPR, quindi, lascia ampia libertà agli Stati membri di emanare leggi che disciplinino il rapporto tra la legislazione europea ed il diritto nazionale del lavoro e fissa alcuni principi di riferimento quali il consenso e la trasparenza.

A livello giurisprudenziale, sono numerosi gli interventi delle corti sovranazionali che hanno provveduto a sancire alcuni principi e regole fondamentali in tale settore.

La CGUE ha pronunciato diverse sentenze sull'interpretazione delle norme pertinenti in materia di protezione dei dati applicabili anche in ambito lavorativo, pur non fornendo alcuna indicazione specificamente rivolta a tale contesto applicativo. Ad esempio, nel caso *Rundfunk*[12] la CGUE è stata interpellata affinché si pronunciasse sull'interpretazione di una disposizione dell'ordinamento austriaco, che prevedeva di rendere pubbliche le informazioni sulle retribuzioni di alcuni dipendenti del settore pubblico. La Corte ha affermato che qualsiasi misura nazionale che interferisca con la vita privata delle persone deve essere conforme all'articolo 8 Cedu.

Il caso *Worten*[13], invece, riguardava una legge portoghese che imponeva al datore di lavoro di mettere a disposizione dell'autorità nazionale preposta al controllo delle condizioni di lavoro il registro degli orari di lavoro dei dipendenti, in modo da consentirne l'immediata consultazione. La piccola azienda Worten è stata, così, sanzionata per violazione di tale disposizione, poiché aveva implementato un meccanismo che limitava l'accesso ai registri dell'orario di lavoro dei propri dipendenti. La Corte ha chiarito che gli orari di lavoro dei dipendenti costituiscono dati personali: le informazioni contenute in un registro riguardante i periodi di lavoro giornalieri e di riposo di ciascun lavoratore sono da considerarsi a tutti gli effetti dati personali, in quanto «relativi ad una persona fisica identificata o identificabile».

Anche la Corte Europea dei Diritti Umani (CEDU) ha avuto occasione di pronunciarsi in materia fornendo numerose sentenze che hanno coperto un'ampia gamma di questioni relative alla protezione dei dati ed alla privacy sul posto di lavoro. Due aspetti sono di particolare rilevanza: il monitoraggio e l'accesso ai fascicoli personali dei dipendenti e la sorveglianza occulta sul luogo di lavoro. Con riferimento al primo punto, uno dei casi storici è *Bărbulescu c. Romania*[14], dove la Grande Camera della Corte ha riscontrato una violazione del diritto alla vita privata ai sensi dell'art. 8 CEDU nel monitoraggio occulto dei lavoratori attraverso la raccolta delle loro e-mail private. La Corte di Strasburgo ha ritenuto che le autorità rumene non fossero riuscite a raggiungere un giusto equi-

12 Casi riuniti C-465/00, C-138/01 e C-139/01, Ö*sterreichischer Rundfunk*.

13 Caso C-342-12, *Worten*.

14 CEDU, *Bărbulescu c. Romania* (n. 61496/08).

librio tra gli interessi dell'impresa e quelli del lavoratore. In particolare, ha stabilito che i giudici nazionali non fossero riusciti a determinare se il ricorrente avesse ricevuto preventiva comunicazione da parte del datore di lavoro della possibilità che le comunicazioni private potessero essere controllate; inoltre, non avevano determinato le ragioni specifiche che giustificavano l'introduzione delle misure di controllo e se il datore di lavoro avesse potuto utilizzare misure che comportassero una minore intrusione nella vita privata e nella corrispondenza del ricorrente.

Per quanto riguarda la videosorveglianza, la Corte ha riscontrato una violazione dell'articolo 8 Cedu nel caso *Antovic e Mirkovic c. Montenegro*[15], che riguardava il monitoraggio dei dipendenti sul luogo di lavoro: i giudici nazionali avevano erroneamente ritenuto che i ricorrenti – docenti di alcune università del Montenegro - non avessero alcun diritto alla privacy, in quanto erano stati oggetto di sorveglianza in contesti pubblici.

9.2 L'analisi dell'art. 88 GDPR

Nel fornire una descrizione degli aspetti principali relativi al trattamento dei dati personali nel contesto lavorativo, iniziamo con il proporre il testo dell'art. 88 GDPR:

> 1. Gli Stati membri possono prevedere, con legge o tramite contratti collettivi, norme più specifiche per assicurare la protezione dei diritti e delle libertà con riguardo al trattamento dei dati personali dei dipendenti nell'ambito dei rapporti di lavoro, in particolare per finalità di assunzione, esecuzione del contratto di lavoro, compreso l'adempimento degli obblighi stabiliti dalla legge o da contratti collettivi, di gestione, pianificazione e organizzazione del lavoro, parità e diversità sul posto di lavoro, salute e sicurezza sul lavoro, protezione della proprietà del datore di lavoro o del cliente e ai fini dell'esercizio e del godimento, individuale o collettivo, dei diritti e dei vantaggi connessi al lavoro, nonché per finalità di cessazione del rapporto di lavoro.
> 2. Tali norme includono misure appropriate e specifiche a salvaguardia della dignità umana, degli interessi legittimi e dei diritti fondamentali degli interessati, in particolare per quanto riguarda la trasparenza

15 CEDU, *Antovic e Mirkovic c. Montenegro* (no. 70838/13).

> del trattamento, il trasferimento di dati personali nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune e i sistemi di monitoraggio sul posto di lavoro.
> 3. Ogni Stato membro notifica alla Commissione le disposizioni di legge adottate ai sensi del paragrafo 1 entro il 25 maggio 2018 e comunica senza ritardo ogni successiva modifica.

Come già si ricordava, l'UE ha concesso agli Stati membri un certo margine di discrezionalità nel regolamentare la materia: non è, però, possibile derogare agli standard minimi imposti dal GDPR. Lo scopo dell'art. 88 è, pertanto, quello di permettere l'adozione di regole sul trattamento dei dati nel contesto lavorativo che meglio si adattino alle esigenze del proprio particolare ordinamento giuridico, mantenendosi al tempo stesso in linea con i principi stabiliti dal GDPR. In pratica per molti Stati membri questo articolo serve come base giuridica per confermare l'applicabilità delle leggi nazionali che già esistono e sono state adottate mentre era in vigore la Direttiva 95/46/CE.

Potrebbe, così, verificarsi la circostanza in cui le norme nazionali siano addirittura più rigorose rispetto alla linea fissata dal GDPR. Per questo motivo, il par. 3 impone agli Stati membri di notificare alla Commissione Europea ogni specifica disciplina adottata ai sensi dell'art. 88, nonché ogni successiva modifica che incida su tali norme.

Come noto, il GDPR prevede diverse possibili basi giuridiche per il trattamento dei dati personali (art. 6). Vi sono, tuttavia, diversi aspetti che devono essere presi in considerazione in questo ambito.

Una delle questioni più dibattute al riguardo nasce dalla domanda se il consenso possa essere utilizzato come base giuridica per il trattamento dei dati personali dei dipendenti da parte del datore di lavoro. L'art. 4, pt 11, GDPR definisce il consenso come «liberamente prestato, specifico, informato e non ambiguo» (si veda anche l'art. 7 «Condizioni per il consenso»). Mentre le ultime tre condizioni sono piuttosto semplici e non rappresentano un problema per il datore di lavoro, la prima presenta notevoli criticità. Il WP29 ha sostenuto nei suoi pareri che un consenso di un dipendente raccolto dal datore di lavoro non può considerarsi ottenuto liberamente e, quindi, non può essere ritenuto legittimo (si v. WP29, *Parere 8/2001 sul trattamento dei dati personali nel contesto dell'occupazione* (WP48), del 13 settembre 2001; WP29, *Opinion 2/2017 on data*

processing at work (WP249), dell'8 giugno 2017): il datore di lavoro e il lavoratore non si trovano, infatti, in una eguale posizione di potere. Per questi motivi, nella pratica è generalmente preferibile che i datori di lavoro evitino il consenso come base giuridica per il trattamento dei dati dei dipendenti e si basino invece, ove possibile, su altre basi legittime disponibili [Kuner 2007, 260-261].

Così, il consenso come base giuridica è stato reso, perlopiù, inutilizzabile in questo ambito. Esistono, certo, altre legittimazioni disponibili ai sensi dell'art. 6, par. 1, GDPR (come ad es. l'esecuzione di un contratto (lett. b) e l'adempimento di un obbligo derivante dalla legge (lett. c): queste, però, generalmente riescono a coprire solo parzialmente l'ambito relativo al trattamento posto in essere dal datore di lavoro. Per tali ragioni, il «legittimo interesse» è diventato il fondamento giuridico che più spesso viene richiamato nel contesto lavorativo [Ciucciovino 2021, 952]. Le attività di trattamento finalizzate al miglioramento dell'efficienza lavorativa ed alla tutela del patrimonio materiale e intellettuale del datore di lavoro rientrano facilmente in tale nozione, che richiede, tuttavia, che sia condotto un esercizio di bilanciamento per tenere in considerazione gli interessi del datore di lavoro e quelli dei dipendenti (art. 6, par. 1, lett. f). In particolare, il WP29 ha sottolineato che, qualora si intenda utilizzare tale base, allora: l'interesse deve, appunto, essere legittimo; la tecnologia o il metodo utilizzato per il trattamento dei dati dei dipendenti devono essere necessari e proporzionati; il trattamento deve essere svolto nel modo meno invasivo possibile [Kotschy 2020, 337-339]. Ancora, è essenziale che siano adottate misure specifiche di attenuazione del rischio che garantiscano un adeguato equilibrio tra il legittimo interesse del datore di lavoro ed i diritti e le libertà fondamentali dei lavoratori. Al fine di garantire che la vita privata del lavoratore non sia violata, tali misure dovrebbero limitare l'attività di monitoraggio prevedendo restrizioni di tipo: geografico (ad es. circoscrivendo l'ambito di applicazione solo a luoghi specifici, escludendo di conseguenza aree sensibili come i luoghi religiosi, zone ad uso sanitario e locali destinati alle pause); orientate ai dati (ad es. non si dovrebbero monitorare comunicazioni e file elettronici personali); definite in termini temporali (ad es. monitoraggio a campione, anziché continuo).

Passando ad un altro principio fondamentale del GDPR, la trasparenza rappresenta uno degli elementi chiave che ogni attività di trattamento dei dati personali deve possedere per essere conforme al test di proporzio-

nalità. Le moderne tecnologie consentono di monitorare costantemente ed in tempo reale i dipendenti, nei luoghi di lavoro come nelle loro case, attraverso molti strumenti quali smartphone, desktop, tablet, veicoli e dispositivi indossabili. Esiste, così, un rischio molto elevato che il legittimo interesse dei datori di lavoro al miglioramento dell'efficienza e alla tutela del patrimonio aziendale si trasformi in un monitoraggio costante ingiustificato ed invasivo. Pertanto, il datore di lavoro deve sempre fornire ai dipendenti informazioni di carattere generale su quali misure di monitoraggio sono in atto, determinare secondo quali modalità i dati personali verranno raccolti tramite questi strumenti e chiarire le conseguenze della cattiva condotta eventualmente rilevata attraverso tali attività di controllo.

Per concludere, l'art. 88 è stato inserito nel GDPR al fine di consentire agli Stati membri di rendere conformi le peculiarità dei vari ordinamenti giuridici alle esigenze proprie del Regolamento europeo. Per questa ragione, norme diverse in tema di trattamento dei dati in ambito lavorativo rappresentano una sfida soprattutto per quei datori di lavoro che operano su scala globale.

9.3 La disciplina italiana in pillole

Il d.lgs. 101/2018 che, come già ricordato, ha adattato la nuova disciplina europea nel contesto italiano, ha di fatto mantenuto le disposizioni in materia di trattamento di dati personali dei lavoratori previste dalla l. 20 maggio 1970, d'ora in avanti «Statuto dei lavoratori», e dal Codice Privacy novellando in modo del tutto marginale gli articoli contenuti nel Titolo VIII «Trattamenti nell'ambito del rapporto di lavoro» in tema di: regole deontologiche (art. 111), informazioni in caso di ricezione dei curriculum (art. 111-bis), la raccolta di dati e loro pertinenza (art. 113), le garanzie in materia di controllo a distanza (art. 114), il telelavoro, il lavoro agile e il lavoro domestico (art. 115), regole in materia di istituti di patronato e assistenza sociale (art. 116) [Turco 2019, 518-519, Alvino 2021 e Maresca 2021].

Disposizione normativa oggetto da sempre di analisi e discussione con riferimento alla tutela della privacy del lavoratore è quella contenuta all'art. 4 «Impianti audiovisivi» dello Statuto dei lavoratori così come, da ultimo, novellato dal d.lgs. 14 settembre 2015, n. 151 (il c.d. *Jobs Act*):

> 1. Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali. In alternativa, nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni, tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale. In mancanza di accordo, gli impianti e gli strumenti di cui al primo periodo possono essere installati previa autorizzazione della sede territoriale dell'Ispettorato nazionale del lavoro o, in alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più sedi territoriali, della sede centrale dell'Ispettorato nazionale del lavoro. I provvedimenti di cui al terzo periodo sono definitivi.
> 2. La disposizione di cui al comma 1 non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze.
> 3. Le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196.

Il Jobs Act ha, di fatto, introdotto un regime diversificato a seconda del particolare strumento utilizzato:

– strumenti che consentono il controllo del lavoratore (ad es. la videosorveglianza);
– strumenti di lavoro (personal computer, smartphone, ecc.).

Di conseguenza, ai sensi del primo comma è consentito l'utilizzo di impianti audiovisivi o di altri sistemi dai quali derivi la possibilità di controllo a distanza dell'attività dei lavoratori al ricorrere, però, di due espresse condizioni: esigenze organizzative e produttive, di sicurezza del lavoro e tutela del patrimonio aziendale; esistenza di un preventivo accordo sindacale o, in mancanza, autorizzazione amministrativa, da parte della Direzione territoriale del lavoro. Tali accordi non possono in alcun modo

essere sostituiti dal consenso dei lavoratori. Sul punto si v. Cass., sez. III pen., 17 gennaio 2020, n. 1733:

> Questa procedura - frutto della scelta specifica di affidare l'assetto della regolamentazione di tali interessi alle rappresentanze sindacali o, in ultima analisi, ad un organo pubblico, con esclusione della possibilità che i lavoratori, uti singuli, possano autonomamente provvedere al riguardo - trova la sua ratio nella considerazione dei lavoratori come soggetti deboli del rapporto di lavoro subordinato. La diseguaglianza di fatto, e quindi l'indiscutibile e maggiore forza economico-sociale dell'imprenditore, rispetto a quella del lavoratore, rappresenta la ragione per la quale la procedura codeterminativa sia da ritenersi inderogabile (a differenza di quanto ritenuto invece dalla Sez. 3, n. 22611 del 17/04/2012), potendo essere sostituita dall'autorizzazione della direzione territoriale del lavoro solo nel solo di mancato accordo tra datore di lavoro e rappresentanze sindacali, non già dal consenso dei singoli lavoratori, poiché, a conferma della sproporzione esistente tra le rispettive posizioni, basterebbe al datore di lavoro fare firmare a costoro, all'atto dell'assunzione, una dichiarazione con cui accettano l'introduzione di qualsiasi tecnologia di controllo per ottenere un consenso viziato, perché ritenuto dal lavoratore stesso, a torto o a ragione, in qualche modo condizionante l'assunzione.

L'utilizzo di sistemi di monitoraggio in assenza dell'accordo sindacale configura un vero e proprio reato (artt. 4 e 38 d.lgs. 300 del 1970).

Il secondo comma prevede, invece, che le garanzie non si applicano agli strumenti utilizzati dal lavoratore per svolgere la prestazione lavorativa (es. smartphone, tablet, personal computer), e agli strumenti di registrazione degli accessi e delle presenze. In tali casi l'installazione non richiede alcun accordo sindacale. L'eccezione è limitata agli strumenti che «immediatamente servono al lavoratore per adempiere alle mansioni assegnate». Il Ministero del Lavoro, con nota del 18 giugno 2015, ha stabilito che nel momento in cui lo strumento viene modificato (ad esempio, con l'aggiunta di software di localizzazione), non si considera più rientrante nella categoria. Residuano casi che presentano dubbi interpretativi. Si pensi al caso in cui un GPS venga installato su un'auto aziendale al fine di coordinare le attività di varie squadre di intervento,

ma nel contempo possa essere impiegato per controllare la posizione dei singoli lavoratori.

Infine, il comma 3 stabilisce che le informazioni raccolte tramite gli strumenti di cui al comma 1 e 2, sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che al lavoratore sia fornita adeguata informazione circa le modalità di utilizzo degli strumenti e di effettuazione dei controlli. Tra questi, rientrano, evidentemente, anche i fini tipicamente disciplinari.

Altra questione rilevante è quella che riguarda l'eventuale nomina da parte del datore di lavoro, nei casi previsti dalla legge, di un medico competente al fine di adempiere agli obblighi in materia di tutela e sicurezza nei luoghi di lavoro. Tale figura tratta i dati relativi alla salute dei dipendenti ed archivia i dati richiesti dalla normativa in una cartella sanitaria, la cui conservazione è disciplinata dall'art. 25, co 1, lett. c), TUSL (d.lgs. 9 aprile 2008, n. 81). La normativa prevede sostanzialmente che:

– in vigenza di rapporto, il medico competente custodisca la documentazione sanitaria mantenendo il segreto professionale e nel luogo concordato con il datore di lavoro al momento dell'assegnazione dell'incarico;
– al termine dell'incarico, il medico competente consegni la documentazione sanitaria in originale al datore di lavoro, nel rispetto del Codice Privacy e del segreto professionale;
– lo stesso datore di lavoro debba conservare la documentazione in originale per almeno 10 anni o per il diverso termine particolare specificato dal TUSL;
– alla cessazione del rapporto di lavoro o su richiesta del lavoratore, il medico competente consegni copia della cartella sanitaria e di rischio al lavoratore.

Il datore di lavoro non può in alcun caso accedere alle cartelle sanitarie e concorre unicamente ad assicurarne un'efficace custodia nei locali aziendali. Non può, pertanto, venire a conoscenza delle eventuali patologie accertate dal medico, ma solo della valutazione finale circa l'idoneità – dal punto di visto sanitario – del dipendente allo svolgimento della mansione attribuitagli.

A completare il quadro normativo nel contesto italiano è d'uopo ricordare che il Garante privacy, il 12 dicembre 2018 ha emanato il «Prov-

vedimento che individua le prescrizioni contenute nelle Autorizzazioni generali nn. 1/2016, 3/2016, 6/2016, 8/2016 e 9/2016 che risultano compatibili con il Regolamento e con il d.lgs. n. 101/2018 di adeguamento del Codice», con il fine, appunto di aggiornare le vecchie autorizzazioni generali ed allinearne il contenuto a quanto previsto dal GDPR [vedi → Capitolo 5]. In particolare, la prima tra queste è dedicata alle Prescrizioni relative al trattamento di categorie particolari di dati nei rapporti di lavoro (aut. gen. n. 1/2016).

9.4 Scenari applicativi

Variegati sono gli scenari che riguardano il trattamento di dati personali dei lavoratori. Di seguito, a meri fini esemplificativi, una carrellata di possibili contesti applicativi:

– *trattamento dei dati dei candidati pubblicati sui social network*: la questione riguarda l'utilizzabilità di informazioni estratte dai profili dei social network ai fini dell'assunzione di lavoratori. L'accesso e l'estrazione di dati dai profili devono essere giustificati da una base giuridica e i dati possono essere trattati solo se i profili sono utilizzati per finalità lavorative. Inoltre, il candidato deve essere informato di tale controllo anche tramite indicazione nell'annuncio di lavoro;
– *trattamento dei dati dei lavoratori pubblicati sui social network*: tale attività di controllo potrebbe rendersi utile, ad esempio, nel caso in cui il datore di lavoro abbia inserito clausole di non concorrenza precisando che effettuerà controlli sul loro rispetto anche accedendo ai profili social. I dati possono essere trattati solo se i profili sono utilizzati per scopi lavorativi e se non vi sono altre modalità per realizzare la suddetta finalità;
– *monitoraggio della strumentazione informatica dei lavoratori* (mail, telefonate, navigazione Internet, ricerche online): se gli strumenti elettronici sono stati forniti dall'azienda (es. la casella di posta elettronica) essi sono da considerarsi dotazioni aziendali e quindi controllabili dal datore ed inutilizzabili a fini personali. Tale monitoraggio deve essere limitato sia nel tempo che per tipologia. Alcune misure di sicurezza relative ai dispositivi da remoto, quali il monitoraggio dei movimenti del mouse, l'utilizzo di webcam o di

tecnologie di *screen capture*, sono da considerarsi comunque e sempre illegittime. Di contro, la mail privata del dipendente non può mai esser oggetto di controllo da parte del datore di lavoro. La navigazione in Internet tramite gli strumenti aziendali può essere limitata o vietata purché non sussista un trattamento illecito dei dati dei lavoratori. Possono, pertanto, essere applicati appositi filtri per impedire gli accessi a determinati siti, ma i sistemi devono essere configurati in modo da cancellare periodicamente i dati personali. Un monitoraggio sistematico della navigazione su Internet deve ritenersi sempre illecito;

– *rilevazione della presenza dei lavoratori*: alcuni strumenti possono comportare l'indiretto monitoraggio della presenza e dell'attività dei lavoratori sul luogo di lavoro; tali trattamenti sono legittimi in quanto finalizzati a tutelare la perdita o la sottrazione di informazioni aziendali riservate, occorre, però, che venga fornita un'adeguata informativa;
– *trattamenti di dati mediante sistemi di videosorveglianza*: il video monitoraggio dei lavoratori è considerato illecito in quanto sproporzionato rispetto alla tutela dei diritti degli interessati; un sistema di videosorveglianza può essere utilizzato solo per la salvaguardia del patrimonio aziendale, per la sicurezza dei lavoratori e per esigenze organizzative, ovviamente in presenza di un accordo sindacale;
– *geolocalizzazione dei veicoli:* Il trattamento dei dati di geolocalizzazione dei veicoli aziendali è legittimo per la tutela della sicurezza dei veicoli e dei lavoratori, o anche per la pianificazione in tempo reale dell'attività lavorativa. Illecita è la geolocalizzazione nel caso in cui i veicoli aziendali possano essere usati anche per finalità private. Il dipendente deve poter disabilitare il monitoraggio nel momento in cui svolge un'attività di natura personale con l'auto aziendale;
– *controllo degli accessi dei lavoratori*: il controllo degli accessi dei lavoratori è possibile, ma occorre che sia realizzato con misure proporzionate. In particolare, non è valido il consenso come base giuridica, e nel caso di utilizzo di sistemi che trattano dati biometrici occorre che sussista la necessità di un controllo così intrusivo da non poter esser posto in essere adottando strumenti differenti e meno invasivi.

9.5 Intermezzo comparatistico: le regole in materia di trattamento di dati personali nel contesto lavorativo negli Stati Uniti

Il tema della tutela dei dati personali del lavoratore è particolarmente avvertito anche nel contesto statunitense [Solove, Schwartz 2021, 1091-1167]. La sorveglianza da parte dei datori di lavoro dei propri dipendenti è attività appetibile per i datori di lavoro per una serie di ragioni. In primo luogo, essi hanno tutto l'interesse ad assumere persone competenti che non causino interruzioni dell'attività lavorativa o che si comportino in modo negligente ed avventato. In secondo luogo, desiderano monitorare i propri dipendenti al fine di favorire un aumento della produttività e ridurre possibili cattive condotte. In terzo luogo, sussistono motivazioni legate a possibili procedimenti disciplinari.

Un ampio spettro di leggi regola la privacy dei dipendenti. Per capire come si applica questo apparato normativo, la prima distinzione da porre in essere è tra settore pubblico e privato.

Settore pubblico

Il governo federale è il più grande datore di lavoro negli Stati Uniti. Ci sono circa 2,1 milioni di dipendenti federali e 1,2 milioni di membri in servizio attivo nelle forze armate statunitensi. Anche i governi statali e locali danno lavoro a milioni di persone.

I dipendenti del settore pubblico sono protetti da una serie di regole.

Il Quarto emendamento si applica a tutti i funzionari del governo ed a tutti i datori di lavoro governativi. I dipendenti in tale settore godono, quindi, di protezione a livello costituzionale, anche se in modo talvolta limitato. Il diritto costituzionale alla riservatezza delle informazioni può tutelare dalla divulgazione di informazioni da parte del datore di lavoro. In *Whalen. v. Roe* (429 US 589 (1977)), la Corte Suprema ha ritenuto che il diritto alla privacy comprenda «individual interest in avoiding disclosure of personal matters» [vedi → Capitolo 1]. Esistono, inoltre, anche disposizioni contenute in alcune costituzioni statali che possono trovare applicazione.

Si applica, poi, ai datori di lavoro governativi, la legge federale sulle intercettazioni telefoniche che limita la loro capacità di condurre determinate forme di sorveglianza elettronica. L'eventuale disciplina statale

può prevedere ulteriori tutele. L'Americans with Disabilities Act (ADA) del 1990 vieta, inoltre, ai datori di lavoro di porre determinate domande ai propri dipendenti. Il Privacy Act federale può essere applicato al fine di evitare o limitare la divulgazione da parte di enti governativi di informazioni relative ai dipendenti federali in determinate circostanze.

Possono, infine, entrare in gioco anche specifici *tort*, attivabili dai dipendenti che intendono citare in giudizio i propri datori di lavoro per violazione della privacy, in particolare per: *instrusion upon seclusion*, *public disclosure of private facts*, e *false light*.

Settore privato

I dipendenti del settore privato godono di alcune delle tutele che abbiamo visto interessare i dipendenti pubblici, sebbene il Quarto Emendamento e la maggior parte delle costituzioni statali non si applichino al loro caso.

La legge federale sulle intercettazioni si applica non solo ai datori di lavoro governativi, ma anche agli attori del settore privato. Inoltre, l'ADA, le regole sulla violazione del contratto e i suddetti *tort* possono essere utilizzati per tutelare la privacy dei dipendenti del settore privato [Determan, Sprague 2011 e Ajunwa 2017].

A seconda del tipo di contratto di lavoro, i dipendenti possono disporre di ulteriori rimedi contrattuali. Accade così che in taluni casi i dipendenti possano essere licenziati solo per determinati motivi, quali prestazioni inadeguate, condotta non professionale o violazioni disciplinari. Se un dipendente viene licenziato ed il motivo non è legittimo, egli può agire in giudizio per risoluzione illecita e violazione del contratto. Purtroppo, molte altre figure contrattuali in ambito lavorativo vengono definite «at-will» e quindi questi dipendenti possono essere licenziati appunto «per capriccio» del datore di lavoro. In genere, in tali casi non potrà essere attivata un'azione di licenziamento illegittimo. Tuttavia, in molte giurisdizioni, esistono eccezioni a questa regola qualora il soggetto coinvolto sia stato licenziato per un motivo che viola l'ordine pubblico (ad esempio quando ciò è avvenuto per ragioni discriminatorie).

Infine, i dipendenti licenziati a causa del rifiuto di sottoporsi a test, interrogatori o monitoraggio invasivi per la loro privacy o licenziati a causa di fatti rivelati da tali attività possono in determinati casi citare in giudizio

il datore di lavoro per licenziamento illegittimo in violazione dell'ordine pubblico.

Il quadro giuridico statunitense è, dunque, particolarmente variegato, in quanto determinato dall'intersezione di discipline derivanti da fonti diverse sia a livello federale che statale e fortemente caratterizzato dall'intervento delle pronunce degli organi giurisdizionali, come è evidente che sia in un paese di common law [Solove, Schwartz 2021, 1094-1167]. Si può a ragione affermare che la tutela apprestata, comunque, non sia paragonabile a quella che gli ordinamenti europei riconoscono ai lavoratori.

9.6 Casi 9-1, 9-2, 9-3

Caso 9-1

Durante un processo di assunzione di nuovo personale, l'impresa Loki controlla i profili dei candidati sui vari social network e include le informazioni provenienti da questi network (e qualsiasi altra informazione disponibile su Internet) nel processo di screening.
Questo tipo di attività è legittima? Se sì, quando?
Qual è la base legittima per questo eventuale trattamento?
Quali misure il datore di lavoro deve adottare nel caso in cui tale trattamento sia considerato legittimo?

Caso 9-2

L'impresa Loki monitora i profili LinkedIn degli ex dipendenti che avevano precedentemente sottoscritto alcune clausole di non concorrenza. Lo scopo di questo monitoraggio è verificare il rispetto di tali clausole. Il monitoraggio è limitato a questi ex dipendenti.
Quando tale trattamento è considerato legittimo?
Qual è la base legittima per questo trattamento?

Caso 9-3

L'impresa Loki ha implementato uno strumento di prevenzione della perdita di dati per monitorare automaticamente le e-mail in uscita da parte dei propri dipendenti, allo scopo di prevenire la trasmissione non

autorizzata di dati riservati (ad esempio le informazioni relative ai propri clienti). Una volta che un'e-mail viene considerata come la potenziale fonte di una violazione dei dati, vengono eseguite ulteriori indagini. L'impresa fa affidamento sulla necessità per il suo legittimo interesse di proteggere i dati personali dei clienti nonché i suoi beni contro l'accesso non autorizzato o la fuga di dati.
Quando è legittimo tale trattamento?
Cosa succede in caso di un avviso di «falso positivo» che comporta l'accesso non autorizzato a e-mail legittime inviate dai dipendenti?
Quali misure di sicurezza devono essere adottate al fine di mitigare i rischi?

CAPITOLO 10.
Le Autorità garanti per la protezione dei dati personali

Paolo Guarda

10.1 Le autorità garanti per la protezione dei dati personali

Un elemento caratterizzante la disciplina europea è stato fin da subito la scelta di istituire alcune «agenzie» di garanzia: i c.d. «Garanti». Queste sono autorità indipendenti previste già dalla Convenzione di Strasburgo (Convenzione n. 108 del 28 gennaio 1981 sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale) [Finocchiaro 2012, 319-321].

La Direttiva 95/46/CE riprendeva l'indicazione della Convenzione appena citata e all'art. 28, par. 1, prevedeva che:

> Ogni Stato membro dispone che una o più autorità pubbliche siano incaricate di sorvegliare, nel suo territorio, l'applicazione delle disposizioni di attuazione della presente direttiva, adottate dagli Stati membri. Tali autorità sono pienamente indipendenti nell'esercizio delle funzioni loro attribuite.

Il GDPR conferma tale impostazione e dedica alla materia un apposito Capo VI «Autorità di controllo indipendenti» (artt. 51-59). L'art. 51, par. 1, così recita:

> Ogni Stato membro dispone che una o più autorità pubbliche indipendenti siano incaricate di sorvegliare l'applicazione del presente regolamento al fine di tutelare i diritti e le libertà fondamentali delle persone

> fisiche con riguardo al trattamento e di agevolare la libera circolazione dei dati personali all'interno dell'Unione (l'«autorità di controllo»).

Ogni Stato deve avere una o più Autorità di controllo, autonoma e indipendente (art. 52). I componenti devono essere nominati in base ad una procedura trasparente per almeno quattro anni (art. 53).

L'Autorità di Controllo ha i seguenti compiti (art. 51, par. 1):

> a) sorveglia e assicura l'applicazione del presente regolamento;
> b) promuove la consapevolezza e favorisce la comprensione del pubblico riguardo ai rischi, alle norme, alle garanzie e ai diritti in relazione al trattamento. Sono oggetto di particolare attenzione le attività destinate specificamente ai minori;
> c) fornisce consulenza, a norma del diritto degli Stati membri, al parlamento nazionale, al governo e ad altri organismi e istituzioni in merito alle misure legislative e amministrative relative alla protezione dei diritti e delle libertà delle persone fisiche con riguardo al trattamento;
> d) promuove la consapevolezza dei titolari del trattamento e dei responsabili del trattamento riguardo agli obblighi imposti loro dal presente regolamento;
> e) su richiesta, fornisce informazioni all'interessato in merito all'esercizio dei propri diritti derivanti dal presente regolamento e, se del caso, coopera a tal fine con le autorità di controllo di altri Stati membri;
> f) tratta i reclami proposti da un interessato, o da un organismo, un'organizzazione o un'associazione ai sensi dell'articolo 80, e svolge le indagini opportune sull'oggetto del reclamo e informa il reclamante dello stato e dell'esito delle indagini entro un termine ragionevole, in particolare ove siano necessarie ulteriori indagini o un coordinamento con un'altra autorità di controllo;
> g) collabora, anche tramite scambi di informazioni, con le altre autorità di controllo e presta assistenza reciproca al fine di garantire l'applicazione e l'attuazione coerente del presente regolamento;
> h) svolge indagini sull'applicazione del presente regolamento, anche sulla base di informazioni ricevute da un'altra autorità di controllo o da un'altra autorità pubblica;
> i) sorveglia gli sviluppi che presentano un interesse, se e in quanto incidenti sulla protezione dei dati personali, in particolare l'evoluzione delle tecnologie dell'informazione e della comunicazione e le prassi commerciali;

j) adotta le clausole contrattuali tipo di cui all'articolo 28, paragrafo 8, e all'articolo 46, paragrafo 2, lettera d);
k) redige e tiene un elenco in relazione al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'articolo 35, paragrafo 4;
l) offre consulenza sui trattamenti di cui all'articolo 36, paragrafo 2;
m) incoraggia l'elaborazione di codici di condotta ai sensi dell'articolo 40, paragrafo 1, e fornisce un parere su tali codici di condotta e approva quelli che forniscono garanzie sufficienti, a norma dell'articolo 40, paragrafo 5;
n) incoraggia l'istituzione di meccanismi di certificazione della protezione dei dati nonché di sigilli e marchi di protezione dei dati a norma dell'articolo 42, paragrafo 1, e approva i criteri di certificazione a norma dell'articolo 42, paragrafo 5;
o) ove applicabile, effettua un riesame periodico delle certificazioni rilasciate in conformità dell'articolo 42, paragrafo 7;
p) definisce e pubblica i criteri per l'accreditamento di un organismo per il controllo dei codici di condotta ai sensi dell'articolo 41 e di un organismo di certificazione ai sensi dell'articolo 43;
q) effettua l'accreditamento di un organismo per il controllo dei codici di condotta ai sensi dell'articolo 41 e di un organismo di certificazione ai sensi dell'articolo 43;
r) autorizza le clausole contrattuali e le altre disposizioni di cui all'articolo 46, paragrafo 3;
s) approva le norme vincolanti d'impresa ai sensi dell'articolo 47;
t) contribuisce alle attività del comitato;
u) tiene registri interni delle violazioni del presente regolamento e delle misure adottate in conformità dell'articolo 58, paragrafo 2; e
v) svolge qualsiasi altro compito legato alla protezione dei dati personali.

L'Autorità Garante dispone, inoltre, di una serie di poteri, soggetti a garanzie adeguate, incluso il ricorso giurisdizionale effettivo ed il giusto processo (art. 58).

I poteri d'indagine, che hanno finalità preventiva, sono (par. 1):

a) ingiungere al titolare del trattamento e al responsabile del trattamento e, ove applicabile, al rappresentante del titolare del trattamento o del responsabile del trattamento, di fornirle ogni informazione di cui necessiti per l'esecuzione dei suoi compiti;
b) condurre indagini sotto forma di attività di revisione sulla protezione dei dati;

c) effettuare un riesame delle certificazioni rilasciate in conformità dell'articolo 42, paragrafo 7;
d) notificare al titolare del trattamento o al responsabile del trattamento le presunte violazioni del presente regolamento;
e) ottenere, dal titolare del trattamento o dal responsabile del trattamento, l'accesso a tutti i dati personali e a tutte le informazioni necessarie per l'esecuzione dei suoi compiti; e
f) ottenere accesso a tutti i locali del titolare del trattamento e del responsabile del trattamento, compresi tutti gli strumenti e mezzi di trattamento dei dati, in conformità con il diritto dell'Unione o il diritto processuale degli Stati membri.

I poteri correttivi hanno, invece, finalità repressiva e sono (par. 2):

a) rivolgere avvertimenti al titolare del trattamento o al responsabile del trattamento sul fatto che i trattamenti previsti possono verosimilmente violare le disposizioni del presente regolamento;
b) rivolgere ammonimenti al titolare e del trattamento o al responsabile del trattamento ove i trattamenti abbiano violato le disposizioni del presente regolamento;
c) ingiungere al titolare del trattamento o al responsabile del trattamento di soddisfare le richieste dell'interessato di esercitare i diritti loro derivanti dal presente regolamento;
d) ingiungere al titolare del trattamento o al responsabile del trattamento di conformare i trattamenti alle disposizioni del presente regolamento, se del caso, in una determinata maniera ed entro un determinato termine;
e) ingiungere al titolare del trattamento di comunicare all'interessato una violazione dei dati personali;
f) imporre una limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento;
g) ordinare la rettifica, la cancellazione di dati personali o la limitazione del trattamento a norma degli articoli 16, 17 e 18 e la notificazione di tali misure ai destinatari cui sono stati comunicati i dati personali ai sensi dell'articolo 17, paragrafo 2, e dell'articolo 19;
h) revocare la certificazione o ingiungere all'organismo di certificazione di ritirare la certificazione rilasciata a norma degli articoli 42 e 43, oppure ingiungere all'organismo di certificazione di non rilasciare la certificazione se i requisiti per la certificazione non sono o non sono più soddisfatti;

i) infliggere una sanzione amministrativa pecuniaria ai sensi dell'articolo 83, in aggiunta alle misure di cui al presente paragrafo, o in luogo di tali misure, in funzione delle circostanze di ogni singolo caso; e
j) ordinare la sospensione dei flussi di dati verso un destinatario in un paese terzo o un'organizzazione internazionale

Infine, i poteri consultivi ed autorizzativi, volti alla verifica di requisiti particolari per poter procedere al trattamento (par. 3) sono:

a) fornire consulenza al titolare del trattamento, secondo la procedura di consultazione preventiva di cui all'articolo 36;
b) rilasciare, di propria iniziativa o su richiesta, pareri destinati al parlamento nazionale, al governo dello Stato membro, oppure, conformemente al diritto degli Stati membri, ad altri organismi e istituzioni e al pubblico su questioni riguardanti la protezione dei dati personali;
c) autorizzare il trattamento di cui all'articolo 36, paragrafo 5, se il diritto dello Stato membro richiede una siffatta autorizzazione preliminare;
d) rilasciare un parere sui progetti di codici di condotta e approvarli, ai sensi dell'articolo 40, paragrafo 5;
e) accreditare gli organismi di certificazione a norma dell'articolo 43;
f) rilasciare certificazioni e approvare i criteri di certificazione conformemente all'articolo 42, paragrafo 5;
g) adottare le clausole tipo di protezione dei dati di cui all'articolo 28, paragrafo 8, e all'articolo 46, paragrafo 2, lettera d);
h) autorizzare le clausole contrattuali di cui all'articolo 46, paragrafo 3, lettera a);
i) autorizzare gli accordi amministrativi di cui all'articolo 46, paragrafo 3, lettera b);
j) approvare le norme vincolanti d'impresa ai sensi dell'articolo 47.

L'Autorità garante deve elaborare una relazione annuale sulla propria attività (art. 59).

10.2 La procedura di cooperazione e il meccanismo dello «sportello unico»

Il Regolamento europeo ha potenziato notevolmente le procedure di cooperazione tra le Autorità di controllo. Ciò al fine di garantire un'inter-

pretazione uniforme tra gli Stati membri dei principi in materia di protezione dei dati personali ed una loro omogenea attuazione.

Merita, quindi, di esser anzitutto analizzato il c.d «one stop shop», ovvero lo «sportello unico».

Per agevolare i titolari e responsabili con diramazioni organizzative situate in diversi paesi membri o il cui trattamento possa potenzialmente incidere in modo sostanziale sugli interessati con sede in più Stati, l'Autorità di controllo dello stabilimento principale funge da «autorità capofila» (art. 56). Questa sarà, allora, tenuta a cooperare con le altre autorità interessate e sarà competente per l'adozione di decisioni vincolanti. Ogni singola autorità nazionale rimarrà competente a trattare casi locali qualora l'oggetto dello specifico trattamento riguardi unicamente l'attività effettuata in un singolo Stato membro e coinvolga soltanto interessati situati nel suo territorio.

Per determinare lo «stabilimento principale» o lo «stabilimento unico» si fa riferimento all'art. 4, pt. 16, dove si stabilisce che:

> a) per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale;
> b) con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento.

Ai sensi dell'art. 60, inoltre, l'Autorità di controllo capofila dovrà cooperare con le altre Autorità interessate al fine di raggiungere un consenso, scambiandosi tutte le informazioni ritenute utili (par. 1).

Al fine di garantire un'applicazione coerente del regolamento in tutto il territorio dell'Unione, il GDPR prevede anche il c.d. «meccanismo di coerenza» per la cooperazione (artt. 63-65). Ciò avviene soprattutto quando si voglia adottare una misura intesa a produrre effetti giuridici con riguardo ad attività di trattamento che incidono in modo sostanziale su un numero significativo di interessati in vari Stati membri. Tale procedura ha più funzioni [D'Agata 2018, 133]:

– agevolare la cooperazione tra Autorità nei casi in cui il Comitato europeo per la protezione dei dati (vedi *ultra*) sia tenuto ad emanare un parere su progetti di decisione che, per caratteristiche intrinseche, necessitano della stessa applicazione in tutti gli Stati membri;
– rimarcare il ruolo nomofilattico del Comitato europeo per la protezione dei dati personali mediante il potere di emanare un parere in caso di questioni di portata generale o che possono produrre effetti in diversi Stati membri (art. 64, par. 2);
– definire, con la valenza di una decisione vincolante, eventuali controversie tra Autorità di controllo o tra Autorità e Comitato europeo (art. 65).

10.3 Il Comitato europeo per la protezione dei dati

Il Comitato europeo per la protezione dei dati (più comunemente conosciuto nella versione anglosassone di «European Data Protection Board» – EDPB) è un nuovo organismo indipendente creato dal GDPR con il compito di promuovere l'applicazione coerente del Regolamento (artt. 68-76) [Zambrano 2019]. Esso rappresenta l'erede diretto del «Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali», più diffusamente conosciuto come «Gruppo art. 29» o WP29, il quale era stato previsto dall'art. 29, appunto, della Direttiva 95/46/CE.

L'art. 68 apre la sezione dedicata al Comitato statuendo che:

> Il comitato europeo per la protezione dei dati («comitato») è istituito quale organismo dell'Unione ed è dotato di personalità giuridica.

Non si tratta più, dunque, di un semplice gruppo a carattere consultivo come previsto appunto per il Gruppo art. 29, ma assurto alla qualifica di

«organismo» diviene a tutti gli effetti parte integrante del quadro istituzionale dell'Unione. Ciò è volto soprattutto a garantire una maggiore indipendenza del Comitato dalle istituzioni europee, eliminando anche materialmente qualsiasi legame diretto con la Commissione e rimarcando la sua indipendenza:

> Nell'esecuzione dei suoi compiti o nell'esercizio dei suoi poteri ai sensi degli articoli 70 e 71, il comitato opera con indipendenza (art. 69, par. 1).

L'EDPB è composto dalla figura di vertice delle Autorità di controllo di ciascuno Stato membro e dal Garante europeo per la protezione dei dati (European Data Protection Supervisor – EDPS) (art. 68). La composizione è, quindi, di fatto invariata rispetto al Gruppo art. 29, con la sola differenza della esplicita previsione della partecipazione del Garante europeo (che è stato creato successivamente alla Direttiva grazie al Regolamento (CE) n. 45/2001 del 18 dicembre 2000). La Commissione partecipa alle attività senza diritto di voto.

Il Comitato svolge le seguenti funzioni (art. 70):

- sorveglia il Regolamento e ne assicura l'applicazione corretta;
- fornisce consulenza nei confronti della Commissione;
- elabora e pubblica di linee guida, raccomandazioni e migliori prassi;
- elabora per le Autorità di controllo linee guida riguardanti l'applicazione delle misure correttive e la fissazione delle sanzioni amministrative pecuniarie;
- accredita gli organismi di certificazione ai sensi dell'art. 43 GDPR;
- emette pareri sui progetti di decisione delle Autorità di controllo conformemente al meccanismo di coerenza;
- emette pareri sui codici di condotta redatti a livello UE.

10.4 Alcuni esempi di Autorità garanti nazionali nel contesto europeo

Ogni Paese membro ha previsto un'apposita Autorità di controllo all'interno del proprio ordinamento.

Nel contesto italiano abbiamo, così, il «Garante per la protezione dei dati personali» che è appunto un'autorità amministrativa indipendente istituita con legge 31 dicembre 1996, n. 675, poi disciplinata dal Codice

Privacy, così come modificato dal Decreto di adeguamento n. 101/2018[1]. Il Garante italiano è particolarmente attivo nella predisposizione di linee guida e pareri volti ad agevolare il processo di adozione della disciplina europea nei più svariati scenari applicativi [vedi → Capitolo 5].

In Francia abbiamo, invece, la «Commission nationale de l'informatique et des libertés» (CNIL)[2] che, tra le altre attività, ha messo a disposizione un software di ausilio ai titolari in vista della effettuazione della DPIA. Il software - gratuito e liberamente scaricabile dal sito del Garante[3] - offre un percorso guidato alla realizzazione della DPIA, secondo una sequenza conforme alle indicazioni fornite dal Gruppo art. 29 nelle Linee-guida sulla DPIA. Anche quest'autorità pubblica prepara varie tipologie di documentazione utile per i titolari del trattamento e, più in generale, per l'interpretazione del GDPR e della legge nazionale [vedi → Capitolo 5].

La «Data Protection Commission» (DPC)[4] irlandese è, poi, particolarmente nota per aver giocato un ruolo chiave nelle controversie giurisprudenziali in tema di trasferimento transfrontaliero dei dati [vedi → Capitolo 6] in quanto lo stabilimento principale di Facebook si trova proprio nel suo territorio.

L'«Agencia Española de Protección de Datos» (AEPD)[5] è conosciuta per aver pubblicato l'8 ottobre 2020 una guida pratica volta a facilitare l'applicazione dei principi della privacy by design e by default al trattamento dei dati personali[6]. Le linee guida si compongono di 3 allegati e 9 parti.

La «Datatylsinet» norvegese[7] ha prodotto, invece, nel 2017 delle utilissime linee guida in tema di sviluppo software e Data Protection by Design e by Default[8]. Queste linee guida sono destinate principalmente a sviluppatori, architetti software, project manager, tester, DPO e consulenti per

1 https://www.garanteprivacy.it/.

2 https://www.cnil.fr/.

3 https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil.

4 https://www.dataprotection.ie/.

5 https://www.aepd.es/es.

6 https://www.aepd.es/sites/default/files/2019-12/guia-privacidad-desde-diseno_en.pdf.

7 https://www.datatilsynet.no/.

8 https://www.datatilsynet.no/en/about-privacy/virksomhetenes-plikter/innebygd-personvern/data-protection-by-design-and-by-default/.

la sicurezza: in generale a tutti i soggetti che sviluppano o contribuiscono allo sviluppo di software che contiene o elabora dati personali.

Infine, sempre nel contesto europeo (sebbene non più membro dell'UE) gioca un ruolo rilevante anche il Garante inglese: «Information Commissioner's Office» (ICO)[9]. Quest'Autorità è conosciuta tra le altre cose per le schede informative che costantemente mette a disposizione e che permettono agli operatori di accedere con più facilità a concetti e previsioni della disciplina privacy. Vari possono essere gli esempi di ciò. Ricordiamo la «Guided to the General Data Protection Regulation (GDPR)» del 2 agosto 2018, rivolta a coloro che hanno la responsabilità quotidiana della protezione dei dati e finalizzata ad illustrare le disposizioni del Regolamento al fine di aiutare concretamente le aziende nel loro processo di adeguamento[10].

10.5 Cenni ad esperienze d'oltreoceano

Nel contesto statunitense manca la previsione specifica di una «Agenzia federale» dedicata appositamente alla protezione dei dati personali. Come noto [vedi → Capitoli 1 e 5] in tale ambito, la disciplina persegue l'obiettivo di regolamentare il trattamento dei dati in ambiti specifici e con un approccio settoriale, in particolar modo con attenzione alle attività economiche coinvolte e nella misura in cui vi possano essere rischi per il cittadino considerato quale consumatore. La privacy non si configura quindi come un diritto fondamentale dell'individuo, ma come un diritto specifico del consumatore da bilanciare eventualmente con le esigenze delle imprese. Non sorprende, quindi, come non sia in tale contesto prevista una apposita «Agency» federale, ma che alcune funzioni che per noi sono tipiche dell'Autorità di controllo siano state delegate alla «Federal Trade Commission» (FTC), ovvero l'agenzia deputata alla tutela dei consumatori. Tale attività ha iniziato ad affermarsi sin dagli anni Settanta in occasione dell'applicazione di una delle prime leggi federali in materia: il Fair Credit Reporting Act. Come visto nel Capitolo 6, la FTC gioca un

9 https://ico.org.uk/.

10 https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf.

ruolo rilevantissimo anche con riferimento agli accordi volti a regolare il trasferimento transfrontaliero dei dati.

Il sistema federale canadese prevede, invece, un «Officer of the Privacy Commissioner of Canada»[11]. L'Ufficio del Garante fornisce consulenza e informazioni ai cittadini in merito alla protezione delle informazioni personali e applica la disciplina federale in materia di trattamento dei dati personali [vedi → Capitolo 5]. In tale contesto, ricordiamo la figura di Ann Cavoukian, già Privacy Officer per la Provincia canadese dell'Ontario, a cui dobbiamo le prime teorizzazioni del concetto di privacy by design di cui è stato diffusamente trattato nel Capitolo 4.

10.6 Casi 10-1, 10-2

Caso 10-1

L'impresa Midgard è particolarmente attiva nel settore del commercio elettronico e ha come business principale quello della vendita online di beni da lei direttamente prodotti o di altre aziende. Ha sedi e diramazioni in diversi Stati europei. La sua sede principale si trova in Irlanda. Roskva si trova in Francia ed acquista regolarmente prodotti tramite la piattaforma di Midgard. Un giorno si accorge, però, che le sue credenziali sono state rubate. Si rivolge allora a Midgard Francia per chiedere il recupero delle stesse ed esercitare il diritto d'accesso per avere informazioni sui dati ma non riceve alcuna risposta. Navigando in Rete scopre che altri utenti in tutta Europa hanno riscontrato lo stesso problema. Decide quindi di proporre un reclamo.
A quale Autorità di controllo può rivolgersi?
Cosa può lamentare?
Nel caso in cui il Garante francese non risponda in modo soddisfacente a quale altro Garante può rivolgersi?

Caso 10-2

L'impresa Asgard offre beni e servizi assicurativi ai cittadini europei. La sua sede è in Olanda. Freya vive nel medesimo stato e lamenta la mancanza di informativa privacy da parte dell'impresa Asgard e presenta reclamo innanzi alla Autorità garante in Olanda. Nel frattempo, Heimdall, che vive in Germania, propone il medesimo reclamo innanzi al Garante

11 https://www.priv.gc.ca/en/.

tedesco. Risulta, poi, che decine di altri cittadini europei residenti in altri Stati presentano medesimi reclami.
C'è un'autorità garante di riferimento che possa coordinare le indagini?
Quali obblighi hanno le altre Autorità adite nell'ambito di questo procedimento?
Da chi riceveranno risposta Freya e Heimdall?

CAPITOLO 11.
Il danno da lesione alla privacy e alla protezione dei dati: responsabilità e tutele

Giorgia Bincoletto

11.1 Il danno da lesione alla privacy

Il tema della responsabilità conseguente alla lesione alla privacy può essere articolato separando le due accezioni e dimensioni di violazione del diritto alla riservatezza e alla protezione dei dati personali.

In generale, gli ordinamenti giuridici prevedono tutele sia in sede amministrativa che giurisdizionale, civile e in alcuni casi anche penale, e vengono adottati diversi approcci a seconda della presenza o assenza di autorità di controllo e delle forme di responsabilità che tradizionalmente differiscono tra sistemi di civil law e common law. Nelle prossime sezioni verrà inquadrato questo tema molto complesso, cercando di fornire una sintesi degli approdi più rilevanti a livello legislativo, giurisprudenziale e dottrinale prendendo a riferimento alcuni sistemi e dedicando ampio spazio al contesto europeo.

11.2 Il danno da lesione della riservatezza in alcuni ordinamenti di civil law e common law[1]

Negli ordinamenti di common law la tutela della privacy nella dimensione di riservatezza, e perciò non di *informational privacy*, è innanzitutto

1 Si ringrazia il Prof. Guido Noto la Diega per la collaborazione e il confronto sul sistema giuridico inglese.

affidata alla *tort law*, ossia all'insieme delle regole in materia di illecito civile elaborate dal formante giurisprudenziale. Da definizione, infatti, il *tort* è considerabile un illecito civile, ossia un'azione o un'omissione che provoca una lesione ad un diritto o un danno ad un'altra persona e genera una responsabilità nel suo autore[2]. In caso di responsabilità, il danneggiato può ottenere il risarcimento dei *damages* o richiedere una specifica *injunction*.

Negli Stati Uniti, come precedentemente illustrato [vedi → Capitolo 1], fin dagli anni Sessanta del secolo scorso sono stati elaborati quattro privacy *tort* che consentono una tutela giurisdizionale in presenza di particolari circostanze [Prosser 1960 e Solove, Schwartz 2021]:

– *intrusion upon seclusion or solitude, or into the plaintiff's private affairs*, che può essere utilizzato con riferimento alla divulgazione di veritiere informazioni riguardanti una persona, considerate imbarazzanti, molto offensive per una *reasonable person* e non di interesse pubblico;
– *public disclosure of embarrassing private facts*, che fornisce rimedio in caso di ottenimento di informazioni private, senza che ne venga data pubblicità, quindi solo a livello visivo ed uditivo, e qualora siano informazioni considerate imbarazzanti e molto offensive per una *reasonable person*;
– *appropriation of name or likeness*, che può tutelare il soggetto qualora un altro si appropri ingiustamente del nome o delle sue caratteristiche;
– *false light in the public eye*, che consente di ottenere un rimedio in presenza di pubblicazione o divulgazione di fatti che pongano il soggetto pubblicamente in una *false light*.

Oltre a questi rimedi, assumono particolare importanza giurisprudenziale i seguenti *tort* [Giovanella 2017, 164-165 e Solove, Schwartz 2021]:

– *breach of confidence*, nel caso di divulgazione di informazioni riservate del cliente da parte di un professionista, come nel caso di avvocati, medici, banchieri;

2 Si v. ad es. le definizioni del Legal Information Institute della Cornell Law School disponibili in https://www.law.cornell.edu/wex/tort.

– *defamation*, che deriva dal *tort of libel and slander* e fornisce tutela qualora taluno divulghi un'informazione falsa che danneggi l'altrui reputazione in forma scritta o orale;
– *infliction of emotional distress*, che può essere invocato in presenza di condotte altamente offensive che intenzionalmente causino una sofferenza psicologica ad altri;
– *trespass*, uno dei tipici *tort* che tutela il diritto di proprietà, in caso di violazione del domicilio, quale luogo intimo della persona e della sua famiglia.

Come chiarito dal «Restatement of Torts» (2d), se l'azione basata su un *tort* è fondata e provata, chi ha violato il diritto alla privacy (convenuto o *defendant*) di un soggetto (attore o *plaintiff*) è considerato responsabile per il danno provocato e sarà condannato al pagamento dei *damages* (§ 652A: «one who invades the right of privacy of another is subject to liability for the resulting harm to the interests of the other»).

Inoltre, nell'ordinamento statunitense il soggetto può agire in sede giudiziale contro chi ha violato la sua riservatezza sulla base di alcuni emendamenti della Costituzione, come nel caso di intrusione ingiustificata dell'autorità pubblica in un luogo in cui ha una *reasonable expectation of privacy* [vedi → Capitolo 1], grazie all'interpretazione del Quarto Emendamento e alla possibilità di avere ristoro per i *civil damages* ai sensi del Titolo 42 del U.S.C. (United States Code) § 1983, che recita:

> Every person who, under color of any statute, ordinance, regulation, custom, or usage, of any State or Territory or the District of Columbia, subjects, or causes to be subjected, any citizen of the United States or other person within the jurisdiction thereof to the deprivation of any rights, privileges, or immunities secured by the Constitution and laws, shall be liable to the party injured in an action at law, suit in equity, or other proper proceeding for redress, except that in any action brought against a judicial officer for an act or omission taken in such officer's judicial capacity, injunctive relief shall not be granted unless a declaratory decree was violated or declaratory relief was unavailable. For the purposes of this section, any Act of Congress applicable exclusively to the District of Columbia shall be considered to be a statute of the District of Columbia.

Nel Regno Unito, invece, non è previsto uno specifico *tort* in ambito di violazione della riservatezza, ma in alcuni casi è stato utilizzato il rimedio del *breach of confidence*, applicabile per la protezione del segreto e delle informazioni confidenziali, ed è stato riconosciuto un *common law right to privacy*. Nel caso *Kaye (Gordon) v*. *Robertson* [1991] FSR 62, la corte statuiva che «in English law there is no right to privacy, and accordingly there is no right of action for breach of a person's privacy».

Successivamente, il *tort breach of confidence*, quale tradizionale common law right, veniva utilizzato come *cause of action* per l'utilizzo illecito di informazioni riservate. Con il caso *Campbell v*. *Mirror Group Newspapers Ltd* [2004] UKHL 22, l'House of Lords ha riconosciuto per la prima volta il «misuse of private information» quale nuova *cause of action* in caso di divulgazione illecita di informazioni private [vedi → Capitolo 5]. Ciò nonostante, non è ad oggi invocabile un *general tort of invasion of privacy*, come invece è possibile in altri sistemi di common law. Tuttavia, è possibile utilizzare la tutela dell'art. 8 della Cedu, grazie allo Human Rights Act del 1998 che ha trasposto internamente la Convenzione. Nel caso *Campbell v*. *Mirror Group Newspapers Ltd*, infatti, l'House of Lords, per stabilire la nuova *cause of action*, si è proprio basata sull'art. 8 della Cedu. Secondo la corte un giudice per valutare la presenza di una *reasonable expectation of privacy* dell'individuo in caso di invasione nella vita privata, e così per determinare se la protezione della riservatezza sia prevalente rispetto alla tutela di altri diritti e libertà fondamentali, come la libertà di espressione, dovrà effettuare un bilanciamento dei diritti e delle libertà in gioco caso per caso. Il *misuse of private information* si è così affermato come *cause of action* autonoma rispetto al *breach of confidence*. Sul piano rimediale, qualora la violazione risulti accertata e fondata, il soggetto potrà richiedere l'imposizione di una *injunction* e il risarcimento dei danni (*damages*), che potranno essere *compensatory* o *explanatory*.

Nel sistema misto canadese, il diritto alla riservatezza è tutelato dalle corti grazie alle interpretazioni delle Section 7 e 8 del Charter of Rights and Freedoms (1982), che sono di rango costituzionale e si applicano con riferimento ai rapporti tra individuo e governo o istituzioni [vedi → Capitolo 5]. Sulla base di tali sezioni il soggetto può agire con ricorso giurisdizionale per la tutela sia degli aspetti di *territorial privacy*, ossia di invasione del domicilio o di un luogo in cui si ha un'aspettativa di inti-

mità, che di *personal or corporal privacy*, qualora la violazione riguardi il corpo umano o la personalità del soggetto, e ottenere così il risarcimento dei danni subiti. Oltre alla protezione fornita dal Charter, che è limitata per scopo tra cittadino e istituzioni, nell'ordinamento canadese sono presenti i rimedi dei *torts* in common law, quali *misappropriation of personality* e *intrusion upon seclusion*. La Provincia del Québec, tuttavia, può essere considerata un sistema misto che, oltre a basarsi sulla common law, è dotato di un Civil Code. Agli artt. 3 e 35 del Civil Code del 1991 si tutelano i diritti della personalità, tra cui la privacy. Qualora vi sia una violazione della riservatezza, come nei casi previsti dall'art. 36 Civil Code, quali l'intrusione dell'abitazione altrui, o l'utilizzo illecito dell'immagine o della corrispondenza, il soggetto potrà agire in sede di responsabilità civile di tipo extracontrattuale per ottenere la condanna al risarcimento dei *damages* subiti.

Con riferimento all'ordinamento dell'Unione europea che tutela il rispetto della vita privata e familiare all'art. 7 della Carta di Nizza, è stato affermato che la Corte di Giustizia ha spesso richiamato la norma nella sua giurisprudenza, attribuendone però un'importanza marginale rispetto al riconoscimento di altri diritti fondamentali; il potenziale di questa disposizione non sarebbe pienamente sviluppato dalla Corte, se non in alcuni casi relativi alle materie di cittadinanza, alla violazione di dati personali, nel settore delle comunicazioni elettroniche o della giustizia [Martinico 2021, 22-35]. In ogni caso, all'interno dell'ordinamento dell'UE è possibile invocare direttamente l'art. 7 per tutelare situazioni in cui la sfera intima e riservata dell'individuo ha subito un danno a causa di un fatto attribuibile ad altri.

Negli ordinamenti di civil law il diritto alla riservatezza è comunemente tutelato in ambito di responsabilità extracontrattuale sulla base del principio del *neminem laedere.* In Francia, il diritto alla riservatezza (*vie privée*) trova protezione nell'art. 9 del Code Civil che protegge la vita privata («chacun a droit au respect de sa vie privée»). In caso di violazione della riservatezza, questa norma prevede la possibilità di richiedere al giudice in sede civile sia il risarcimento del danno subito che la condanna a misure volte a cessare o prevenire la situazione lesiva, quali il sequestro e la confisca, anche attraverso un sistema di cognizione sommaria [Custers 2019, 137-151]. La forma del risarcimento segue, quindi, la disciplina dell'art. 1382 del Code Civil, quale clausola generale che attribu-

isce l'obbligo del risarcimento del danno a chi ha cagionato illegittimamente e con colpa un danno ad altri («tout fait quelconque de l'homme, qui cause à autrui un dommage, oblige celui par la faute duquel il est arrivé à le réparer»).

Nel sistema giuridico federale tedesco il diritto alla riservatezza (*Privatsphäre*) non è esplicitamente inserito nel codice civile (BGB). Tuttavia, esso è tutelato grazie all'interpretazione giurisprudenziale delle regole relative ai diritti della personalità e del sistema di responsabilità civile che, pur in assenza di una clausola generale in materia, consente il risarcimento dei danni subiti a seguito di un illecito quando è violata una situazione giuridica soggettiva meritevole di tutela secondo la legge [Alpa, Resta 2019, 180-193, 289-298]. Dalla lettura del § 823(1) del BGB è stato così riconosciuto il diritto della personalità come «altro diritto», ossia bene giuridico meritevole di protezione.

Nell'ordinamento spagnolo la protezione della vita privata e dell'intimità, anche familiare (*intimidad personal* e *familiar*), è garantita direttamente ed esplicitamente all'interno della Costituzione (art. 18.1); la tutela del diritto è stata così elaborata principalmente dalla giurisprudenza del Tribunal Constitucional, ma è al contempo è consentita a livello di responsabilità civile di tipo extracontrattuale tra privati [Famiglietti 2005].

Anche in Italia il danno alla riservatezza è tutelabile in questa sede. La prossima sezione sarà interamente dedicata al contesto italiano.

11.3 Il danno da lesione della riservatezza in Italia

Come anticipato, In Italia il diritto alla riservatezza è considerato un aspetto particolare del generale diritto della personalità (art. 2 Cost.). Questo diritto attiene alla protezione delle vicende private dell'individuo, inclusa la sua vita privata e familiare, le comunicazioni e la protezione del domicilio (art. 7 Carta di Nizza). Nell'abrogato art. 2 del Codice Privacy la riservatezza veniva tutelata al pari dell'identità personale e del diritto alla protezione dei dati personali.

In caso di violazione del diritto alla riservatezza all'interno dell'ordinamento italiano, sin dalla pronuncia sul caso Soraya [vedi → Capitolo 2], l'individuo ha diritto al ricorso giurisdizionale secondo le regole della responsabilità civile extracontrattuale per fatto illecito. Se un soggetto

ritiene di aver subito un danno ingiusto alla sua riservatezza, derivante eziologicamente da una condotta attiva od omissiva, colposa o dolosa altrui, potrà agire in sede civile invocando l'art. 2043 c.c. che obbliga colui che ha commesso il fatto illecito a risarcire il danno. Il fatto illecito è, infatti, una delle fonti delle obbligazioni ai sensi dell'art. 1173 c.c. e l'art. 2043 c.c. rappresenta la clausola generale di tutela per i danni ingiusti alla sfera giuridica altrui, ossia per le lesioni ad interessi meritevoli di tutela che risultano *non iure*, non poste in essere nell'esercizio di un diritto e la cui condotta non è scriminata, e *contra ius*, in quanto in contrasto con il diritto e idonee ad arrecare un pregiudizio.

Il danneggiato dovrà provare il nesso di causalità, il profilo soggettivo di dolo o colpa del danneggiante e il danno occorso. Con riferimento al danno patrimoniale, l'attore dovrà provare il danno emergente e il lucro cessante derivante dal fatto illecito, come conseguenza immediata e diretta ai sensi dell'art. 1223 c.c., operante in materia extracontrattuale per il richiamo dell'art. 2056 c.c.; per quanto riguarda, invece, il danno non patrimoniale, come il danno morale a cui è ricondotta generalmente la violazione della riservatezza, la questione della risarcibilità risulta più complessa e si intreccia con le regole del sistema civilistico italiano e con l'interpretazione giurisprudenziale delle sue funzioni.

Senza pretesa di esaustività, tale questione potrebbe essere così riassunta. L'art. 2059 c.c. in tema di risarcimento del danno non patrimoniale stabilisce un principio generale: la risarcibilità di questa tipologia di danno è prevista solo nei casi determinati dalla legge. Secondo una tradizionale interpretazione, la disposizione si sarebbe riferita, oltre ai casi in cui la legge espressamente prevede un risarcimento, alla presenza di fatti astrattamente qualificabili come reati. Nel 2003 la Corte di Cassazione ha riconosciuto che è risarcibile il danno anche nei casi in cui non sia configurabile un reato (Cass., 11 luglio 2003, n. 233). Nel 2008 le Sezioni Unite della Corte hanno fissato un ulteriore principio di diritto, adottando un'interpretazione costituzionalmente orientata della norma: sono risarcibili i danni derivanti da un fatto illecito che abbia violato «in modo grave diritti inviolabili della persona, come tali oggetto di tutela costituzionale» (sentenze gemelle di San Martino, Cass., sez. un. 11 novembre 2008, nn. 26972, 26973, 26974, 26975). Tra questi diritti è ricompreso il diritto alla riservatezza, in quanto tutelato principalmente dall'art. 2 della Cost., ma anche dagli artt. 3 e 15 della Carta sulla dignità

e segretezza della corrispondenza, quale una delle situazioni giuridiche soggettive meritevoli di tutela secondo l'ordinamento giuridico. La gravità della violazione sussiste quando il danno è serio, non bagatellare, ossia quando supera la soglia minima di tollerabilità: il dovere di solidarietà previsto dall'art. 2 Cost. impone di tollerare le intrusioni nella propria sfera giuridica che si considerano minime, quali i fastidi e i meri disagi.

Inoltre, è ammissibile il ricorso alla tutela cautelare d'urgenza ai sensi dell'art. 700 c.p.c. in presenza dei presupposti di *fumus boni iuris* e *periculum in mora*. Il primo riguarda la ragionevole e approssimativa probabilità circa l'esistenza del diritto, mentre il secondo la sussistenza del pericolo nel ritardo dell'emanazione del provvedimento definitivo da parte del giudice. Il procedimento è regolato dagli artt. 669-*bis* e ss. del c.p.c. e consente una tutela strumentale ed immediata quando il tempo per valere il diritto in un processo a piena cognizione possa vanificare il diritto stesso. Questa tutela, essendo atipica, non è predeterminata nel contenuto del provvedimento che il giudice può adottare. Perciò, il giudice potrà ideare varie soluzioni per proteggere provvisoriamente ed efficacemente il diritto alla riservatezza.

Il panorama giurisprudenziale in materia di riservatezza riguarda di regola casi di:

- violazione del diritto all'oblio, quale particolare dimensione del diritto alla riservatezza come diritto ad essere dimenticati su una vicenda personale con il trascorrere del tempo [vedi → Capitolo 8];
- violazione delle regole sulla videosorveglianza tra datore di lavoro e dipendente [vedi → Capitolo 9];
- violazione delle regole relative all'anonimato della madre in ipotesi di parto anonimo e di adozione del figlio che desideri in età adulta conoscere le proprie origini [vedi → Capitolo 2];
- violazione delle regole sull'installazione di telecamere all'interno della proprietà privata, come nei condomini o in abitazioni private, o all'interno di strutture pubbliche [vedi → Capitolo 18];
- violazione della riservatezza in connessione con il diritto all'immagine e i diritti all'onore e alla reputazione, in presenza di divulgazione di fotografie, ritratti, notizie private, di fatti o scritti personali (artt. 2, 3, 10 Cost.);

– violazione della riservatezza nella dimensione della diffusione al pubblico di comunicazioni private, interviste, o diffusione illecita di intercettazioni telefoniche (ad es., si v. CEDU, 9 marzo 2021, n. 76521);
– violazione connesse al diritto alla protezione dei dati personali, quando vengono diffusi illegittimamente dati personali, come dati di contatto, informazioni sanitarie, fiscali, dati giudiziari, anche in ipotesi di richiesta di anonimizzazione della sentenza, poi comunque pubblicata con gli estremi identificativi, qualora oltre alla dimensione informazionale venga lesa anche l'intimità privata del singolo e la sua dimensione morale (ad es., Cass., sez. un., 22 luglio 2019, n. 19611; Cass., sez. un., 22 luglio 2020, n. 19681).

11.4 Le regole previste dal GDPR in caso di violazione di dati personali

Nell'Unione europea in caso di violazione della normativa in materia di protezione dei dati personali si applicano le regole previste dal Capo VIII del GDPR, artt. 77-84, che prevedono un sistema di tutela per l'interessato garantendo tre diritti a proporre:
1. un reclamo all'autorità di controllo;
2. un ricorso giurisdizionale effettivo nei confronti dell'autorità di controllo;
3. un ricorso giurisdizionale effettivo nei confronti del titolare o responsabile del trattamento.

Il ricorso «effettivo» dinanzi al giudice rimanda al diritto garantito dall'art. 47 della Carta di Nizza qualora i diritti e le libertà garantiti dal diritto dell'UE siano violati.

Sono esempi di violazione di dati personali:
– la perdita dei dati, o *data breach*, da cui possono derivare discriminazioni, furto o usurpazione d'identità, pregiudizio alla reputazione dell'interessato;
– il trattamento di dati personali senza la presenza di una valida base giuridica o di particolari categorie di dati senza i necessari presupposti (artt. 6 e 9, par. 2, GDPR);

– la raccolta di dati eccedenti rispetto alle finalità perseguite dal titolare del trattamento;
– illegittime comunicazioni o divulgazioni di dati personali;
– l'impossibilità di esercizio di uno dei diritti dell'interessato (artt. 15-22 GDPR).

Alla luce dei diritti sopra menzionati, sono tre le forme di tutela garantite dal GDPR: la tutela amministrativa dinanzi l'autorità garante dello Stato membro, la tutela giurisdizionale successiva alla decisione di tale autorità e la tutela giurisdizionale diretta.

In primo luogo, l'art. 77 stabilisce il diritto a proporre reclamo all'autorità di controllo nello Stato membro in cui l'interessato ha la residenza, dove svolge attività lavorativa o dove si è verificata la presunta violazione dei suoi dati personali (ad es., alla Commission nationale de l'informatique et des libertés - CNIL se l'individuo vive in Francia). Legittimato attivo al reclamo è, dunque, l'interessato o, in forza dell'art. 80, un ente a cui conferisce mandato, qualora si tratti di un organismo, organizzazione o associazione senza scopo di lucro, legalmente costituito in uno Stato membro, i cui obiettivi da statuto siano riferiti ad un interesse pubblico e dedicati alla protezione dei diritti e delle libertà in materia di dati personali. Un esempio di tale ente è Noyb.eu, associazione no profit fondata da Maximilian Schrems nel 2018 e gestita da esperti del settore privacy, che oltre a promuovere progetti di ricerca e sensibilizzazione, monitora servizi e attività online e presenta frequentemente reclami alle autorità competenti per conto degli interessati[3]. Note sono le azioni legali contro Facebook presso l'autorità garante irlandese e contro Google presso la CNIL [vedi → Capitolo 6].

Il criterio alternativo del luogo consente ad un interessato residente in un Paese terzo e che non lavora in uno Stato membro di accedere agli strumenti di tutela del GDPR qualora la violazione si sia verificata nell'Unione, ossia se il fatto generatore o il danno si siano verificati all'interno dei suoi confini [Bolognini, Pelino 2019, 419]. Il criterio di giurisdizione risponde al principio di prossimità e di certezza del foro competente. Nel caso di violazione tramite la Rete, il luogo del fatto generatore corrisponderebbe alla sede dello stabilimento del titolare, come stabilito dal-

3 Si v. https://noyb.eu/it/idea.

la Corte di Giustizia in materia di violazione del diritto d'autore [Bolognini, Pelino 2019, 420]. In presenza di trattamenti transfrontalieri di dati, troveranno applicazione le esigenze di coordinamento tra autorità adita dall'interessato e autorità capofila, competente dove si trova lo stabilimento del titolare, secondo le regole previste dagli artt. 56 e 60 GDPR.

Il reclamo è di regola gratuito, salvo si tratti di una richiesta manifestamente infondata o eccessiva, come nel caso di ripetizioni di ricorso, quando è possibile richiedere un contributo spese basato sui costi sostenuti dall'autorità o persino non soddisfare la richiesta (art. 57, par. 3 e 4 GDPR). L'autorità dovrà comunque provare l'abuso del diritto da parte del soggetto e motivare la mancata risposta.

L'interessato può, in generale, agire e difendersi personalmente e non dovrà seguire particolari requisiti formali nella redazione del reclamo. In alcuni casi, gli Stati membri hanno specificato dei contenuti minimi o hanno previsto dei modelli o guide[4].

In caso di avvio di un procedimento, l'interessato dovrà ricevere informazioni sullo stato e sull'esito del reclamo (art. 77, par. 2 GDPR). Dovrà, inoltre, essere informato della possibilità di adire un giudice avverso la decisione dell'autorità di controllo, attraverso le previsioni dell'art. 78 GDPR. Non solo l'interessato, ma ogni persona fisica e giuridica possono proporre ricorso contro una decisione se giuridicamente vincolante e se la riguarda (art. 78, par. 1, GDPR).

In caso di fondatezza di un reclamo, l'autorità di controllo dello Stato membro potrà adottare provvedimenti correttivi (quali avvertimenti, ammonimenti, ingiunzioni) e comminare sanzioni amministrative pecuniarie, come previsto dall'art. 58, par. 2 del GDPR.

Le sanzioni amministrative pecuniarie sono inflitte seguendo i dettagliati criteri e gli elementi elencati nell'art. 83 del GDPR, lunghissima disposizione che ha rappresentato una novità molto discussa, anche per l'entità dei massimali previsti. L'art. 83, par. 1, richiede che le sanzioni siano effettive, proporzionate e dissuasive e il par. 8 che l'esercizio dei poteri da parte dell'autorità di controllo sia soggetto a «garanzie procedurali adeguate in conformità del diritto dell'Unione e degli Stati membri, inclusi il ricorso giurisdizionale effettivo e il giusto processo», già tutelato dalla Carta di Nizza all'art. 47. Le sanzioni di questa disposizione

4 Si v. le istruzioni della CNIL in https://www.cnil.fr/fr/adresser-une-plainte.

possono essere inflitte in aggiunta alle misure adottabili da un'autorità di controllo ai sensi dei poteri correttivi previsti dall'art. 58, par. 2, da lett. a) a h) e j) GDPR. Per poter decidere sull'imposizione di una sanzione e del suo ammontare l'autorità di controllo dovrà tenere conto dei seguenti elementi (art. 83, par. 2, GDPR):

– «la natura, la gravità e la durata della violazione tenendo in considerazione la natura, l'oggetto o a finalità del trattamento» e «il numero di interessati lesi dal danno e il livello del danno da essi subito», in questo modo richiedendo un accertamento e analisi dei tipici elementi di un fatto illecito;
– «il carattere doloso o colposo della violazione», in capo al titolare o al responsabile del trattamento;
– «le misure adottate dal titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati», a seguito dell'evento dannoso;
– «il grado di responsabilità del titolare del trattamento o del responsabile del trattamento», alla luce delle misure tecniche e organizzative implementate per rispettare gli obblighi di data protection by design e by default e di sicurezza (artt. 25 e 32 GDPR), che assumono quindi un ruolo proattivo chiave per la prevenzione del rischio;
– «eventuali precedenti violazioni pertinenti commesse dal titolare del trattamento o dal responsabile del trattamento», indice, probabilmente, di minor responsabilizzazione;
– «il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi», visto anche l'obbligo di cooperazione previsto dall'art. 31 del Regolamento;
– «le categorie di dati personali interessate dalla violazione», considerando, ad esempio, che il trattamento di particolari categorie richiede maggiori garanzie;
– «la maniera in cui l'autorità di controllo ha preso conoscenza della violazione, in particolare se e in che misura il titolare del trattamento o il responsabile del trattamento ha notificato la violazione», come ad esempio nel caso di notifica di un *data breach* ai sensi dell'art. 33 o, invece, di presentazione del reclamo da parte dell'interessato;
– «qualora siano stati precedentemente disposti provvedimenti» da parte dell'autorità di controllo ai sensi dei poteri correttivi e sanzionatori di cui all'articolo 58, paragrafo 2, «nei confronti del titolare del

trattamento o del responsabile del trattamento in questione relativamente allo stesso oggetto, il rispetto di tali provvedimenti», indice di responsabilizzazione;
– l'adesione a codici di condotta (art. 40 GDPR) o a meccanismi di certificazione (art. 42 GDPR), quali strumenti di supporto alla *compliance* direttamente previsti dal Regolamento e attuati grazie ad una rete di enti indipendenti di valutazione operanti a livello nazionale; e
– «eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso, ad esempio i benefici finanziari conseguiti o le perdite evitate, direttamente o indirettamente, quale conseguenza della violazione».

In caso di violazione di più disposizioni del Regolamento, l'ammontare della sanzione non potrà superare l'importo per la violazione più grave (art. 83, par. 3, GDPR). Con riferimento alle previsioni, la normativa prevede due categorie di violazioni a cui sono assegnati diversi trattamenti sanzionatori.

Il paragrafo 4 dell'art. 83 assoggetta a sanzione fino ai 10 milioni di euro o, per le imprese, fino al 2% del fatturato mondiale annuo dell'esercizio precedente, se superiore, la violazione degli obblighi relativi:
– alle condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione, ossia alla necessità che abbia almeno sedici anni per prestare autonomo consenso, o altra età minima stabilita dalla legge nazionale, o che in alternativa sia prestato dal titolare della responsabilità genitoriale (art. 8 GDPR);
– ai trattamenti che non richiedono l'identificazione, in cui i dati non dovrebbero essere conservati, acquisiti o trattati per identificare l'interessato, che deve essere informato e che potrebbe non poter esercitare i diritti per non dover fornire ulteriori informazioni (art. 11 GDPR);
– all'adozione dei principi di data protection by design e by default da parte del titolare, che, come visto, richiedono l'implementazione di misure tecniche e organizzative adeguate a incorporare e rispettare efficacemente i principi e i diritti tutelati dal Regolamento (art. 25 GDPR);
– alla gestione della contitolarità del trattamento, prevedendo congiuntamente le responsabilità e funzioni un uno specifico accordo (art. 26 GDPR);

– alla designazione del rappresentante del titolare o del responsabile nell'Unione europea, qualora non sia stabilito al suo interno ma tratti dati personali di interessati che qui si trovano offrendo beni o prestazioni di servizi, o monitorando il loro comportamento (art. 27 GDPR, che si applica nei casi previsti dall'art. 3, par. 2);
– alla designazione del responsabile del trattamento e alle condizioni per l'esercizio del suo ruolo, alla luce del contratto di autorizzazione e delle necessarie garanzie (artt. 28-29 GDPR);
– alla tenuta del registro delle attività di trattamento contenente le varie informazioni sul trattamento (art. 30 GDPR);
– alla necessaria cooperazione con l'autorità di controllo nell'esecuzione dei suoi compiti (art. 31 GDPR);
– all'adozione delle misure tecniche e organizzative di sicurezza da parte del titolare e del responsabile per garantire un livello di protezione adeguato al rischio del trattamento (art. 32 GDPR);
– alla notifica di un *data breach* all'autorità di controllo senza ingiustificato ritardo (art. 33 GDPR);
– alla comunicazione di un data breach all'interessato senza ingiustificato ritardo (art. 34 GDPR);
– all'elaborazione della valutazione di impatto sulla protezione dei dati – o DPIA – alla presenza dei presupposti e all'eventuale consultazione preventiva con l'autorità di controllo (artt. 35-36 GDPR);
– alla designazione del responsabile della protezione dei dati – o DPO – quando necessario (artt. 37-38-39 GDPR);
– per gli organismi di certificazione, alla corretta applicazione degli artt. 42-43 GDPR;
– per l'organismo di controllo di un codice di condotta, all'applicazione dell'art. 41, par. 4 GDPR.

Il paragrafo 5 dell'art. 83 assoggetta a sanzione fino ai 20 milioni di euro o, per le imprese, fino al 4% del fatturato mondiale annuo dell'esercizio precedente, se superiore, la violazione degli obblighi relativi:
– ai principi del trattamento dei dati e alle condizioni di liceità relative al consenso e alle altre basi giuridiche del trattamento (artt. 5, 6, 7, 9 GDPR);
– ai diritti degli interessati: diritti all'informazione, all'accesso, alla rettifica, alla cancellazione dei dati, alla limitazione del trattamento, alla

portabilità dei dati, all'opposizione al trattamento, a non essere sottoposti a un processo decisionale automatizzato (artt. 12-22 GDPR);
– ai trasferimenti transfrontalieri dei dati (artt. 44-49 GDPR);
– alle previsioni legislative adottate dallo Stati membro ai sensi del Capo IX del Regolamento per specifiche situazioni di trattamento: trattamento e libertà d'espressione e di informazione; trattamento e accesso del pubblico ai documenti ufficiali; trattamento del numero di identificazione nazionale; trattamento dei dati nell'ambito dei rapporti di lavoro; garanzie e deroghe in materia di ricerca scientifica o storica, a fini statistici o di archiviazione nel pubblico interesse; obblighi di segretezza; norme di protezione dei dati presso chiese e associazioni religiose (artt. 85-91 GDPR);
– all'inosservanza di «un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati», o «il negato accesso» stabiliti dall'autorità di controllo ai sensi dell'articolo 58, paragrafi 1 e 2.

In caso di imposizione di un ordine, di una limitazione provvisoria o definitiva del trattamento, o di un ordine di sospensione dei flussi di dati da parte dell'autorità di controllo attraverso i poteri correttivi previsti all'articolo 58, paragrafo 2, GDPR, il titolare del trattamento potrà essere condannato ad una sanzione amministrativa pecuniaria fino a 20 milioni di euro o per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore (art. 83, par. 6, GDPR).

Oltre a queste categorie di violazioni, lo Stato membro potrà prevedere ulteriori disposizioni relative all'imposizione di sanzioni amministrative pecuniarie ad autorità pubbliche e organismi pubblici istituiti in tale ordinamento (art. 83, par. 7, GDPR). L'ultimo paragrafo dell'articolo 83 prevede, infine, che qualora in uno Stato membro non siano stabilite sanzioni amministrative pecuniarie, il Regolamento può essere applicato

> in maniera tale che l'azione sanzionatoria sia avviata dall'autorità di controllo competente e la sanzione pecuniaria sia irrogata dalle competenti autorità giurisdizionali nazionali, garantendo nel contempo che i mezzi di ricorso siano effettivi e abbiano effetto equivalente alle sanzioni amministrative pecuniarie irrogate dalle autorità di controllo.

Le sanzioni erogabili in caso di violazione di dati personali sono proporzionate alle concrete caratteristiche del trattamento dei dati e della violazione (art. 83 GDPR).

Un reclamo presso la competente autorità di controllo non pregiudica il diritto dell'interessato ad utilizzare altri strumenti amministrativi o giurisdizionali previsti a livello nazionale (art. 77, par. 1 GDPR). Deve, peraltro, essere sempre garantito il diritto a un ricorso giurisdizionale effettivo nei confronti del titolare o responsabile del trattamento (art. 79 GDPR).

Il Regolamento prevede, in aggiunta, una peculiare disciplina in presenza di litispendenza internazionale e di connessione per oggetto o titolo della domanda giudiziale, che è volta a lasciar decidere al primo giudice adito per evitare che il secondo decida in modo difforme (art. 81 GDPR).

L'interessato dovrà comunque agire giurisdizionalmente per richiedere il risarcimento del danno, visto il rinvio alla competenza dell'autorità giurisdizionale in materia (art. 82, par. 6 GDPR). Il GDPR, infatti, sancisce il diritto al risarcimento del danno materiale e immateriale causato dalla violazione delle sue norme da parte del titolare o del responsabile del trattamento, ma rinvia alla competenza giurisdizionale nazionale (art. 82 GDPR).

Legittimato attivo è l'interessato, o suo ente mandatario, e legittimati passivi sono il titolare, i contitolari e il responsabile del trattamento. I titolari possono rispondere per il danno cagionato da un trattamento che violi una o più norme del Regolamento, mentre il responsabile può rispondere soltanto se non ha adempiuto agli obblighi specificamente diretti al suo ruolo (ad es. art. 28 GDPR) o se ha agito in modo difforme o contrario alle istruzioni ricevute dal titolare (art. 82, par. 2 GDPR). In presenza di più titolari (contitolarità) e responsabili (pluralità di nomine) si applicano le regole della responsabilità solidale. L'eventuale presenza di un sub-responsabile rileva soltanto sul piano interno tra responsabile e soggetto delegato, in cui può operare un regresso in presenza di concorso causale nella determinazione dell'evento dannoso; all'esterno, ossia per il soggetto interessato, rimane ferma la responsabilità del responsabile del trattamento [Tosi 2019, 43].

Opera un esonero di responsabilità qualora titolare e responsabile provino che l'evento danno non è a loro imputabile (art. 82, par. 3, GDPR). L'onere della prova grava, dunque, in capo al soggetto conve-

nuto nell'azione di risarcimento, che dovrà dimostrare la mancanza del nesso eziologico con il danno occorso dovuta ad un fattore esterno alla sua attività e controllo, come nel caso di caso fortuito, forza maggiore, o intervento di terzi.

Il Regolamento, infine, affida agli Stati membri la possibilità di introdurre ulteriori sanzioni amministrative o penali (art. 84 GDPR), le quali non possono tuttavia essere in contrasto con il principio del *ne bis in idem* (Cons. 149 GDPR), previsto peraltro dall'art. 50 della Carta di Nizza.

I legislatori nazionali hanno previsto sanzioni penali per reprimere comportamenti particolarmente lesivi del diritto a protezione dei dati personali, tra cui la violazione delle misure in ambito di sicurezza o il trattamento illegittimo di particolari categorie di dati, ma risultano scarsamente applicate [Lynskey 2021a, 1196-1197].

11.5 La tutela per la violazione di dati personali in Italia

In Italia, l'interessato potrà rivolgersi al Garante per la protezione dei dati personali, tramite reclamo, o dinanzi all'autorità giudiziaria ordinaria (artt. 140-*bis* - 143 del Codice Privacy); in aggiunta, l'interessato può effettuare una segnalazione al Garante, quale ulteriore mezzo di tutela amministrativa (art. 144 del Codice Privacy). Il reclamo non può essere proposto se è già stata adita l'autorità giudiziaria, secondo un meccanismo di alternatività dei piani di tutela introdotto dopo l'adeguamento del Codice Privacy al GDPR con il d.lgs. 101/2018, malgrado nel Regolamento non sia affatto previsto, essendo i rimedi esperibili senza pregiudizio reciproco (art. 140-*bis* Codice Privacy). Questa alternatività non si applica alla segnalazione, esperibile da chiunque, ma che può non essere esaminata dall'autorità che non è obbligata a valutarla.

Per quanto concerne il reclamo, l'interessato, o l'ente che lo rappresenta (art. 80 GDPR), dovrà fornire un'indicazione «per quanto possibile dettagliata dei fatti e delle circostanze su cui si fonda, delle disposizioni che si presumono violate e delle misure richieste», oltre ai riferimenti del titolare o del responsabile coinvolto nella presunta violazione (art. 142, co. 1, Codice Privacy). Il reclamo dovrà essere sottoscritto dall'interessato, che dovrà fornire un recapito per l'invio delle comunicazioni, e il reclamante potrà agire e difendersi personalmente, o tramite un avvoca-

to, previa procura. Il Garante ha reso disponibile un modello di reclamo sul proprio sito istituzionale[5].

Il procedimento è disciplinato dal Regolamento 1/2019 (doc-web 9107633) del Garante che divide due fasi, istruttoria preliminare e procedimento amministrativo, e orienta l'esame di reclamo (e anche di segnalazioni) a criteri di «semplicità delle forme osservate, di celerità ed economicità, anche in riferimento al contraddittorio» (art. 9). Il reclamo dovrà essere deciso entro nove o dodici mesi dalla data di presentazione in caso di particolari esigenze istruttorie (art. 143 Codice Privacy). L'interessato dovrà comunque essere informato sullo stato del reclamo entro tre mesi dalla sua proposizione ai sensi dell'art. 78, par. 2, GDPR. Il Codice Privacy novellato ha introdotto alcuni criteri di applicazione delle sanzioni amministrative pecuniarie e dei poteri correttivi e sanzionatori dell'autorità (art. 166).

Un provvedimento del Garante potrà poi essere impugnato avanti al giudice ordinario competente - Tribunale per materia e foro alternativo tra residenza dell'interessato e sede del titolare del trattamento per territorio - entro trenta giorni dalla comunicazione del provvedimento (in caso di interessato residente all'estero il termine sarà di sessanta giorni), secondo il rito lavoristico e seguendo le regole previste dall'art. 10 del d.lgs. 150/2011, modificato nel 2018 con il decreto di attuazione del GDPR, e dall'art. 152 del Codice Privacy. La successiva impugnazione dovrà essere esperita tramite ricorso per Cassazione poiché la sentenza non è appellabile.

Come anticipato nella precedente sezione, il profilo risarcitorio dell'eventuale violazione è di esclusiva competenza dell'autorità giurisdizionale (art. 82, par. 6, GDPR). La risarcibilità del danno da violazione della protezione dei dati personali ha sollevato varie questioni giuridiche che verranno ora brevemente analizzate.

Innanzitutto, si è discusso sia a livello giurisprudenziale che dottrinale sulla risarcibilità del profilo non patrimoniale dello stesso, qualora la condotta illecita del titolare o del responsabile non integri una fattispecie di reato e sulla distribuzione dell'onere della prova del danno. Con riferimento alla risarcibilità, è stato anticipato che la lettura costituzio-

5 Si v. il modello italiano in https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/4535524.

nalmente orientata dell'art. 2059 c.c. tutela in caso di violazione grave di un diritto inviolabile della persona, quale il diritto alla protezione dei dati personali che è ricompreso nel generale diritto della personalità sulla base dell'art. 2 della Costituzione, e che consente il risarcimento dei danni non patrimoniali anche in assenza di un reato. Relativamente ai danni patrimoniali, il danneggiato dovrà provare il danno emergente e il lucro cessante derivante dall'illecito del titolare o del responsabile del trattamento.

Il danno da trattamento di dati personali riceve tutela in Italia ai sensi dell'art. 82 GDPR applicato nel contesto della responsabilità aquiliana. L'art. 82 andrà, quindi, ricollegato all'impianto codicistico interno che vede nell'art. 2043 c.c. la norma centrale. Tuttavia, il sistema di responsabilità civile per trattamento illecito di dati personali è considerato speciale e polifunzionale rispetto al regime ordinario, assumendo per certi versi una funzione ulteriore preventiva-dissuasiva-sanzionatoria rispetto a quella tradizionale reintegrativa-compensativa [Tosi 2021, 611-615].

Prima dell'adeguamento interno al GDPR, il Codice Privacy richiamava espressamente l'art. 2050 c.c. nella disciplina relativa al ricorso giurisdizionale. Questa norma presume la responsabilità dell'esercente dell'attività pericolosa, generando una forma di responsabilità oggettiva, a meno che il convenuto non provi di aver adottato tutte le misure idonee a evitare il danno. L'attore, dal canto suo, se lamenta un danno, non deve provare l'elemento doloso o colposo della condotta visto che la responsabilità è presunta, ma la prova del nesso di causalità tra attività e danno patito. Da questo richiamo la dottrina e la giurisprudenza ricostruivano la responsabilità civile per illecito trattamento dei dati personali come responsabilità oggettiva o aggravata dalla presunzione di colpa [Tosi 2019, 31-34].

A seguito del d.lgs. 101/2018, il richiamo alla disposizione civilistica è stato eliminato; tuttavia, l'art. 82 del GDPR prescrive che il titolare o il responsabile del trattamento possono fornire la prova della non imputabilità del danno, che può liberare quindi da responsabilità. È stato, pertanto, sostenuto che in termini fattuali l'onere probatorio non sia cambiato dopo il GDPR: il nesso eziologico tra condotta attiva od omissiva non sussiste se si prova che il danno deriva da terzi, da forza maggiore o dal caso fortuito o se si hanno adottato tutte le misure idonee ad evitare il danno [Bolognini, Pelino 2019, 445]. Questo approccio è stato

seguito anche dalla Corte di Cassazione (si v. Cass. 17 settembre 2020, n. 19328): il danneggiato deve dimostrare l'esistenza del danno e il nesso di causalità tra trattamento illecito e danno subito, mentre il danneggiante deve provare di aver adottato tutte le misure per evitare il danno. Ciò è coerente con il principio di responsabilizzazione, o accountability, del GDPR, che attribuisce il rischio di gestione dell'attività del trattamento al titolare [Tosi 2021, 562-569, 593-594].

L'imputazione della responsabilità da illecito trattamento di dati personali rimarrebbe perciò a titolo di responsabilità aggravata per colpa presunta o di responsabilità oggettiva a seconda della soluzione interpretativa adottata [Tosi 2021, 594-599].

La prova liberatoria non si deve limitare alla dimostrazione (negativa) di non aver violato una disposizione normativa. Occorre fornire la prova positiva di aver valutato il rischio, di aver attuato le misure di sicurezza e organizzative a eliminare o ridurre questo rischio. Se, invece, i soggetti sono considerati entrambi responsabili, si avrà una forma di responsabilità pro-quota e non solidale, come emerge dalla possibilità di agire in regresso.

Un contrasto giurisprudenziale è sorto in relazione alla possibilità che il danno da violazione di dati personali sia considerato in *re ipsa* e che, quindi, sia insito nella violazione, senza necessità di specificare le conseguenze negative subite dall'illecito. L'opposto orientamento, invece, sostiene la necessaria prova e l'analitico accertamento del danno lamentato dal ricorrente, per non snaturare le funzioni della responsabilità aquiliana che, al contrario, risulterebbe di portata sanzionatoria e non compensativa o consolatoria. Per questo secondo orientamento sarebbe necessaria sia la prova del danno-evento, quale lesione del diritto causata dall'illecito, sia del danno-conseguenza, ossia del concreto pregiudizio subito. L'orientamento relativo al danno in *re ipsa* in questa materia è stato sostenuto sulla base delle decisioni relative alla risarcibilità del danno non patrimoniale per violazione di un diritto fondamentale della persona tutelato dalla Costituzione (sentenze gemelle delle Sezioni Unite n. 26972-26975/2008). Adottando questa prospettiva, la violazione di un tale diritto non dovrebbe richiedere la prova effettiva della gravità e l'allegazione del pregiudizio in quanto la responsabilità sorgerebbe per il solo fatto che il trattamento dei dati personali sia stato effettuato illegittimamente.

Tuttavia, tale orientamento è oggi superato dalla giurisprudenza di legittimità. La Corte di Cassazione adotta la seconda posizione e segue il seguente principio di diritto: il danno non patrimoniale a seguito della violazione di dati personali non si sottrae alla verifica della «gravità della lesione» e della «serietà del danno»; il danno, perciò, dovrà sempre essere allegato e provato, anche attraverso presunzioni (Cass. 18 luglio 2019, n. 1943; Cass. ord. 10 giugno 2021, n. 16402). La lesione minima del diritto di protezione dei dati personali è giustificabile per un bilanciamento con principio di solidarietà dell'art. 2 della Cost., secondo un principio di tolleranza, mentre è ingiustificabile una violazione che «offenda in modo sensibile» la portata delle norme. L'accertamento di fatto è inevitabilmente rimesso al giudice di merito, poiché riguarda il particolare contesto temporale e sociale della vicenda dedotta in giudizio. Peraltro, la possibilità di ricorrere a presunzioni, anche semplici, agevola la prova del danno. Se il danno viene giudicato esiguo, il ricorrente può incorrere in responsabilità aggravata per abuso del processo (v. Cass. 8 febbraio 2017, n. 3311).

Tra i parametri per definire l'ammontare del risarcimento del danno la giurisprudenza utilizza [Tosi 2019, 242-243, 245]:
- la gravità del pregiudizio;
- la durata del pregiudizio a seguito della violazione dei dati personali e dell'attività illecita;
- l'ambito del trattamento;
- le categorie dei dati trattati;
- il rilievo economico del trattamento illecito;
- la notorietà del danneggiato e quindi la sua condizione soggettiva;
- il ravvedimento operoso del danneggiante e le sue condizioni oggettive, tra cui quelle economiche, sociali e professionali.

Oltre alla tutela civilistica, il Codice Privacy prevede alcune fattispecie di reato (artt. 167-172), anche nel contesto delle comunicazioni elettroniche:
- trattamento illecito di dati;
- comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala;
- acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala;

– falsità delle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante;
– inosservanza dei poteri del Garante;
– violazione delle disposizioni in materia di controlli a distanza e indagini sulle opinioni dei lavoratori.

Le sanzioni penali sono poste a tutela sia della protezione dei dati personali, ma anche della riservatezza, dell'identità personale dell'individuo e per rafforzare l'azione amministrativa del Garante [Manes, Mazzacuva 2021, 1670]. Le fattispecie di maggior rilievo sono quelle tipizzate dall'art. 167 del Codice Privacy come «trattamento illecito di dati personali», che recita:

> 1. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, operando in violazione di quanto disposto dagli articoli 123, 126 e 130 o dal provvedimento di cui all'articolo 129 arreca nocumento all'interessato, è punito con la reclusione da sei mesi a un anno e sei mesi.
> 2. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, procedendo al trattamento dei dati personali di cui agli articoli 9 e 10 del Regolamento in violazione delle disposizioni di cui agli articoli 2-sexies e 2-octies, o delle misure di garanzia di cui all'articolo 2-septies arreca nocumento all'interessato, è punito con la reclusione da uno a tre anni.
> 3. Salvo che il fatto costituisca più grave reato, la pena di cui al comma 2 si applica altresì a chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, procedendo al trasferimento dei dati personali verso un paese terzo o un'organizzazione internazionale al di fuori dei casi consentiti ai sensi degli articoli 45, 46 o 49 del Regolamento, arreca nocumento all'interessato.
> 4. Il Pubblico ministero, quando ha notizia dei reati di cui ai commi 1, 2 e 3, ne informa senza ritardo il Garante.
> 5. Il Garante trasmette al pubblico ministero, con una relazione motivata, la documentazione raccolta nello svolgimento dell'attività di accertamento nel caso in cui emergano elementi che facciano presumere l'esistenza di un reato. La trasmissione degli atti al pubblico ministero avviene al più tardi al termine dell'attività di accertamento delle violazioni delle disposizioni di cui al presente decreto.

6. Quando per lo stesso fatto è stata applicata a norma del presente codice o del Regolamento a carico dell'imputato o dell'ente una sanzione amministrativa pecuniaria dal Garante e questa è stata riscossa, la pena è diminuita.

11.6 Casi 11-1, 11-2, 11-3

Caso 11-1

In Italia l'avvocato Tizio riceve dieci e-mail promozionali in tre anni dalla società Alfa che promuove eventi e formazione. Non avendo mai prestato il consenso per il trattamento dei dati, Tizio lamenta un illecito trattamento dei suoi dati personali (indirizzo e-mail) e promuove un giudizio presso il Tribunale territorialmente competente, chiedendo il risarcimento dei danni subiti quantificati in euro 360,00.
Quali sono le norme del Regolamento e del Codice Privacy richiamabili dal presente caso?
Quali difese potrà adottare la società Alfa?
Quali sono i criteri che il giudice dovrà valutare per esaminare la domanda di Tizio?
Tizio potrà ottenere il risarcimento del danno?

Caso 11-2

La società Gamma statunitense vende prodotti online sul proprio sito di e-commerce, previa registrazione e creazione di un apposito account dell'utente. In data 15.05.2022 Mevio acquista un prodotto utilizzando la propria carta di credito. In data 25.06.2022 si verifica un incidente di sicurezza ai server di Gamma e tutti i dati relativi agli acquisti, compresi i dati bancari dei clienti, vengono divulgati online. Soltanto dopo tre giorni Mevio si accorge che dalla sua carta sono stati sottratti 1.000,00 euro, legge una notizia sul data breach in un quotidiano online di settore e scrive a Gamma per avere informazioni sui propri dati. In data 15.09.2022 Mevio si rivolge al legale di fiducia perché Gamma non ha mai risposto e intende conoscere i suoi diritti.
Cosa può fare Mevio per tutelare i suoi diritti?
Mevio può invocare la tutela del GDPR?
Quali sono le norme del GDPR richiamabili dal presente caso?

Caso 11-3

Caia e Sempronia rendono deposizioni testimoniali in un processo penale quali vittime di un reato a sfondo sessuale. Durante il processo la rete nazionale italiana organizza una serie di riprese delle udienze e delle deposizioni, chiedendo il consenso ai partecipanti, al giudice e alle parti processuali, per poter creare una puntata della trasmissione televisiva di punta sui processi penali in Italia. Caia e Sempronia accettano di essere riprese durante la loro deposizione, a condizione di non essere riprese nel volto e nel tono di voce per mantenere l'anonimato. La puntata viene trasmessa in prima serata e Caia e Sempronia risultano perfettamente identificabili. Le donne si rivolgono dunque al legale di fiducia per ottenere informazioni su come agire nei confronti della rete televisiva.
Caia e Sempronia possono lamentare la violazione di quali diritti?
Quali sono le norme del Regolamento e del Codice Privacy richiamabili dal presente caso?
Quali sono i rimedi invocabili?
Caia e Sempronia potranno ottenere il risarcimento del danno?

PARTE II
Il diritto alla riservatezza e il diritto alla protezione dei dati personali. Problemi della nuova era tecnologica

CAPITOLO 12.
Anonimizzazione e pseudonimizzazione

Giorgia Bincoletto

12.1 Dato personale e non personale, dato pseudonimizzato, dato anonimizzato, dato anonimo

La nozione di dato è qualificata in modo diverso a seconda del contesto epistemologico di riferimento [Guarda 2021, 13]. Da un punto di vista giuridico, il dato può essere personale o non personale in base alla riferibilità, o meno, del suo nucleo informazionale ad una persona fisica. Da questa complessa differenziazione discende l'applicazione della normativa analizzata nella Parte I di questo Manuale, che disciplina proprio la protezione dei dati personali (si v., ad es., l'art. 1 GDPR).

Ai dati non personali all'interno dell'ordinamento dell'UE, invece, si applica il Regolamento 2018/1807, relativo alla libera circolazione di questa tipologia di dati, che li definisce come «dati diversi dai dati personali» (art. 3). I dati non personali sono definiti in contrapposizione a quelli personali. La distinzione, tuttavia, è molto complessa e richiede maggiori specificazioni. Non è, peraltro, possibile individuare una categoria intermedia [Comandè 2022 e Graziadei 2021].

Si ricorda, in aggiunta, che la dicitura «personal information», tipica degli ordinamenti di common law, non può considerarsi pienamente sovrapponibile a quella di «dato personale» perché può, in generale, riferirsi soltanto ai dati che rendono una persona direttamente identificabile [vedi → Capitoli 1 e 5]. Le seguenti considerazioni dovranno, perciò, essere limitate all'ordinamento europeo.

La definizione di dato personale fornita dal GDPR come «qualsiasi informazione riguardante una persona fisica identificata o identificabile» è ampia, flessibile e dinamica [vedi → Capitolo 3]. Oltre a dati comuni, come nome e cognome, indirizzo e numero di telefono, si possono individuare particolari categorie di dati personali che richiedono una maggiore protezione (art. 9, par. 1, GDPR). Il nucleo informativo può riguardare sia elementi oggettivi (la presenza di una malattia in un dato soggetto) che soggettivi (opinioni, credenze del medesimo soggetto) [Finck, Pallas 2020]. Il dato può essere espresso in forma di linguaggio scritto o di numero, di immagine, o di video. La persona dovrà essere identificata o identificabile attraverso un elemento, che non è necessariamente il nome e cognome. L'identificabilità potrà essere compiuta dal titolare del trattamento o da terzi.

Nella nozione di dato personale può essere ricompreso anche il dato pseudonimizzato, quale dato sottoposto ad un procedimento di pseudonimizzazione, ossia quel trattamento che impedisce l'attribuzione del dato ad un interessato specifico senza l'utilizzo di informazioni aggiuntive, che sono conservate separatamente e soggette a misure tecniche e organizzative che garantiscono la non attribuzione del medesimo dato alla persona fisica (art. 2, n. 5, GDPR). Dopo il procedimento, generalmente volto ad esigenze di maggiore sicurezza e di protezione del dato, anche in ottica di data protection by design [vedi → Capitolo 4], l'interessato è potenzialmente identificabile grazie all'utilizzo delle informazioni aggiuntive conservate dal titolare del trattamento o dal responsabile. Per tale ragione, il dato, seppur separato dalle informazioni che rendono la persona direttamente identificabile, rimane personale.

Sono, all'opposto, considerati non personali i dati anonimizzati, ossia dati personali sui quali sono state applicate tecniche di anonimizzazione, i dati riferiti alle persone giuridiche, che per definizione non sono protette dal regolamento, e i cd. dati anonimi, quali dati che non sono mai riferibili a persone fisiche. Come anticipato nel Capitolo 3, il GDPR menziona le informazioni anonime al Considerando 26 come le

> 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.

Nella prima parte del testo si farebbe riferimento ai dati anonimi, mentre nella seconda ai dati anonimizzati, come dati personali resi «sufficientemente anonimi».

I dati anonimizzati sono diversi da quelli pseudonimizzati perché non possono essere attribuiti ad una persona fisica con l'utilizzo di informazioni aggiuntive a disposizione del titolare del trattamento. Dal processo di anonimizzazione si ottiene una nuova rappresentazione del dato che fuoriesce dall'applicazione della normativa europea [D'Acquisto, Naldi 2017, 35].

Il Regolamento 2018/1807 fornisce alcuni esempi specifici di dati non personali (Cons. 9):

> gli insiemi di dati aggregati e anonimizzati usati per l'analisi dei megadati, i dati sull'agricoltura di precisione che possono contribuire a monitorare e ottimizzare l'uso di pesticidi e acqua, o i dati sulle esigenze di manutenzione delle macchine industriali.

Questi dati dovrebbero circolare liberamente all'interno dell'UE per rendere più competitiva l'economia digitale del Mercato Unico (Cons. 1), ormai sempre più basato sui Big Data, quali enormi aggregazioni di dati dal grande potenziale in molti settori economici [vedi → Capitolo 13].

In ambito statistico e di ricerca sono sempre più utilizzati i «dati sintetici», ossia informazioni generate *ex novo* da algoritmi di intelligenza artificiale a partire da dataset reali di dati personali, ma successivamente scollegate dagli stessi e non riferibili a persone fisiche [Floridi 2020]. Inoltre, è frequente il trattamento di dataset «misti», ossia di insiemi strutturati di dati personali e dati anonimi [è il caso dell'*Internet of Things*, vedi → Capitolo 15]. Se i dati personali sono separabili da quelli anonimi, la disciplina a protezione dei dati personali si applicherà ai primi e il Regolamento 2018/1807 ai secondi (art. 2); se ciò non è possibile, o è economicamente inefficiente o non tecnicamente praticabile la separazione, la prima normativa si applicherà all'intero dataset.

L'anonimizzazione consente inoltre di riutilizzare i dati personali al di fuori del limite di compatibilità richiesto dal principio di limitazione della finalità. Nei vari testi legislativi, tuttavia, non è ancora presente una definizione di anonimizzazione. A seconda del contesto lo stesso dato potrebbe essere personale o non, e tale distinzione risulta complessa

[Bholasing 2022 e Finck, Pallas 2020]. Per poter comprendere quando un'informazione sia resa anonima fino al punto da impedire o da non consentire l'identificazione dell'interessato è necessario utilizzare un approccio interdisciplinare e seguire le indicazioni provenienti da autorità garanti e da studi tecnici di settore, come verrà presentato nella prossima sezione.

12.2 L'anonimizzazione di dati personali e il Regolamento 2018/1807

L'anonimizzazione è una soluzione alternativa alla cancellazione dei dati quando si intende conservarli ed utilizzarli al di fuori dei limiti della normativa privacy. Una sua definizione è stata fornita a livello di soft-law dal Parere 05/2014 sulle tecniche di anonimizzazione del Gruppo art. 29 come «il risultato del trattamento di dati personali volto ad impedire irreversibilmente l'identificazione». L'anonimizzazione, dunque, è un trattamento successivo di dati personali e fino alla sua conclusione si applicano le regole previste a loro protezione [D'Acquisto, Naldi 2017, 35].

In quanto attività di trattamento, l'anonimizzazione richiede la presenza di una base giuridica e dovrà essere compatibile con la finalità originaria, come richiesto dall'art. 5, par. 1, lett. b) del GDPR [Gross, van Veen 2020]. I dati personali devono, infatti, essere stati raccolti e trattati in conformità alle regole giuridiche e, solo se ne esistono i presupposti, quei dati potranno essere anonimizzati per realizzare ulteriori finalità. Un caso di incompatibilità che impedirebbe l'anonimizzazione è la necessità di consentire per un certo tempo l'esercizio di diritti da parte dell'interessato [Comandè 2022, 44].

Un dato è considerabile anonimizzato quando sono rimossi tutti gli elementi identificativi in modo efficace ed irreversibile. In concreto, tuttavia, il processo potrebbe essere successivamente aggirato tramite tecniche di *reverse engineering*. Con l'evoluzione tecnologica che continua ad avanzare, le tecniche di anonimizzazione che oggi vengono ritenute efficaci ed irreversibili potrebbero non esserlo in un breve o medio periodo. Da un punto di vista giuridico, perciò, si considera anonimizzato il dato a cui è associabile un rischio accettabile di re-identificazione; il rischio, infatti, non potrebbe mai essere pari a zero perché i) il concetto di rischio è per sua natura scalabile e ii) un livello di rischio zero sarebbe tecnicamente impossibile da ottenere [Podda, Vigna 2021].

La Corte di Giustizia nel caso *Patrick Breyer v. Bundesrepublik Deutschland* (C- 582/14) ha sul punto statuito che la re-identificazione della persona interessata dovrebbe essere «praticamente irrealizzabile, per esempio a causa del fatto che implicherebbe un dispendio di tempo, di costo e di manodopera, facendo così apparire in realtà insignificante il rischio di identificazione». Una volta anonimizzato, il dataset potrebbe essere reso accessibile a chiunque con l'assunzione del rischio di eventuale re-identificazione, in ottica di accountability.

Secondo il Gruppo art. 29, un dato personale è composto da un insieme di valori e attributi, ossia elementi costitutivi, e la loro combinazione consente l'identificazione della persona interessata. L'autorità ha individuato tre rischi essenziali per l'anonimizzazione nel momento in cui si ha accesso al dato:

– (l') *individuazione*, che corrisponde alla possibilità di isolare alcuni o tutti i dati che identificano una persona all'interno dell'insieme di dati;
– (la) *correlabilità*, vale a dire la possibilità di correlare almeno due dati concernenti la medesima persona interessata o un gruppo di persone interessate (nella medesima banca dati o in due diverse banche dati). Se un intruso riesce a determinare (ad esempio mediante un'analisi della correlazione) che due dati sono assegnati allo stesso gruppo di persone, ma non è in grado di identificare alcuna persona del gruppo, la tecnica fornisce una protezione contro l'individuazione, ma non contro la correlabilità;
– (la) *deduzione*, vale a dire la possibilità di desumere, con un alto grado di probabilità, il valore di un attributo dai valori di un insieme di altri attributi.

In sintesi, un efficace processo di anonimizzazione impedisce che il singolo interessato sia individuabile nel gruppo presente nel dataset, che il dato sia collegabile ad altri dati personali della persona all'interno del medesimo dataset e che da quel dato siano deducibili altre informazioni riferibili allo stesso singolo [Comandè 2022, 46 e D'Acquisto, Naldi 2017, 35]. La tecnica scelta per l'anonimizzazione dovrà, pertanto, limitare tutti e tre i rischi menzionati. Si suggerisce dunque di applicare congiuntamente diverse tecniche. Peraltro, l'identificabilità dovrebbe essere eliminata sia per il titolare del trattamento che per ogni altro terzo sogget-

to. Tuttavia, questo approccio assoluto è stato criticato dalla dottrina e, come visto, il caso Breyer della CGUE ha adottato una prospettiva relativistica e contestuale [Finck, Pallas 2020].

L'anonimizzazione, quale risultato di un'attività compiuta sul dato personale, può essere ottenuta attraverso una pluralità di metodologie presenti allo stato dell'arte che differiscono per la modalità con cui l'attribuzione del dato alla persona viene eliminata o resa più improbabile. Già nel 2014, il Gruppo art. 29 individuava le principali famiglie di tecniche nella randomizzazione, che consente di eliminare la correlazione tra i dati e la persona modificando i valori originali, e nella generalizzazione, che diluisce gli attributi dei dati variando la loro scala o l'ordine di grandezza. All'interno di queste famiglie, l'autorità approfondiva le seguenti tecniche:

– l'*aggiunta del rumore statistico*, che appartiene alla famiglia della randomizzazione e consiste nel modificare gli attributi dei dati rendendoli meno accurati grazie ad un programma automatico (ad es., aumentando l'età o l'altezza di una persona). Il rumore consiste in una variabile aleatoria ottenuta da un generatore di numeri pseudocasuali che rende la singola informazione vera meno accurata, mantenendo al contempo l'accuratezza dell'intero set di informazioni [D'Acquisto, Naldi 2017, 71];
– le *permutazioni*, ovvero forme di randomizzazione che mescolano i valori degli attributi in modo da collegarli a più interessati. Gli attributi dei dati perciò rimangono invariati, ma il disaccorpamento associa i valori di Tizio a Caio, scelto causalmente nel dataset. Ciò è vantaggioso per mantenere la correttezza delle analisi a livello aggregato;
– la *privacy differenziale o differential privacy*, che utilizza algoritmi per aggiungere rumore matematico ai dati e aggregarli fin dalla loro raccolta. In particolare, questa tecnica utilizza un algoritmo randomizzato che alle interrogazioni per ottenere informazioni da due dataset che differiscono per i dati di una sola persona fornisce le stesse risposte in cui vi sono elementi di casualità [D'Acquisto, Naldi 2017, 74];
– l'*aggregazione*, quale forma di generalizzazione che raggruppa i dati in numero elevato per impedirne l'individuazione del singolo interessato;
– il *k-anonimato*, dove la k individua la dimensione di un gruppo in cui gli attributi dei singoli non sono distinguibili perché i medesimi attri-

buti sono condivisi da k soggetti. In altre parole, nel gruppo di interessati ci sono k combinazioni di uguali attributi;
– la *l-diversità*, altra forma di generalizzazione che amplia i valori degli attributi in l diversi, e la *t*-vicinanza, che mantiene i dati prossimi agli originali creando classi di equivalenza.

Le tecniche di randomizzazione modificano, quindi, la veridicità dei dati creando incertezza nell'attribuzione del dato alla persona grazie all'introduzione di un elemento casuale, mentre quelle di generalizzazione diluiscono i dati rendendo improbabile tale attribuzione [D'Acquisto, Naldi 2017, 36]. Alla base delle soluzioni vi sono concetti della teoria della probabilità. La tecnica adottata, in aggiunta, dovrebbe essere oggetto di riesame periodico da parte del titolare del trattamento.

Trattandosi di distorsioni, le tecniche di anonimizzazione potrebbero diminuire l'accuratezza e idoneità dei dati alla finalità prescelta. Il titolare del trattamento e il responsabile dovranno perciò valutare se i valori e gli attributi dei dati anonimizzati rimangono utili per la finalità che intendono perseguire o se sia più opportuno mantenere i dati originali e pianificare una loro gestione secondo le regole giuridiche applicabili.

Secondo il Gruppo art. 29, utilizzare un dataset anonimizzato per una finalità, senza cancellare il dataset originale, anche per mera conservazione, non consente di sottrarsi all'applicazione della normativa in materia di dati personali. Certamente, soltanto dati efficacemente anonimizzati potranno essere trattati, e anche condivisi e pubblicati, senza i vari limiti dell'ordinamento. Si potrebbe, perciò, ipotizzare che in alcuni casi non sia possibile minimizzare il dato attraverso l'anonimizzazione. Nei trattamenti per finalità di ricerca, ad esempio, non sempre è possibile definire anticipatamente la necessità di un dato personale per lo scopo dello studio. Si creerebbe in questi casi una sorta di antinomia tra ricerca e minimizzazione.

Il Parere del Gruppo art. 29 del 2014 sulle tecniche di anonimizzazione dovrebbe essere aggiornato alle recenti innovazioni. L'anonimizzazione, come peraltro la pseudonimizzazione, è un concetto dinamico che dipende dall'evoluzione tecnologica [Podda, Palmirani 2021]. Secondo alcuni, inoltre, il concetto di irreversibilità che l'autorità propone è inapplicabile e dovrebbe essere sostituito da quello di impossibilità o comunque da un approccio relativo basato sul rischio [Finck, Pallas 2020]. Una

parte autorevole della dottrina, infatti, sostiene che sia preferibile un approccio basato sul rischio che limita il concetto di identificabilità ad uno standard di ragionevolezza, ossia suggerisce di considerare come anonimizzato il dato che non viene identificato dai mezzi che potrebbero essere ragionevolmente utilizzati per identificare [Weitzenboeck et al. 2022 e Stalla-Bourdillon, Knight 2017]. Tale approccio sarebbe utilizzato anche nel Considerando 26 del GDPR dove si specifica 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. Per accertare la ragionevole probabilità di utilizzo dei mezzi per identificare la persona fisica, si dovrebbe prendere in considerazione l'insieme dei fattori obiettivi, tra cui i costi e il tempo necessario per l'identificazione, tenendo conto sia delle tecnologie disponibili al momento del trattamento, sia degli sviluppi tecnologici.

Adottare un approccio basato sul rischio risulterebbe in linea con quanto è previsto in tema di accountability, di data protection by design e di misure di sicurezza. I dati personali circolano, vengono creati nuovi insiemi di dati e i terzi potrebbero essere in possesso di informazioni che consentono il collegamento tra un dato considerato anonimizzato e un elemento identificativo che re-identifica l'interessato di cui il titolare del trattamento originario non è a conoscenza; di conseguenza, appare molto complesso tracciare i confini tra dati personali e non personali [Finck, Pallas 2020]. Limitarsi a considerare il rischio di ragionevole re-identificazione, invece, significa considerare efficace una tecnica utilizzata che rende l'identificazione non più ragionevolmente probabile.

Si attende sul punto da tempo la pubblicazione di specifiche linee guida da parte dell'EDPB, autorità che ha sostituito il Gruppo art. 29 a partire dal 2018. L'autorità garante è stata recentemente sollecitata dal Parlamento Europeo nella Risoluzione del 25 marzo 2021 su una strategia europea per i dati (2020/2217(INI)) nel fornire chiarezza in materia di anonimizzazione, anche in collaborazione con le istituzioni nazionali.

Come anticipato, ai dati non personali si applica il Regolamento 2018/1807. La Commissione Europea nella Comunicazione «Guidance on the Regulation on a framework for the free flow of non-personal data

in the European Union» del 2019[1] ha chiarito che questo Regolamento è caratterizzato dai seguenti aspetti significativi. Innanzitutto, le sue regole vietano agli Stati membri di imporre obblighi sui luoghi in cui i dati non personali dovrebbero essere localizzati, ad eccezione di esigenze di sicurezza pubblica e nel rispetto del principio di proporzionalità (art. 4, par. 1). Esso poi istituisce un meccanismo di cooperazione per garantire che le autorità possano accedere a dati trattati in un altro Stato membro (art. 5). Si prevedono infine incentivi per l'industria per sviluppare codici di autoregolamentazione – codici di condotta – riguardanti il cambio di fornitore di servizi e la portabilità dei dati.

L'applicazione della normativa è limitata alle attività di trattamento effettuate all'interno dell'Unione che (art. 2):

> a) sono fornite come servizio ad utenti residenti o stabiliti nell'Unione, indipendentemente dal fatto che il fornitore di servizi sia o non sia stabilito nell'Unione, o
> b) sono effettuate da una persona fisica o giuridica residente o stabilito nell'Unione per le proprie esigenze.

Nel caso di un insieme di dati composto sia da dati personali che da dati non personali, ai dati non personali si applica 2018/1807 e a quelli personali il GDPR. Tuttavia, se i dati personali e non personali sono indissolubilmente legati nel dataset, si applicherà il GDPR all'insieme (art. 2).

Il Regolamento 2018/1807 prevede soltanto nove disposizioni. Questa normativa è orientata al principio della libera circolazione dei dati nell'UE; pertanto, un obbligo di localizzazione di dati in una specifica posizione geografica (uno Stato membro) previsto a livello legislativo nazionale per la protezione dei dati ostacolerebbe questa circolazione e viene vietato (art. 4). Eventuali obblighi adottati sulla base di motivi di sicurezza pubblica dovranno essere dichiarati in un portale unico nazionale online di informazione (art. 4, par. 4). Il Regolamento incentiva la messa a disposizione dei dati non personali ad autorità competenti nell'esercizio delle loro funzioni ufficiali (art. 5).

1 Si v. la comunicazione in https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52019DC0250&from=DE.

Con riferimento alla portabilità dei dati, il Regolamento incoraggia l'elaborazione di codici di condotta tra i portatori di interesse, tra i quali già individua start-up, utenti e fornitori di servizi cloud (art. 6). Questi codici dovrebbero regolare vari aspetti dello scambio dei dati tra diversi Stati membri, compresi gli standard di trasmissione e gli obblighi informativi. La procedura di cooperazione tra le autorità nazionali che intendono accedere ai dati comprende richieste formali e la creazione di punti di contatto all'interno di ciascun ordinamento nazionale (art. 7).

L'anonimizzazione, quando possibile, è una tecnica indispensabile per l'adozione dell'approccio di *Open Data* volto alla libera condivisione e il gratuito riuso delle informazioni [Guarda 2021]. La Direttiva europea 2019/1024 sui dati aperti e il riutilizzo delle informazioni del settore pubblico stabilisce delle norme per il riuso dei dati, richiedendo l'anonimizzazione dei dati personali (art. 6). La diffusione di database in accesso aperto tuttavia aumenta i rischi per la protezione dei dati personali perché la re-identificazione opera attraverso più fonti liberamente (e più facilmente) accessibili.

Qualora non sia possibile o utile ottenere un dato anonimizzato, o il rischio di de-identificazione non sia trascurabile, il titolare e il responsabile del trattamento potranno adottare delle tecniche di pseudonimizzazione per mitigare tale rischio e assicurare integrità, confidenzialità e riservatezza dei dati personali.

12.3 La pseudonimizzazione di dati personali

La pseudonimizzazione nel GDPR ed è stata definita come

> 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 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 (art. 4, pt. 14).

Affinché un dato sia pseudonimizzato sono, pertanto, necessarie due condizioni: i) il dato deve subire un processo che elimini il collegamento

con l'interessato senza la necessità di ulteriori informazioni e ii) queste informazioni devono essere conservate separatamente con l'implementazione di specifiche misure a loro protezione [Tosoni 2020].

Questa attività di trattamento è considerata una misura adeguata sia dall'art. 25 sulla data protection by design [vedi → Capitolo 4], come espressione del principio di minimizzazione, sia dall'art. 32 in materia di misure di sicurezza [vedi → Capitolo 3]. Il GDPR considera, infatti, la pseudonimizzazione come una misura adeguata a mitigare il rischio che il trattamento comporta (Cons. 28). L'art. 40 del GDPR sui codici di condotta inserisce la pseudoanonimizzazione tra gli aspetti che possono essere precisati in un codice da parte delle associazioni e degli altri organismi rappresentanti le categorie di titolari o responsabili del trattamento (art. 40, par. 2, lett. d) GDPR) [vedi → Capitolo 3]. L'art. 89 del GDPR sulle garanzie e deroghe relative al trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici [vedi → Capitolo 16] utilizza la pseudoanonimizzazione come esempio di misure attuative del principio di minimizzazione dei dati.

Come definisce l'«European Union Agency for Cybersecurity» (ENISA) nel documento «Tecniche di pseudonimizzazione e migliori pratiche del 2019» lo pseudonimo o «nome in codice» è «un'informazione associata all'identificativo di un individuo o ad altri tipi di dati personali»[2]. La pseudonimizzazione si ottiene tramite la sostituzione di un attributo univoco di un dato, ossia l'identificativo, con un altro ugualmente univoco e non immediatamente intellegibile, lo pseudonimo [D'Acquisto, Naldi 2017, 38]. La non immediatezza dell'identificabilità tutela la confidenzialità del dato. Il dato pseudonimizzato è, e rimane, un dato personale. La funzione di recupero è infatti in grado di sostituire lo pseudonimo con l'identificativo.

La principale soluzione per pseudonimizzare i dati personali è la crittografia o cifratura, la quale utilizza una o più chiavi – in concreto sequenza di bit – generate da specifici algoritmi e che codificano o decodificano le informazioni [D'Acquisto, Naldi 2017, 117-118]. Attualmente le chiavi crittografiche sono di regola composte da 128 bit. A titolo di esempio, un messaggio di testo può essere crittografato grazie ad un algoritmo che

2 Il contributo è consultabile presso https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices_it/at_download/file.

ne codifica il contenuto, impedendo ad un soggetto esterno di leggerlo senza l'utilizzo di una chiave che lo decodifichi. Soltanto quel destinatario in possesso della chiave potrà decodificare il messaggio originario.

Le soluzioni crittografiche vengono generalmente suddivise tra tecniche a chiave privata o simmetrica e tecniche a chiave pubblica o asimmetrica. Nel primo caso il mittente e il destinatario di un messaggio utilizzano la stessa chiave per cifrare e decifrare e tale chiave è associata soltanto alla loro identità [D'Acquisto, Naldi 2017, 120-127]. Se il mittente intende inviare un altro messaggio ad un diverso destinatario, infatti, utilizzerà una chiave differente. Questo schema garantisce la riservatezza del messaggio, ma richiede un gran numero di chiavi per tutte le possibili coppie di utenti e impone l'assoluta segretezza delle chiavi di cui si dispone. Nel secondo caso, invece, ogni soggetto dispone di due chiavi, di cui una pubblica, ossia conoscibile all'esterno, e una privata. Tali chiavi potranno essere utilizzate per qualsiasi destinatario. Il mittente dovrà codificare il messaggio con la chiave pubblica del destinatario, che potrà poi usare la sua chiave privata per decifrarlo. Soltanto lui potrà farlo.

Il report «Data Pseudonymisation: advanced techniques & use cases» dell'European Union Agency for Cybersecurity del 2021 fornisce un'utile guida pratica in materia di pseudonimizzazione e protezione dei dati personali riferendosi al più recente stato dell'arte delle soluzioni adottabili. A titolo di esempio, la crittografia omomorfica o *homomorphic encryption* è una tecnica di cifratura che consente a una terza parte (come un fornitore di servizi cloud) di eseguire determinati calcoli sui testi cifrati senza conoscere la relativa chiave di decifrazione. Secondo l'agenzia quando si implementa una tecnica di pseudonimizzazione è importante chiarire in primo luogo lo scenario applicativo, ossia il contesto di trattamento, e i diversi ruoli coinvolti, in particolare identificare l'entità che in concreto procederà alla separazione degli attributi, che infatti può essere sia il responsabile del trattamento che una terza parte. In ogni specifico contesto sarà quindi necessario considerare la migliore tecnica presente nello stato dell'arte, valutando i vantaggi e le insidie che comporta. Ovviamente, non esisterà un approccio univoco, ossia l'analisi dei rischi deve essere effettuata caso per caso in ottica di accountability.

Oltre alla crittografia simmetrica, l'ENISA suggerisce l'utilizzo delle seguenti tecniche «di base»:

– *contatore*, quale funzione che sostituisce gli identificatori dei dati con un numero scelto da un contatore monotono. Si tratta di una tecnica semplice che fornisce pseudonimi senza alcun legame con gli identificatori iniziali. Tuttavia, questa soluzione è utile per piccoli dataset, ma può presentare problemi di implementazione e scalabilità per maggiori quantità di informazioni e la sequenzialità dei numeri attribuiti potrebbe rivelare elementi sui dati anche in casi minori;
– *generatore di numeri casuali*, che è simile al contatore, con la differenza che all'identificatore viene assegnato un numero casuale. Questa soluzione offre una forte protezione ai dati, ma potrebbero sorgere problemi di scalabilità;
– *funzione crittografica di hash*, quale funzione che si applica direttamente a un identificatore di input per ottenere lo pseudonimo corrispondente in modo unidirezionale («è computazionalmente impraticabile trovare input che si associno a output specificati in precedenza») e senza collisioni di output («è computazionalmente impraticabile trovare due input distinti che si associno al medesimo output»). Come si vedrà, la funzione di hash è usata per lo sviluppo di una blockchain [vedi → Capitolo 17].

Con riferimento a quest'ultima soluzione l'EDPS e l'Autorità garante spagnola AEPD hanno pubblicato il contributo «Introduction to the hash function as a personal data pseudonymisation technique»[3]. Le due istituzioni chiariscono che la funzione di *hash* è un processo che trasforma dei dati in ingresso in una serie di caratteri a lunghezza fissa detta anche «codice hash». Il termine *hash* è spesso utilizzato sia per indicare la funzione che il valore ottenuto in output[4]. Il dato iniziale viene quindi tradotto in una serie di bit, una stringa, che non lo rende immediatamente identificabile. Oltre al testo, una funzione di *hash* può applicarsi a immagini, video, file.

3 Il contributo è disponibile in inglese presso: https://edps.europa.eu/data-protection/our-work/publications/papers/introduction-hash-function-personal-data_en.

4 Ad esempio, applicando al termine «hello» la funzione «SHA256» si ottiene il seguente codice: 104123755207289804956272089233072171500574028163694787093464498999073160165519.

Così come per l'anonimizzazione, per applicare tecniche di pseudonimizzazione dovrà essere valutato il concreto contesto di trattamento; non è, quindi, possibile indicare un'unica soluzione per tutti gli scenari possibili e l'approccio dovrà essere valutato in base al rischio. Per entrambe le soluzioni il titolare del trattamento dovrà essere supportato da responsabili del trattamento di elevata competenza che adottino livelli di protezione adeguati allo stato dell'arte.

12.3 Casi 12-1, 12-2, 12-3

Caso 12-1

La società di produzione Alfa, stabilita in Francia, raccoglie i dati sulla qualità e sulla popolarità dei suoi prodotti per indagini statistiche sulle sue vendite. Questi dati vengono raccolti tramite questionari somministrati via e-mail ai clienti e vengono poi riportati in sintesi in report interni che considerano la provenienza territoriale degli ordini.
Quali tipologie di dati raccoglie Alfa?
Alle attività di Alfa si applicherà la normativa a protezione dei dati personali?
Se sì, quali tecniche Alfa potrebbe adottare per escludere l'applicazione del GDPR?
Se no, quale normativa si applicherà?

Caso 12-2

La banca Beta, stabilita in Svizzera eroga servizi bancari a cittadini di tutta l'Unione europea. Beta raccoglie le informazioni sui clienti, sia persone fisiche che giuridiche, i dettagli delle transazioni delle carte di credito e debito a loro intestate, i documenti sui contratti finanziari e di prestito. La banca inoltre utilizza i dati aggregati delle transazioni per tenere monitorato l'andamento finanziario della società.
Quali tipologie di dati raccoglie Beta?
Alle attività di Beta si applicherà la normativa a protezione dei dati personali?
Se sì, quali tecniche potrebbe adottare per escludere l'applicazione del GDPR? Se no, quale normativa si applicherà?

Caso 12-3

Il fornitore di servizi in cloud Gamma, stabilito negli Stati Uniti, offre servizi a clienti residenti nell'Unione europea. Gamma affitta server situati nel Regno Unito e in Polonia per conservare i dati che i suoi clienti europei caricano sulle cartelle in cloud. La maggior parte dei clienti di Gamma sono imprese e società commerciali, che conservano dati sui loro clienti e dipendenti.
Quali tipologie di dati raccoglie Gamma?
Alle attività di Gamma si applicherà la normativa a protezione dei dati personali?
Se sì, quali tecniche potrebbe adottare per escludere l'applicazione del GDPR?
Se no, quale normativa si applicherà?

CAPITOLO 13.
Big Data, intelligenza artificiale e protezione dei dati personali

Paolo Guarda

13.1 Tra Big Data ed intelligenza artificiale

Società dell'informazione, era dei dati, infosfera, nuovo petrolio del ventunesimo secolo [Floridi 2012 e Floridi 2017]. Le espressioni suggestive per tratteggiare il nuovo contesto storico e l'importanza che i dati stanno in esso acquisendo si sprecano.

La raccolta e lo «stoccaggio» dei dati è attività continua, incessante, inesorabile. I dati vengono prodotti dalle nostre interazioni con le piattaforme online, con gli strumenti di uso quotidiano (frigoriferi, assistenti virtuali, televisioni, telefonini: il fenomeno dell'Internet of Things (IoT) è oramai pervasivo [Giovanella 2019; vedi → Capitolo 14], con i mezzi di trasporto o derivano da misurazione di fenomeni naturali (meteo, inquinamento, ecc.). Le informazioni che da tali dati vengono estratte concorrono a loro volta a costituire silos, ossia contenitori, basi di dati che serviranno nella continua interazione con nuove fonti, per creare nuovi dati, nuova informazione, e si spera nuova conoscenza.

Per descrivere tale fenomeno si fa spesso riferimento al termine «Big Data» [Mantelero 2017 e Mantelero 2016]: grazie alle nuove tecnologie digitali ed ai sistemi di ricerca e comunicazione abbiamo ora a disposizione enormi quantità di dati cui si associano capacità computazionali sempre più sorprendenti. Dati che vengono da fonti differenti possono essere assemblati, analizzati, inferiti seguendo traiettorie sempre nuove ed inesplorate.

Il concetto di Big Data, inoltre, è multiforme ed è di regola connesso ad altri fenomeni: l'«open data» (accesso ai dati libero da barriere di carattere tecnico, economico o giuridico), il «cloud computing» (la gestione dell'archiviazione dei dati), la profilazione (in special modo se connessa all'uso di tecniche di intelligenza artificiale), la sorveglianza sociale di carattere pubblico o privato, in particolare quando i dati provengono da IoT, ecc. [Palmirani 2020, 74].

Gli approcci per descrivere questa categoria in letteratura sono variegati [Leonelli 2020, 19]; un possibile punto di partenza è [De Mauro, Greco, Grimaldi 2016, 122]:

> the information asset characterized by such a high volume, velocity and variety to require specific technology and analytical methods for its transformation into value.

Gli elementi caratterizzanti sono andati via via aggiungendosi per meglio definire i contorni (con l'effetto, però, di renderli anche meno chiari). Si ricorre, spesso, ad una elencazione di qualità che iniziano con la lettera «V» e si parla di tre, cinque, sette V, a seconda dell'autore che si consulta [Sætnan, Schneider, Green 2018 e Borgmann 2015]. All'inizio si impose un primo modello definitorio che si basava su «3 V»:

– *Volume*: si riferisce alla quantità di dati generati ed alla loro dimensione;
– *Varietà*: si riferisce alla differente tipologia dei dati che vengono generati, accumulati ed utilizzati (dati in formati non-digitali, in formato digitale, ma non facilmente analizzabili tramite algoritmi, dati strutturati e non strutturati, ecc.);
– *Velocità*: si riferisce alla velocità con cui i nuovi dati vengono generati.

Con il passare del tempo le «V» sono diventate cinque, comprendendo:

– *Veridicità*: la qualità dei dati acquisiti può variare notevolmente, influenzando l'accuratezza dell'analisi;
– *Valore*: si riferisce alla capacità di trasformare i dati in valore, eventualmente a questi assegnato da settori diversi della società, in contesti spazio-temporali che possono variare.

Ma gli autori fanno riferimento anche ad altre caratteristiche quali:
– *Variabilità*: l'incoerenza del set di dati può ostacolare i processi per gestirlo;
– *Validità*: i dati possono essere validi o meno rispetto ai modi in cui vengono analizzati;
– *Volatilità nel tempo*: i set di dati possono avere differenti capacità di rimanere affidabili e leggibili nonostante l'evoluzione di nuove tecnologie di archiviazione;
– *Visualizzazione*: si fa riferimento alle metodologie di visualizzazione dei dati che possono agevolare la comprensibilità, in special modo per il consumo umano;
– *Vulnerabilità*: si riferisce ai possibili problemi di sicurezza creati dalla gestione dei Big Data.

Un altro fenomeno che sicuramente entra in gioco, e che anzi trova la propria linfa in tale contesto, è quello relativo all'implementazione di sistemi di «Intelligenza Artificiale» (IA) [Barfield, Pagallo 2020]. Esistono molte versioni, definizioni e concetti di IA. Puristi e tecnici del settore discutono su ciò che possa essere veramente inteso come «intelligente» e su ciò che non lo è affatto, o su quale sia la terminologia corretta per fare riferimento a questo tipo di tecnologia [Legg, Hutter 2007]. Si distingue allora tra intelligenze virtuali c.d. «deboli» (quali ad esempio alcuni assistenti virtuali, come Siri o Google Assistant), progettate per organizzare informazioni e rispondere a domande in un contesto relativamente limitato, e altre forme, invece, chiamate «forti», le quali secondo molti sarebbero semplicemente al di là delle attuali possibilità tecniche e apparirebbero come possibili scenari futuri. Senza alcuna pretesa di risolvere la controversia terminologica, possiamo fare riferimento, tra le tante, alla definizione proposta dalla Comunicazione della Commissione europea su «Intelligenza artificiale per l'Europa» del 25 aprile 2018:

> L'intelligenza artificiale (IA) si riferisce a sistemi che mostrano comportamenti intelligenti analizzando il loro ambiente e prendendo azioni – con un certo grado di autonomia – per raggiungere obiettivi specifici.

Il termine IA è, in generale, applicato quando una macchina imita le funzioni «cognitive» che noi associamo ad altre menti umane, come l'apprendimento e la risoluzione di problemi (più o meno complessi).

La Commissione ha recentemente presentato una proposta di regolamento: «Proposal for a Regulation of the European Parliament and of the Council laying down Harmonized Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending certain Union Legislative Act», Brussels, del 21 aprile 2021. Essa rappresenta il primo quadro giuridico in tema di IA mai realizzato in Europa, e un piano - coordinato con gli Stati membri - per garantire la sicurezza e i diritti fondamentali di cittadini e imprese, che rafforzi, nel contempo, l'adozione della tecnologia e gli investimenti e l'innovazione nel settore in tutta l'UE. Le nuove norme seguono un approccio basato sul rischio («rischio inaccettabile», «alto rischio», «rischio limitato» o «rischio minimo») [Malgieri, Pasquale 2022]. L'art. 3, pt. 1, ci propone una nuova definizione di IA:

> «artificial intelligence system» (AI system) means software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with.

Le applicazioni che riguardano i sistemi di IA sono innumerevoli e caratterizzate dalla eterogeneità dei settori coinvolti, tanto che risulta difficile una loro catalogazione completa. A livello industriale esse concorrono ad individuare quella che prende il nome di «industria 4.0». La programmazione automatica è uno di questi settori, in special modo nel contesto della continua evoluzione nel controllo a distanza di automobili a guida autonoma [Brock 2015]. Alla base di questa si trovano, infatti, complessi algoritmi che sono in grado di prendere decisioni, come frenare o sterzare in determinate circostanze, oltre che guidare l'automobile stessa. Si registrano, poi, applicazioni anche in ambito giudiziario [Palmirani, Sapienza 2022, Noto La Diega 2018, 16-24 e Noto La Diega 2016, 394-400]. Infine, un altro settore in cui l'IA ha un impatto notevole è quello medico, dove l'uso di strumenti dotati di sistemi intelligenti può realizzare non solo una maggiore equità nell'accesso alle strutture sanitarie, ma anche un complessivo miglioramento delle prestazioni stesse,

che si riflette in un livello di salute, individuale e collettiva, più elevato [Guarda, Petrucci 2020 e Guarda 2019] [Si veda → Capitolo 15].

13.2 Protezione dei dati personali e intelligenza artificiale

L'utilizzo dell'IA e, in generale, degli algoritmi che ne determinano l'azione è ovviamente al centro dell'attenzione anche nel campo della protezione dei dati.

Da un punto di vista normativo, l'origine della disciplina risale alla legge francese sulla protezione dei dati del 1978 («Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux liberté»). Nella sua versione originale, l'art. 2 vietava decisioni giudiziarie, amministrative o di carattere personale riguardanti la valutazione del comportamento umano nella misura in cui fossero basate esclusivamente su trattamenti automatizzati di dati volti a definire il profilo o la personalità dell'interessato.

A livello di fonti europee, il primo riferimento normativo è rappresentato dall'art. 15 della Direttiva 95/46/CE:

> 1. Gli Stati membri riconoscono a qualsiasi persona il diritto di non essere sottoposta ad una decisione che produca effetti giuridici o abbia effetti significativi nei suoi confronti fondata esclusivamente su un trattamento automatizzato di dati destinati a valutare taluni aspetti della sua personalità, quali il rendimento professionale, il credito, l'affidabilità, il comportamento, ecc.
> 2. Gli Stati membri dispongono, salve le altre disposizioni della presente direttiva, che una persona può essere sottoposta a una decisione di cui al paragrafo 1, qualora una tale decisione:
> a) sia presa nel contesto della conclusione o dell'esecuzione di un contratto, a condizione che la domanda relativa alla conclusione o all'esecuzione del contratto, presentata dalla persona interessata sia stata accolta, oppure che misure adeguate, fra le quali la possibilità di far valere il proprio punto di vista garantiscano la salvaguardia del suo interesse legittimo, oppure
> b) sia autorizzata da una legge che precisi i provvedimenti atti a salvaguardare un interesse legittimo della persona interessata.

Il recepimento nazionale di tale articolo è stato caratterizzato da notevoli divergenze. Alcuni Stati membri, infatti, l'avevano inteso come un diritto da esercitare a discrezione di ciascuna persona: consentendo così che il processo decisionale potesse avvenire anche in assenza dell'esercizio di tale diritto, a condizione che l'operazione di trattamento dei dati avesse soddisfatto gli altri requisiti di legge (si veda ad es. la sezione 29 Swedish Personal Data Act 1992, in seguito abrogato). Questa forma di trasposizione si conformava strettamente al testo dell'art. 15, par. 1. Altri Stati avevano, invece, optato per l'affermazione di un esplicito divieto di processi decisionali automatizzati (si veda, ad es., l'art. 12.*bis* Belgian Data Protection Law del 1992, poi abrogato). Altri ancora avevano adottato un approccio ibrido, creando un divieto per alcuni tipi di decisione ed un diritto di opporsi per altri (si veda art. 14, Codice Privacy italiano) [Bygrave 2020a, 529].

Il GDPR dedica un articolo *ad hoc* al trattamento unicamente automatizzato [Pierucci 2019, 436-445 e Bygrave 2020a]. L'art. 22, par. 1, infatti, esordisce con un divieto di carattere generale:

> 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.

Sul punto aveva già avuto occasione di intervenire il Gruppo art. 29 attraverso le «Linee guida sul processo decisionale individuale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del Regolamento 2016/679» adottate il 3 ottobre 2017 e da ultimo riviste il 6 febbraio 2018 (di seguito: «Linee Guida sui processi decisionali automatizzati»). In questo documento veniva sottolineata l'importanza di due concetti in materia di protezione dei dati personali: «accountability», tema chiave del GDPR e nuova bussola dell'azione del titolare, e «trasparenza», principio che dovrebbe essere alla base di tutte le attività relative al trattamento dei dati personali.

Sottolineiamo alcuni passaggi fondamentali della nuova previsione europea. Anzitutto, il divieto si applica alle decisioni che si basano «unicamente» su trattamenti automatizzati: occorre, quindi, che l'eventuale intervento umano, se presente, sia del tutto marginale e che quindi

la «macchina» abbia processato in modo del tutto autonomo i dati e sia giunta, in modo altrettanto indipendente ad una decisione. Le Linee Guida sui processi decisionali automatizzati raccomandano di trattare questo diritto come un divieto generale. Esso, poi, può essere fatto valere solo se la decisione «produce effetti giuridici» nei confronti dell'interessato «o incida in modo analogo significativamente sulla persona». La nozione di «effetto giuridico» comprende tutti gli scenari in cui una decisione possa pregiudicare i diritti di un soggetto, quali ad esempio la libertà di associarsi altre persone, di votare nel contesto di una elezione, di intraprendere azioni legali. Può, inoltre, succedere allorquando la decisione possa influire sullo status giuridico di una persona o sui suoi diritti derivanti da un contratto: si pensi al caso della concessione o negazione del diritto ad ottenere l'indennità di alloggio o prestazione per figli a carico, al rifiuto di ammissione in un paese o alla negazione della cittadinanza, alla risoluzione di un contratto (Linee Guida sui processi decisionali automatizzati, 23).

L'espressione, invece, «in modo analogo» associata a «incida significativamente» indica che gli effetti del trattamento considerato devono essere sufficientemente rilevanti ed esser in grado di incidere in maniera significativa sulle circostanze, sul comportamento o sulle scelte dell'interessato; avere un impatto prolungato e permanente su questo; o addirittura portare all'esclusione o alla discriminazione di persone (Linee Guida sui processi decisionali automatizzati, 24). Il Considerando 71 propone alcuni esempi:

> il rifiuto automatico di una domanda di credito online o pratiche di assunzione elettronica senza interventi umani.

La previsione normativa fa, inoltre, direttamente riferimento al concetto di «profilazione». Questo passaggio merita un approfondimento perché potrebbe indurre in alcuni errori applicativi. La definizione di «profilazione» è fornita dall'art. 4, punto 4, GDPR:

> 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 situa-

> zione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica.

La mera classificazione di un individuo sulla base di caratteristiche note non determina di per sé una profilazione, ma ciò dipenderà semmai dallo scopo della classificazione stessa. Il divieto di cui all'art. 22, par. 1, inoltre, non si applicherà direttamente al solo ricorrere di un'attività di profilazione, rimanendo condizione imprescindibile che il processo automatizzato sia posto in essere in modo del tutto autonomo da parte della macchina e senza alcun intervento di carattere umano.

Confermando una consueta tecnica di drafting normativo del legislatore europeo, il secondo paragrafo dell'art. 22 prevede alcune eccezioni al divieto generale, il quale non si applica nel caso in cui la decisione:

> a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento;
> b) sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato;
> c) si basi sul consenso esplicito dell'interessato.

Nel caso in cui il processo decisionale riguardi, poi, categorie particolari di dati, ai sensi del quarto paragrafo dell'art. 22 il divieto non si applicherà nel caso in cui:

– l'interessato abbia espresso il proprio consenso esplicito (ex art. 9, par. 1, lett. a)), con tutte le difficoltà relative agli obblighi informativi connessi al trattamento nel contesto di un processo intrinsecamente non trasparente in quanto caratterizzato dal c.d. fenomeno delle «black box»; o
– il trattamento sia 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 (art. 9, par. 1, lett. g));

– e in ogni caso il titolare abbia adottato misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato.

Il paragrafo 3 dell'art. 22, infine, prevede gli obblighi connessi a tale trattamento in capo al titolare:

> Nei casi di cui al paragrafo 2, lettere a) e c), 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.

Qualora, quindi, il processo decisionale unicamente automatizzato sia basato sulla necessità di concludere od eseguire un contratto o sul consenso esplicito dell'interessato, il titolare del trattamento dovrà applicare appunto misure appropriate e in particolare riconoscere alcuni diritti fondamentali agli interessati i quali dovranno, quindi, sempre godere del diritto di ottenere l'intervento umano, di esprimere il proprio punto di vista e di impugnare la decisione. È, dunque, essenziale che queste previsioni siano incorporate fin dall'inizio anche nelle architetture digitali che gestiscono questi processi (in un'ottica di data protection by design). Soprattutto in contesti particolarmente sensibili quali ad esempio quello medico, si pongono problematiche di carattere etico legate al ruolo di questo c.d. «man in the loop» e alla reale libertà che questi abbia di discostarsi dalla decisione della macchina.

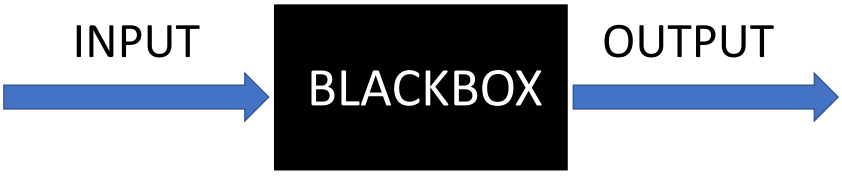
Si ritiene, infine, che quanto previsto dal terzo paragrafo si applichi in special modo ai trattamenti legittimati dalle eccezioni previste nel caso di categorie particolari di dati; anzi si può a ragione sostenere che il legislatore avrebbe dovuto adottare una sequenza logica più coerente nel paragrafare questo articolo.

13.3 Intelligenza artificiale, trasparenza e obblighi informativi

Un «peccato originale» che affligge l'IA, soprattutto nei contesti in cui il trattamento dei dati personali diventa cruciale, è legato al fatto che il «come» e il «perché» del suo funzionamento non appaiano così chiaro

o immediatamente comprensibili. Tipicamente, non è agevole determinare e spiegare il processo che ha portato tali tecnologie a raggiungere determinate conclusioni [Burrell 2016]. Il quadro diviene ancora più complesso se consideriamo che in alcune metodologie utilizzate, quali quelle di «machine learning», i dati via via processati vengono utilizzati al fine di migliorare le previsioni future, e soprattutto per modificare gli stessi algoritmi che fanno funzionare il sistema. Tali algoritmi, pertanto, non solo si caratterizzano per opacità, ma sono pure soggetti a modifica nel tempo.

Si ricorre, così, all'evocativa espressione delle c.d. «black box» al fine di meglio spiegare tale fenomeno [Pasquale 2015]. Il termine, spesso citato in informatica e ingegneria, indica un sistema che, similmente ad una «scatola nera», è essenzialmente descrivibile nei suoi aspetti esteriori, cioè solo per come reagisce in uscita ad un determinato input, ma il cui funzionamento interno non è visibile o è sconosciuto.



Si possono identificare tre diversi tipi di black box [Noto la Diega 2016, 9-10 e 11-16]:

– organizzative: gli algoritmi sono spesso implementati da soggetti privati che massimizzano il profitto e che operano con obblighi di trasparenza minimi: quindi, non ci sono incentivi reali che li spingano a meglio chiarire le modalità di trattamento delle informazioni;
– tecnologiche: l'IA rende spesso la logica delle decisioni intrinsecamente difficile da raggiungere (si pensi alle cosiddette «reti neurali» che sono modellate sul cervello umano);
– giuridiche: l'applicazione di diritti di proprietà intellettuale (si pensi anzitutto al segreto commerciale) può avere un impatto sulla gestione, e sulla trasparenza, di tali tecnologie.

Questa intrinseca mancanza di trasparenza ha forti ripercussioni sulla questione dell'accountability, principio che abbiamo visto ispirare e caratterizzare l'approccio GDPR. Garantire un trattamento equo, lecito e

trasparente diventa, quindi, molto difficile, tenuto conto di quanto questi sistemi operino in ambienti di apprendimento automatico, integrati in flussi operativi più generali, e coinvolgono dati provenienti da fonti diverse e con diversi gradi e livelli di affidabilità [Kuner et al. 2017].

Come già si ricordava, la trasparenza può essere annoverata tra i principi fondanti del GDPR. Il trattamento dei dati personali deve essere reso il più possibile intelligibile per l'interessato. Lo strumento principale diviene, quindi, l'informativa. Il trattamento può considerarsi equo e trasparente solo se viene fornita una specifica informativa, che riguarda, tra gli altri, essenzialmente i seguenti aspetti (art. 13, par. 2, lett. f)):

> l'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.

Il c.d. «right to explanation» può assumere significati diversi, a seconda del contesto a cui si riferisce [Wachter, Mittelstadt, Floridi 2017, 78-79]:

– «funzionalità di sistema»: si concentra quindi sulla logica, sul significato, sulle conseguenze attese e sulle funzionalità generali di un sistema decisionale automatico (es. specificazione dei requisiti di sistema, alberi decisionali, criteri, ecc.);
– «decisioni specifiche»: riguarda qui la logica, le ragioni, le circostanze individuali di una specifica decisione automatizzata (es. ponderazione delle caratteristiche, regole decisionali specifiche del caso definite da una macchina, ecc.).

La spiegazione può, inoltre, intervenire in due momenti distinti:

– *ex ante*: avviene prima che sia messo in atto il processo decisionale automatizzato (in questo caso riguarda le sole funzionalità del sistema);
– *ex post*: si verifica dopo l'attuazione di un processo decisionale automatizzato (può concernere sia la funzionalità del sistema che la logica della decisione specifica).

Alcuni autori hanno criticamente osservato che il diritto alla spiegazione non sarebbe esplicitamente menzionato nell'articolato del GDPR e la

sua omissione sarebbe intenzionale, trovando spazio solo nel Considerando 71 [Wachter, Mittelstadt, Floridi 2017, 79 ss.]:

> In ogni caso, tale trattamento dovrebbe essere subordinato a garanzie adeguate, che dovrebbero comprendere la specifica informazione all'interessato e il diritto di ottenere l'intervento umano, di esprimere la propria opinione, di ottenere una spiegazione della decisione conseguita dopo tale valutazione e di contestare la decisione.

Un *right to explanation* potrebbe essere fondato su più basi giuridiche.

Questo potrebbe derivare, anzitutto, dall'obbligo in capo al titolare del trattamento di adottare misure idonee a tutelare i diritti, le libertà e i legittimi interessi dell'interessato secondo quanto stabilito dal già citato art. 22, par. 3, GDPR.

Il diritto in questione può essere, inoltre, ricostruito sulla base degli obblighi di notifica di cui agli articoli 13 e 14 come specificati dai considerando 60-62. In particolare, il secondo paragrafo di entrambi gli articoli precisano che i titolari del trattamento devono fornire all'interessato alcune ulteriori informazioni necessarie a garantire un trattamento corretto e trasparente.

Secondo il Gruppo art. 29, la spiegazione relativa alla «logica utilizzata» includerebbe anche i dettagli sulle ragioni di base, o sui criteri sottostanti, utilizzati al fine di giungere alla decisione, senza necessariamente tentare una spiegazione complessa degli algoritmi utilizzati o una divulgazione dell'intero algoritmo (Linee Guida sui processi decisionali automatizzati, 28-29). Non è ovviamente possibile apprestare un'informativa privacy in grado di coprire qualsiasi tipo di tecnologia di apprendimento automatico o di intelligenza artificiale. Essa dovrebbe, però, almeno delineare le principali caratteristiche, la fonte delle informazioni che hanno fatto da base per il processo decisionale e la loro rilevanza.

Infine, un altro riferimento al diritto a ricevere una spiegazione può essere individuato nel diritto di accesso previsto dall'art. 15 GDPR, che riprende la stessa formulazione degli artt. 13, par. 2, lett. f), e 14, par. 2, lett. h) e stabilisce che l'interessato ha il diritto di ottenere l'accesso alle seguenti informazioni [Wachter, Mittelstadt, Floridi 2017, 83-84]:

> l'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.

Si registra, dunque, un dibattito sull'esistenza o meno nell'ambito del GDPR di un diretto e specifico diritto alla spiegazione (un *right to explanation*) in capo all'interessato. Il confinamento nei Considerando del riferimento esplicito a tale previsione, determinatosi durante l'iter di approvazione del Regolamento europeo, porterebbe ad affermare che esso non sia ad oggi di natura cogente [Edward, Veale 2017]. Da una prospettiva di più ampia veduta, però, è probabilmente sostenibile un'interpretazione dei diritti di informazione previsti dal GDPR relativamente ai processi decisionali automatizzati (quanto al significato e alle conseguenze della decisione) tale da far riconoscere un vero e proprio diritto alla spiegazione. Ragionare a contrario presenterebbe possibili rischi e, soprattutto, potrebbe determinare un abbassamento delle garanzie riconosciute all'interessato, vanificando il potenziale effetto della nuova normativa europea in materia di protezione dei dati personali [Malgieri, Comandè 2017 e Noto la Diega 2016, 23-24]. Le corti, europee e nazionali, potrebbero sfruttare queste brecce ed ampliare la portata degli obblighi informativi in tali scenari applicativi.

13.4 Casi giurisprudenziali

La CGUE non ha ancora avuto occasione di pronunciarsi direttamente con riferimento all'art. 22 GDPR, né lo aveva mai fatto prima con riferimento all'art. 15 della Direttiva 95/46/CE [Bygrave 2020a, 529].

Nel Parere 1/15 del 26 luglio 2017 (Grande Sezione) essa aveva affrontato marginalmente la questione nell'ambito dell'analisi di un progetto di accordo sui codici di prenotazione dei passeggeri (Passenger Name Record – PNR) tra UE e Canada:

> nei limiti in cui le analisi automatizzate dei dati PNR comportano necessariamente, com'è stato constatato al punto 169 del presente parere, un certo tasso d'errore, qualsiasi risultato positivo ottenuto a seguito di un trattamento automatizzato di detti dati, in forza dell'articolo 15 dell'accordo previsto, deve essere sottoposto a un riesame in-

> dividuale con strumenti non automatizzati prima dell'adozione di una misura individuale che produca effetti pregiudizievoli nei confronti dei passeggeri aerei interessati. Così, una siffatta misura non può, in forza di tale articolo 15, essere fondata in modo determinante soltanto sul risultato di un trattamento automatizzato dei dati PNR.

A livello di corti nazionali, nel 2014, la Corte federale di giustizia tedesca (*Bundesgerichtshof*) ha pronunciato una sentenza in una causa che ha riguardato la portata delle norme tedesche di recepimento dell'art. 15 DPD. Il caso riguardava l'uso di sistemi automatizzati di «credit scoring». Il giudice ha ritenuto che il sistema decisionale impugnato esulasse dall'ambito di applicazione delle norme in questione in quanto la decisione finale relativa all'erogazione del credito veniva presa da una persona e quindi non si trattava di un processo completamente automatizzato (*Bundesgerichtshof*, URteil vom 28.01.2014, para. 34) [Bygrave 2020a, 529, nt. 18].

Da ultimo nel contesto italiano il Consiglio di Stato (sez. VI, 8 aprile 2019, n. 2270, in *Foro it*., 2019, III, 606) ha avuto l'occasione di pronunciarsi sul punto. Il problema di fondo verteva sul fatto se fosse legittima una procedura amministrativa che, per formulare proposte di assunzione a tempo indeterminato di docenti della scuola pubblica, individuava i ruoli e le sedi mediante un algoritmo il cui funzionamento rimaneva di fatto sconosciuto [Cavallaro, Smorto 2019 e Caso 2021, 296-299]. La corte amministrativa italiana così sosteneva:

> In primo luogo, come già messo in luce dalla dottrina più autorevole, il meccanismo attraverso il quale si concretizza la decisione robotizzata (ovvero l'algoritmo) deve essere «conoscibile», secondo una declinazione rafforzata del principio di trasparenza, che implica anche quello della piena conoscibilità di una regola espressa in un linguaggio differente da quello giuridico.
> Tale conoscibilità dell'algoritmo deve essere garantita in tutti gli aspetti: dai suoi autori al procedimento usato per la sua elaborazione, al meccanismo di decisione, comprensivo delle priorità assegnate nella procedura valutativa e decisionale e dei dati selezionati come rilevanti. Ciò al fine di poter verificare che gli esiti del procedimento robotizzato siano conformi alle prescrizioni e alle finalità stabilite dalla legge o dalla stessa amministrazione a monte di tale procedimento e affin-

ché siano chiare – e conseguentemente sindacabili – le modalità e le regole in base alle quali esso è stato impostato.
In altri termini, la «caratterizzazione multidisciplinare» dell'algoritmo (costruzione che certo non richiede solo competenze giuridiche, ma tecniche, informatiche, statistiche, amministrative) non esime dalla necessità che la «formula tecnica», che di fatto rappresenta l'algoritmo, sia corredata da spiegazioni che la traducano nella «regola giuridica» ad essa sottesa e che la rendano leggibile e comprensibile, sia per i cittadini che per il giudice.
In secondo luogo, la regola algoritmica deve essere non solo conoscibile in sé, ma anche soggetta alla piena cognizione, e al pieno sindacato, del giudice amministrativo.
La suddetta esigenza risponde infatti all'irrinunciabile necessità di poter sindacare come il potere sia stato concretamente esercitato, ponendosi in ultima analisi come declinazione diretta del diritto di difesa del cittadino, al quale non può essere precluso di conoscere le modalità (anche se automatizzate) con le quali è stata in concreto assunta una decisione destinata a ripercuotersi sulla sua sfera giuridica.
Solo in questo modo è possibile svolgere, anche in sede giurisdizionale, una valutazione piena della legittimità della decisione; valutazione che, anche se si è al cospetto di una scelta assunta attraverso una procedura informatica, non può che essere effettiva e di portata analoga a quella che il giudice esercita sull'esercizio del potere con modalità tradizionali.
In questo senso, la decisione amministrativa automatizzata impone al giudice di valutare in primo luogo la correttezza del processo informatico in tutte le sue componenti: dalla sua costruzione, all'inserimento dei dati, alla loro validità, alla loro gestione. Da qui, come si è detto, si conferma la necessità di assicurare che quel processo, a livello amministrativo, avvenga in maniera trasparente, attraverso la conoscibilità dei dati immessi e dell'algoritmo medesimo.
In secondo luogo, conseguente al primo, il giudice deve poter sindacare la stessa logicità e ragionevolezza della decisione amministrativa robotizzata, ovvero della «regola» che governa l'algoritmo, di cui si è ampiamente detto.

La questione è stata, poi, ripresa dalla stessa Corte (Cons. Stato 13 dicembre 2019, n. 8472, in *Foro it*., 2020, III, 340), con un riferimento diretto all'art. 22 GDPR:

> Nel caso in cui una decisione automatizzata «produca effetti giuridici che riguardano o che incidano significativamente su una persona», questa ha diritto a che tale decisione non sia basata unicamente su tale processo automatizzato (art. 22 Reg.). In proposito, deve comunque esistere nel processo decisionale un contributo umano capace di controllare, validare ovvero smentire la decisione automatica. In ambito matematico ed informativo il modello viene definito come HITL (human in the loop), in cui, per produrre il suo risultato è necessario che la macchina interagisca con l'esser umano. In terzo luogo, dal considerando n. 71 del Regolamento 679/2016 il diritto europeo trae un ulteriore principio fondamentale, di non discriminazione algoritmica, secondo cui è opportuno che il titolare del trattamento utilizzi procedure matematiche o statistiche appropriate per la profilazione, mettendo 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 che 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 che comportano misure aventi tali effetti.

Per finire, merita di essere citato un famoso caso statunitense che è intervenuto sull'argomento: *State v. Loomis*, 881 N.W.2d 749 (2016). Nel febbraio 2013, Eric Loomis era stato trovato alla guida di un'auto che era stata utilizzata in una sparatoria. Fu arrestato e dichiarato colpevole in quanto non si era fermato al controllo di polizia. Nel determinare la sua condanna, il giudice aveva preso in considerazione la sua fedina penale, nonché un punteggio assegnato da uno strumento chiamato COMPAS. Il software funziona utilizzando un algoritmo proprietario che considera alcune delle risposte a un questionario di 137 elementi al fine di determinare il profilo di rischio di un individuo. Sviluppato da una società privata chiamata Equivant, COMPAS è stato utilizzato dagli stati di New York, Wisconsin, California, contea di Broward in Florida e altre giurisdizioni. COMPAS aveva classificato Loomis ad alto rischio di recidiva ed era stato, così, condannato a sei anni di reclusione. Loomis aveva impugnato

la sentenza sostenendo che l'utilizzo di tale software nella decisione di condanna violasse il suo diritto ad un giusto processo poiché gli negava la possibilità di contestare la validità scientifica e l'accuratezza di tale test. L'udienza di questo caso avrebbe dato alla corte l'opportunità di decidere se l'utilizzo di uno strumento per la valutazione del rischio il cui funzionamento è protetto da segreto commerciale violi o meno appunto il principio del giusto processo. La Corte Suprema ha, però, respinto il *writ of certiorari*, rifiutandosi così di ascoltare la causa, il 26 giugno 2017: *Loomis v. Wisconsin*, 881 NW2d 749 (Wis. 2016), cert. denied, 137 S.Ct. 2290 (2017) [Noto la Diega 2018].

13.5 Caso 13-1

Caso 13-1

L'ecosistema TrocDiabete è pensato per supportare l'auto-cura ed il monitoraggio remoto dei pazienti affetti da patologia diabetica. È composta da una piattaforma che permette, da un lato, di interoperare con sistemi di terze parti (ad es., Fascicolo sanitario elettronico, Cartella clinica, Sistemi informativi ospedalieri, ecc.), dall'altro, di abilitare applicazioni indirizzate a medici (dotati di un cruscotto clinico) e pazienti (che possono utilizzare un'app di telemedicina). In questo contesto si prevede anche l'utilizzo di un *virtual coaching*, una sorta di assistente virtuale che è volto a sostituire la tradizionale interazione medico-paziente, fornendo un'assistenza diretta e non mediata dall'intervento umano.
Quali sono i dati trattati?
Qual è la base giuridica di questo trattamento?
Quali sono le criticità di questo scenario applicativo?
Quali le misure adeguate da adottare in tale contesto?

CAPITOLO 14.
Privacy e Internet of Things

Paolo Guarda

14.1 Il fenomeno tecnologico

È ormai comunemente noto come non esista più una vita completamente offline, disconnessa dalla Rete, capace di porsi come alternativa alle operazioni che compiamo nel contesto digitale. Mercè l'uso degli smartphone, da tempo viviamo in una dimensione costantemente connessa ad Internet, perennemente online. Le nostre interazioni anche con il modo «reale» sono regolarmente mediate da attività che poniamo in essere attraverso i nostri molteplici device (tablet, smartphone, ecc.). Tutto ciò è ancora più vero se consideriamo, poi, come anche gli «oggetti» diventino parte di questa Rete. Con l'espressione «Internet of Things» (IoT) appunto ci si riferisce all'estensione di Internet al mondo delle cose [Ashton 2009]: un'infrastruttura costituita dall'interconnessione di sensori di cui sono equipaggiati oggetti e dispositivi di uso quotidiano (quali ad es. automobili, elettrodomestici, occhiali, orologi, ecc.) in grado di collazionare dati, personali e non, elaborarli e comunicarli in Rete. Poiché, infatti, ogni dispositivo è associato ad identificatori univoci, essi sono così in grado di interagire con altri oggetti o sistemi. Secondo Floridi il fenomeno fa parte di quella che è stata definita «onlife» [Floridi 2015].

La tecnologia, da strumento a disposizione al fine di raggiungere determinati fini (ad essa anche estranei), diviene contesto, ambiente [Durante 2019, 47-82].

In un mondo IoT, ogni cosa è connessa a Internet, comunica automaticamente con altre cose, trasforma ogni aspetto della nostra vita in informazioni calcolabili e utilizza queste informazioni per agire sulla realtà fisica e produrre cambiamenti spesso imprevedibili nel mondo «reale». Oltre alla sicurezza ed alla privacy, tutto ciò può rappresentare anche una minaccia per altri valori fondamentali, dall'autodeterminazione alla libertà di espressione e all'uguaglianza (Noto la Diega 2023, 2-3].

Chi controlla l'ecosistema di applicazioni e servizi può, pertanto, giovarsi della propria posizione dominante per imporre contratti che cercano di giustificare pratiche sleali ed opache, tra cui l'appropriazione ed il riutilizzo di dati personali e non (c.d. «appropriazione dei dati»). È, infatti, un malinteso comune che i dati IoT sfuggano all'applicazione della disciplina in materia di protezione dei dati personali. Soprattutto nel contesto di sistemi di uso quotidiano (ad es. le c.d. smart home), i vari device possono, infatti, comunicare ai produttori non solo dati sul funzionamento della macchina stessa, ma anche dati granulari sul comportamento del consumatore [Noto la Diega, Sappa 2020, 419-420].

L'impatto dell'IoT sul contesto giuridico non si limita a determinare il ripensamento del concetto di diritto, ma riguarda anche una seria riflessione circa l'importanza - per non dire spesso preminenza - della regola tecnica. L'IoT irrompe ed interrompe molte delle dicotomie su cui si basano i sistemi normativi: hardware-software, materiale-immateriale, consumatore-professionista, consumatore-lavoratore, uomo-macchina, online-offline. Sul punto illuminanti sono le parole di Noto la Diega [2023, 5]:

> More generally, the fact that the IoT is troubling the binary categories that underpin the law calls for a rigorous legal analysis to critically assess whether the law can be 'queered'. By 'queering' the law, I mean the overcoming of the aforementioned binaries through interpretation, legal design, or law reform. A queer approach requires also that the power dynamics hidden behind the 'smart' world be brought to life, which in turn means asking oneself whether traditional legal changes adequately curb the power of IoT capitalists or a more radical upheaval would be desirable.

14.2 Internet delle cose e tutela dei dati personali

I sistemi di IoT si fondano su un vasto e dettagliato trattamento di dati personali posto in essere attraverso sensori progettati per imporsi in modo intrusivo nelle vite delle persone e scambiare dati in modo costante e continuo [Giovanella 2019, 1214].

Il Gruppo art. 29 ha pubblicato un parere sull'IoT che fornisce un quadro analitico sulle principali questioni relative alla protezione dei dati: WP29, *Parere 8/2014 sui recenti sviluppi nel campo dell'Internet degli oggetti*, adottato il 16 settembre 2014 (d'ora in avanti: WP29 Parere IoT). Sebbene il parere si basi sulla Direttiva 95/46, il suo impianto rimane attuale anche con riferimento al nuovo GDPR: la più parte delle considerazioni proposte, infatti, conserva la propria validità. A tale framework è necessario aggiungere alcuni fenomeni che di recente hanno acceso il dibattito accademico, come il tema delle inferenze [Noto la Diega 2023, 239-240].

Un ruolo fondamentale è, inoltre, giocato dal principio della «data protection by design», in connessione con quello «by default», che, come noto, prevede un obbligo in capo al titolare del trattamento di mettere in atto misure tecniche ed organizzative adeguate «sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento». Tale previsione non sarebbe indirizzata solo al titolare del trattamento, ma anche ai produttori dei servizi e delle applicazioni, come recita il Considerando 78 [vedi → Capitolo 4]:

> In fase di sviluppo, progettazione, selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati personali o che trattano dati personali per svolgere le loro funzioni, i produttori dei prodotti, dei servizi e delle applicazioni dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati allorché sviluppano e progettano tali prodotti, servizi e applicazioni e, tenuto debito conto dello stato dell'arte, a far sì che i titolari del trattamento e i responsabili del trattamento possano adempiere ai loro obblighi di protezione dei dati.

Alcuni autori suggeriscono che applicare agli oggetti IoT una certificazione quale il marchio «CE» o un marchio appositamente creato per la disciplina in materia di protezione dei dati personali potrebbe favori-

re l'adozione di standard omogenei e una più compiuta armonizzazione all'interno dell'Unione europea [Giovanella 2019, 1238-1239 e Lachaud 2016].

Altro elemento caratterizzante è rappresentato dalla mancanza di controllo da parte dell'utente rispetto al sistema utilizzato e, conseguentemente, da una chiara situazione di asimmetria informativa [Noto la Diega 2023, 240-241]. È, infatti, alquanto difficile avere contezza di come i vari device interagiscano tra di loro e di quali dati siano poi effettivamente inviati al produttore. Il frigo e il forno potrebbero infatti comunicare con il sistema di allarme e gli assistenti personali, quali Alexa o Google Home, e viceversa. Le aziende coinvolte cercano di mantenere il più possibile segrete tali informazioni. La problematica non è certo nuova in scenari caratterizzati da Big Data [vedi → Capitolo 13) e cloud computing. Qui, però, il quadro è reso ancora più complesso dalla possibilità di combinare dati provenienti da più fonti (WP29 Parere IoT, 7-8):

> l'interazione degli oggetti tra loro, tra gli oggetti e i dispositivi delle persone, tra le persone e altri oggetti e tra oggetti e sistemi di back-end porterà alla creazione di flussi di dati che possono difficilmente essere gestiti dai classici strumenti utilizzati per garantire una tutela adeguata degli interessi e dei diritti degli interessati.

Se si considera, poi, la possibilità di abilitare il monitoraggio da parte di terze parti e la spiccata automazione che contraddistingue questi sistemi, la perdita del controllo è ancora più evidente.

L'IoT pone, infine, vari problemi nel campo della sicurezza: i vincoli ad essa relativi e l'esigenza di risparmiare risorse impongono ai fabbricanti di dispositivi di trovare un compromesso tra l'applicazione delle misure di riservatezza, integrità e disponibilità a tutti i livelli del processo di trattamento e la necessità di ottimizzare l'uso delle risorse computazionali, nonché dell'energia, da parte degli oggetti e dei sensori (WP29 Parere IoT, 10-11) [Chiara 2022].

Diversi sono, dunque, i momenti critici allorquando si cerchi di applicare la disciplina prevista dal GDPR alla tecnologia dell'IoT. Di seguito si analizzeranno, tra i tanti, alcuni aspetti peculiari con riferimento a: il tema del consenso; la gestione dei ruoli privacy; il regime giuridico dei dati inferenziali; l'annosa questione dell'anonimizzazione.

14.2.1 Consenso informato e granularità

Un elemento centrale nell'affrontare il tema del trattamento di dati personali posto in essere nel contesto IoT è quello relativo al consenso che rappresenta pur sempre il primo criterio di liceità del trattamento stesso [Noto la Diega 2023, 241-246].

Questo istituto è fortemente messo in crisi anzitutto per la complessità delle caratteristiche tecniche che contraddistingue lo scenario applicativo e che fa risultare gravoso rendere veramente edotto l'interessato al trattamento delle modalità attraverso le quali i suoi dati personali sono trattati. Inoltre, i tradizionali sistemi di autorizzazione utilizzati per decidere se un richiedente di una risorsa dispone di autorizzazioni sufficienti non sono interamente applicabili all'IoT. Una corretta gestione della protezione dei dati personali imporrebbe, infatti, che fossero indicate esattamente tutte le possibili interazioni con i dati [Noto la Diega 2023, 242]:

> However, consent can be regarded as 'informed' only if the user has sufficient knowledge of the risks and benefits of disclosing information to make a reasonable evaluation.

Il GDPR ha stabilito uno standard elevato di consenso, che deve essere informato, libero, specifico, inequivocabile, granulare, facile da revocare e dimostrabile (artt. 6 e 7).

Il consenso difficilmente può essere considerato informato nella maggior parte degli scenari IoT, in cui è improbabile che gli utenti siano a conoscenza delle attività di elaborazione dei loro dati. Il consenso informato è stato considerato irraggiungibile perché una delle sue caratteristiche principali è la c.d. «sensor fusion», che consiste [WP29 Parere IoT, 9 nota 6]:

> nel combinare i dati da sensori o tratti da diverse fonti al fine di ottenere informazioni migliori e più precise rispetto a quelle che sarebbe possibile ottenere se queste fonti operassero isolatamente.

Tale fusione contribuisce alla quasi impossibilità di de-identificare veramente i dati dei sensori rendendo consigliabile per i titolari del trattamento indagare sulla possibile applicazione di altre basi legittime del

trattamento. Si ricorda, infatti, che qualora i dati non siano anonimizzati, si applicheranno tutte le regole in materia di protezione dei dati personali.

Il consenso deve essere, poi, prestato liberamente. Spesso i gestori dei servizi IoT subordinano la possibilità di accedere a determinati servizi o funzionalità appunto al suo ottenimento. Si risulta «liberi» nello scegliere se acquistare o meno un prodotto o servizio IoT, ma meno liberi nel modulare o governare i propri dati.

Esso deve, inoltre, essere «specifico», cioè deve essere connesso ad una o più finalità ben determinate (v. EDPB, «Guidelines 05/2020 on Consent under Regulation 2016/679», v. 1.1, 13). Questo requisito è strettamente legato al principio di limitazione delle finalità (art. 5, par. 1, lett. b), GDPR), in base al quale i dati personali devono essere «raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità». Il metodico riutilizzo di dati posto in essere dai sistemi IoT, intrinsecamente connesso alla loro inter-connettività, di fatto contrasta con entrambi questi principi. Da un lato, quindi, è praticamente impossibile per i titolari del trattamento prevedere e quindi specificare tutte le finalità per le quali i dati potrebbero essere oggetto di trattamento. D'altra parte, si potrebbe sostenere che, poiché il riutilizzo è una caratteristica fondamentale dell'IoT, quando gli interessati utilizzano questi smart device, essi debbono aspettarsi proprio il riutilizzo dei loro dati.

Granularità, facilità di revoca e dimostrabilità rappresentano aspetti ulteriormente enfatizzati dal GDPR.

Granulare significa che dovrebbero esserci opzioni di consenso separate per diversi tipi di trattamento, e se il consenso dell'interessato è dato nel contesto di una dichiarazione scritta che riguarda anche altre questioni (art. 7, par. 2, GDPR):

> la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Nessuna parte di una tale dichiarazione che costituisca una violazione del presente regolamento è vincolante.

Gli utenti dell'IoT dovrebbero essere liberi di revocare il proprio consenso in qualsiasi momento e con la stessa facilità con cui esso è stato fornito. Ciò significa che quando il consenso è ottenuto tramite mezzi elettronici, quali il semplice clic del mouse, lo scorrimento o la «pressione di un tasto», per revocarlo non possono essere imposte procedure più macchinose.

Infine, il consenso deve essere dimostrabile. Questa è un'applicazione del principio generale di responsabilizzazione che il GDPR ha introdotto per chiarire che la conformità in quanto tale non è sufficiente: i titolari del trattamento devono tenere registri accurati delle loro attività di trattamento e delle modalità con cui si conformano al GDPR. Di conseguenza, le società IoT devono conservare la prova di un consenso valido per tutta la durata del trattamento e, successivamente, per tutto il tempo necessario al rispetto di eventuali obblighi legali o per l'esercizio di diritti.

Il consenso come base legittima potrebbe essere necessario non solo ai sensi del GDPR, ma anche della Direttiva 2002/58/CE 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 (d'ora in avanti: Direttiva comunicazioni elettroniche) [Giovanella 2016, 1228-1231; vedi → Capitolo 7]. Nel caso in cui un oggetto dell'IoT rientri nella definizione di «apparecchio terminale», qualora appunto un soggetto immagazzini dati o acceda a dati già immagazzinati su un oggetto intelligente, sarà allora necessario applicare l'art. 5, par. 3 della Direttiva:

> 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.

Destinatari di questa previsione sono non solo il produttore dell'oggetto, ma anche gli altri soggetti che vorranno avere accesso alle informazioni raccolte ed archiviate mediante il dispositivo. Nel 2017 è stata presentata una 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)» (Regolamento *e-privacy*) [vedi → Capitolo 7] che andrà ad abrogare la Direttiva comunicazione elettroniche e che potrà comportare modifiche per i trattamenti effettuati nei sistemi IoT.

14.2.2 La gestione dei ruoli privacy

Il GDPR prevede una serie di ruoli e di soggetti che possono essere coinvolti nel trattamento di dati personali [vedi → Capitolo 3]. L'applicabilità di questi al contesto IoT non è attività di poco momento [Giovanella 2016, 1234-1236].

I sistemi IoT sono, infatti, caratterizzati dall'intervento simultaneo e combinato di numerosi attori: i produttori degli oggetti, i gestori delle piattaforme, le applicazioni di terze parti, le società che concedono i device in locazione o leasing, intermediari di dati, ecc.

I fabbricanti di dispositivi IoT non si limitano a produrre e mettere in commercio oggetti fisici ai loro clienti; essi possono anche sviluppare o modificare il sistema operativo dello smart device o avervi installato software che determinano la sua funzionalità generale, compresi i dati, la frequenza di raccolta, quando e a chi vengono trasmessi i dati, ecc. Così facendo, spesso, questi soggetti raccolgono e trattano dati personali che sono generati dal dispositivo per finalità e mezzi che hanno determinato nella loro totalità, e sono, pertanto, qualificabili come titolari del trattamento.

Considerazioni simili possono svolgersi per i gestori delle piattaforme, in quanto soggetti che si trovano nella posizione di poter scegliere quali dati raccogliere, secondo quali finalità e di definire le modalità attraverso le quali trattarli, potendo così, a loro volta, configurarsi nel ruolo di titolare.

Inoltre, molti sensori contengono «Application Programming Interface» (API) per agevolare lo sviluppo di applicazioni. Gli utenti devono, allora, installare applicazioni di terzi che consentono a questi di accedere ai loro dati, i quali vengono conservati dal fabbricante del dispositivo. Scaricare queste applicazioni consiste nella maggior parte dei casi nel fornire allo sviluppatore un accesso ai dati attraverso l'API. Generalmente tale installazione avviene sulla base del consenso degli utilizzatori, che, nella pratica, spesso non è preceduto dalle informazioni necessarie perché possa essere considerato specifico e sufficientemente informato e quindi valido in base alla disciplina in materia di protezione dei dati personali.

Infine, terzi diversi dai fabbricanti di dispositivi e dagli sviluppatori di applicazioni possono utilizzare sistemi IoT per raccogliere e trattare informazioni sulle persone. Il Gruppo art. 29 nel Parere IoT (p. 14) propone l'esempio delle compagnie di assicurazione sanitaria, le quali potrebbero voler fornire contapassi agli assicurati per monitorare la frequenza del loro esercizio fisico e adattare di conseguenza i loro premi assicurativi. Contrariamente a quanto accade per i fabbricanti di dispositivi, tali terzi non hanno alcun controllo sul tipo di dati raccolti dall'oggetto; ciononostante sono qualificabili come titolari del trattamento, in quanto raccolgono e conservano i dati generati da tali dispositivi IoT per scopi specifici che essi stessi hanno determinato.

Tutti gli scenari proposti tratteggiano situazioni nelle quali si assiste alla contemporanea presenza di molteplici titolari autonomi (non sarebbe infatti configurabile la c.d. «contitolarità» di cui all'art. 26 GDPR, in quanto essi non determinano congiuntamente scopi e modalità del trattamento). Proprio la compresenza di più soggetti che hanno poteri pregnanti nella determinazione della finalità e dei mezzi del trattamento, ma in un contesto non sempre facilmente determinabile, potrebbe portare ad una applicazione poco efficiente della disciplina in materia di protezione dei dati personali. L'unica soluzione suggeribile appare, allora, quella di porre in essere un'analisi «caso per caso», cercando di determinare la corretta allocazione dei ruoli e la migliore distribuzione di obblighi e responsabilità. Oltre ai titolari, si dovrà verificare la presenza di responsabili del trattamento ed eventuali destinatari.

14.2.3 I dati inferenziali

Il valore dei processi IoT spesso non deriva solo dai dati direttamente elaborati. Assai più profittevoli risultano essere tutte le deduzioni che possono essere tratte da essi [Noto la Diega 2023, 246-247]. Il regime giuridico di questi dati che vengono chiamati «inferenziali» è attualmente dibattuto.

La perfetta alchimia tra Big Data, tecniche evolute di data mining e combinazione di dati provenienti da più fonti porta alla creazione di inferenze di grande valore sul comportamento (presente e futuro) e sulle possibili vulnerabilità degli utilizzatori. Questo permette di passare da un'analisi di tipo meramente predittivo rispetto ai possibili interessi e preferenze dell'utente, al potere sempre più pervasivo, in mano alle aziende IoT, di modificare il modo in cui l'individuo si comporta nel contesto fisico e digitale.

La natura di dato personale relativamente a questi dati inferenziali è questione discussa dalla dottrina. La tesi che vede questi dati come non personali avvantaggia in modo evidente le società che forniscono servizio IoT, in quanto ciò porterebbe ad eludere il principio della limitazione delle finalità ed alla libera riutilizzabilità dei dati desunti per scopi che vanno oltre quello originale per il quale i dati erano stati raccolti. Inoltre, gli utenti non potrebbero invocare i diritti previsti per gli interessati al trattamento, ed in particolare quello di rettifica ai sensi dell'art. 16 GDPR, determinando deduzioni non verificabili che possono portare a processi decisionali automatizzati con effetti discriminatori.

L'applicabilità delle regole in materia di protezione dei dati personali è, pertanto, fondamentale.

A dire il vero la definizione di dato personale fornita dal GDPR riguarda appunto tutte le informazioni che identificano anche potenzialmente e indirettamente una persona fisica (art. 4, pt. 1, GDPR); un'interpretazione così ampia è anteriore al Regolamento europeo e risale alla Convenzione 108 del 1981 (art. 1). La stessa CGUE, la Corte EDU ed i tribunali nazionali tendono a interpretare il concetto in senso lato (vedi ad esempio C-582/14 Breyer [2017] CEDU, 24 aprile 2018, no. 62357/14, *Benedik v. Slovenia App*).

Anche le regole sulla profilazione sembrano applicarsi ai dati inferenziali. Così recita la definizione fornita dall'art. 4, pt. 4, GDPR:

> «profilazione»: 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.

La definizione è sufficientemente ampia da comprendere la maggior parte delle inferenze. E in effetti, come rilevato dal Gruppo art. 29 nelle «Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679», adottato il 3 ottobre 2017 (versione emendata ed adottata in data 6 febbraio 2018 (p. 7):

> Spesso viene impiegata per effettuare previsioni su persone usando dati provenienti da varie fonti per dedurre qualcosa su una persona in base alle qualità di altre persone che sembrano statisticamente simili.

Infine, trova applicazione anche il principio di esattezza (art. 5, par. 1, lett. d, GDPR) che impone alle società IoT di mettere in atto processi adeguati affinché i dati personali, comprese quindi le deduzioni, siano corretti ed aggiornati. L'importanza di deduzioni accurate è stata sottolineata anche dal Consiglio d'Europa, che ha raccomandato di rivalutare periodicamente ed entro un tempo ragionevole la qualità dei dati e delle deduzioni statistiche utilizzate (Council of Europe, The Protection of Individuals with Regard to Automatic Processing of Personal Data in Context of Profiling: Recommendation CM/Rec(2010)13, 11).

14.2.4 L'annosa questione dell'anonimizzazione

L'anonimizzazione rappresenta il primo e più efficace strumento di tutela degli utilizzatori di sistemi IoT. Essa è, però, come noto, caratterizzata da intrinseche difficoltà nel nuovo scenario tecnologico [vedi → Capitolo 12]. Nel nostro contesto risulta ancora più complesso riuscire a porre in

essere un processo di anonimizzazione dei dati completamente affidante.

Innanzitutto, l'IoT produce enormi quantità di dati: più di venti miliardi di megabyte all'anno. Questi, poi, sono fortemente granulari, provenendo da più fonti, e permettono di tracciare tutti i device usati dall'utente in un determinato contesto fisico. Tutte assieme queste informazioni tratteggiano gli aspetti più intimi della vita di un individuo: le tecnologie IoT sono onnipresenti e permeano gli spazi più privati delle persone (casa e corpo). Infine, le «cose» che si trovano nelle immediate vicinanze dell'interessato (ad es. dispositivi indossabili) determinano la disponibilità di identificatori stabili (ad es. indirizzi MAC multipli). Così descrive il fenomeno il WP29 Parere IoT, 10:

> Ad esempio gli oggetti indossabili, tenuti molto vicino agli interessati, rendono disponibile una serie di altri identificativi, quali indirizzi MAC di altri dispositivi, che potrebbero essere utili per generare una fingerprint («impronta digitale») che permetta la localizzazione dell'interessato. La raccolta di vari indirizzi MAC di vari sensori agevolerà la creazione di fingerprint uniche e di identificativi più stabili che i portatori di interessi dell'IoT potranno attribuire a persone specifiche. Tali fingerprint e identificativi potrebbero essere utilizzati per vari scopi, compresa la location analytics o l'analisi degli spostamenti di gruppi di persone e di singoli individui.

Tutto ciò rende di fatto molto difficile garantire una vera anonimizzazione dei dati, i quali possono sempre facilmente essere collegati a persone fisiche ben determinate.

14.3 Considerazioni finali

I sistemi IoT rappresentano una delle maggiori sfide del prossimo futuro. Contribuiscono a costruire l'ecosistema all'interno del quale sempre più viviamo e dove l'utente non è più l'attore principale ma diviene esso stesso fonte di dati ed informazioni di cui il sistema stesso si nutre. Le criticità, per quanto riguarda il trattamento dei dati personali, sono evidenti. L'arsenale giuridico appare nuovamente in affanno e talvolta non adeguato a contrastare fenomeni così pervasivi.

Quanto detto sinora, poi, dal punto di vista dell'analisi giuridica, potrebbe subire profondi cambiamenti con l'emanazione del già ricordato Regolamento *e-privacy*. Questo abrogherà la Direttiva 2002/58 e si applicherà, stante l'attuale formulazione dell'art. 2, par. 1, al trattamento dei dati delle comunicazioni elettroniche effettuato in relazione alla fornitura e alla fruizione dei servizi di comunicazione elettronica e alle informazioni connesse alle apparecchiature terminali degli utenti finali. Proprio alla luce di tale ultimo inciso, non v'è dubbio che esso troverà applicazione anche al contesto IoT. Lo stesso Considerando 12, nell'attuale formulazione, esplicita che:

> I dispositivi e le macchine connessi comunicano sempre più fra loro per mezzo di reti di comunicazione elettroniche (internet delle cose). La trasmissione di comunicazioni da macchina a macchina prevede la trasmissione di segnali attraverso una rete e quindi costituisce un servizio di comunicazione elettronica. Al fine di garantire la piena tutela della vita privata e della riservatezza delle comunicazioni, nonché promuovere un internet delle cose affidabile e sicuro nel mercato unico digitale, è necessario chiarire che il presente regolamento dovrebbe applicarsi alla trasmissione di comunicazioni da macchina a macchina. Pertanto il principio di riservatezza sancito dal presente regolamento dovrebbe applicarsi anche alla trasmissione di comunicazioni da macchina a macchina.

Il Regolamento *e-privacy*, come già anticipato nel Capitolo 7, sarà da considerarsi *lex specialis* rispetto al GDPR. L'interprete sarà nuovamente chiamato ad una attenta attività di coordinamento tra disposizioni.

La partita, dunque, è ancora tutta da giocare. La posta in gioco è molto alta. L'adozione di principi e garanzie proprie della disciplina europea in materia di protezione dei dati personali al contesto dell'IoT rappresenta una questione di vitale rilevanza e dovrà riconoscere ancora una volta il primato dell'uomo sulla macchina e, soprattutto, l'importanza del riconoscimento della dignità dell'individuo nei confronti di tecnologie e modelli di business sempre più invasivi e massificanti.

14.4 Casi 14-1, 14-2, 14-3[1]

Caso 14-1

Pietro indossa un braccialetto atto a registrare il numero dei passi fatti quotidianamente che archivia questa informazione nella sua memoria interna. Pietro ha, poi, installato sul proprio smartphone un'applicazione per scaricare direttamente il numero dei passi dal proprio dispositivo. Il fabbricante del dispositivo desidera caricare i dati dai contapassi sui propri server. Una volta caricati i dati sui propri server, il fabbricante conserva unicamente i dati aggregati sul numero di passi al minuto.
Qual è il problema giuridico?
Il fabbricante deve ottenere il consenso dell'utente per caricare i dati sui propri server?
Qualora un'applicazione terza desideri accedere ai dati salvati sul server del fabbricante si applicherà il GDPR?

Caso 14-2

Un dispositivo sanitario monitora il flusso di sangue che scorre nelle vene al fine di ricavare informazioni sul battito cardiaco. Il dispositivo comprende un altro sensore che misura il livello di ossigeno nel sangue. Non vengono fornite informazioni circa questa raccolta di dati, né sul dispositivo né sull'interfaccia per l'utente.
Come sarà possibile attivare il sensore che misura il livello di ossigenazione nel sangue?
Quale sarà la base legittima utilizzabile?
Quali gli ulteriori requisiti atti a rendere lecito tale trattamento?

Caso 14-3

L'impresa Smettoquandovoglio 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. Il prodotto, compatibile con la maggior parte dei sensori sul mercato, potrebbe essere utilizzato come un'applicazione autonoma o attraverso un'interfaccia web che richiede il caricamento dei dati.
Com'è possibile porre in essere questo ulteriore trattamento?
Qual è la base legittima del trattamento?
Quali le ulteriori possibili misure di sicurezza adottabili?

1 Tratti e, parzialmente modificati, dal WP29 Parere IoT.

CAPITOLO 15.
Privacy e sanità digitale

Paolo Guarda

15.1 Innovazione tecnologica e sanità digitale: premessa

L'incessante sviluppo che caratterizza l'uso delle tecnologie digitali nel contesto sanitario pone sfide per l'interprete, il quale è chiamato ad applicare regole e principi pensati e profilati avendo a riferimento contesti tecnologici ormai mutati. L'obsolescenza che i nomenclatori e le categorie del diritto conoscono in tale ambito è notevole [Guarda 2011, 178-183].

La sanità digitale, ovvero appunto l'applicazione delle tecnologie dell'informazione alla tradizionale attività di cura ed assistenza, rappresenta un'innovazione cruciale che promette di far progredire l'assistenza sanitaria stessa e di migliorare la qualità e l'efficacia dei servizi offerti [Sigulem, Ramos, de Holanda Albuquerque 2017, 152-167].

La digitalizzazione dovrebbe essere considerata qualcosa di più di un processo tecnico poiché coinvolge sia le ICT che le pratiche, i servizi e i processi relativi all'assistenza sanitaria [Bincoletto 2021a, 168 ss]. La Commissione europea nel «eHealth Action Plan 2012-2020. Innovative healthcare for the 21st century» circoscrive lo scenario:

> The use of ICT in health products, services and processes combined with organisational change in healthcare systems and new skills, in order to improve health of citizens, efficiency and productivity in healthcare delivery, and the economic and social value of health.

Il fenomeno riflette una tendenza globale, se è vero che i sistemi sanitari devono affrontare nuove sfide di portata sovranazionale, tra le quali [Sartori 2009, 33-49 e Guarda 2011, 9-12]:

– una crescente domanda di servizi sanitari e sociali, dovuta principalmente ad un progressivo invecchiamento della popolazione mondiale – in particolare nei Paesi occidentali – ed a livelli di reddito e di istruzione più elevati rispetto al passato, che determinano un cambiamento dell'approccio, anche cognitivo, che i cittadini-utenti manifestano nei confronti del servizio sanitario;
– una significativa evoluzione della domanda stessa, in quanto il progresso tecnologico ha esteso il grado di efficacia e di complessità dell'intervento medico con un conseguente aumento delle aspettative sociali e delle richieste da parte dei pazienti;
– l'evoluzione del sistema di fornitura degli stessi servizi sanitari, tenuto conto delle difficoltà che le pubbliche amministrazioni incontrano nel far combaciare le esigenze legate ad investimenti in nuove tecnologie, con la complessa opera di riorganizzazione dei sistemi sanitari impegnati nella missione di garantire di più con meno;
– la crescente mobilità dei pazienti e del personale sanitario, che rischia di determinare (e nei fatti già realizza) fenomeni di «hospital shopping».

Da questo punto di vista, l'informatizzazione del servizio sanitario è considerata una ricetta utile ad aumentare il livello delle prestazioni, da un lato, e ridurre il costo del sistema, dall'altro.

Da più di vent'anni l'UE è impegnata nel promuovere piano d'azione sulla sanità digitale [Bincoletto 2021a, 171-172 e Di Federico, Negri 2020]. Tali piani mirano a promuovere l'adozione dell'e-health in tutto il territorio dell'Unione e a rimuovere gli ostacoli alla sua definitiva affermazione. In particolare, tre sono le priorità individuate dalla Commissione Europea nella «Communication on Digital Transformation of Health Care in the Digital Single Market»[1]:

1 EC European Commission. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society*. European Commission. Brussels: COM (2018), 233 final. 2018.

– garantire ai cittadini l'accesso e la condivisione dei propri dati sanitari in modo sicuro tra gli Stati membri;
– migliorare la qualità dei dati a fini di ricerca, prevenzione delle malattie e realizzazione di un'assistenza sanitaria personalizzata;
– sviluppare strumenti di sanità elettronica per l'empowerment dei cittadini e l'assistenza centrata sulla persona.

Gli strumenti e le soluzioni di *e-health* includono tecnologie multiple ed eterogenee che possono essere suddivise in [Cowie et al. 2016, 63 e Bincoletto 2021a, 172-174]:
– telemedicina e teleassistenza (es. monitoraggio remoto del paziente);
– sistemi informativi clinici (es. i sistemi connessi ai fascicoli sanitari elettronici);
– reti informative integrate e strumenti per generare elettronicamente le ricette ed inviarle direttamente in farmacia dal punto di cura (e-prescribing ed e-referral);
– registri delle malattie e sistemi utilizzati per la gestione di attività formative, per fini di salute pubblica, e più generale per l'assistenza sanitaria;
– applicazioni per smartphone (mobile health);
– salute personalizzata (es. micro e nanotecnologie indossabili o impiantabili);
– Big data (ad es. per la salute predittiva), IA e Internet of Things.

Sempre a livello europeo è necessario ricordare il programma «UE per la salute» (*EU4Health*) per il periodo 2021-2027 nel quale vengono previste ulteriori azioni specifiche a «sostegno all'uso ottimale della telemedicina e della telesalute anche tramite la comunicazione satellitare per le regioni isolate» e volte a «promuovere la sanità elettronica, come il passaggio alla telemedicina e la somministrazione domiciliare delle terapie farmacologiche»[2]. Attraverso il futuro spazio comune europeo di dati sanitari la Commissione adotterà nuove misure settoriali di carattere

2 Si v. art. 1, par. 6, lett. d) e i) dell'Allegato I del Regolamento (UE) 2021/522 del Parlamento europeo e del Consiglio del 24 marzo 2021 che istituisce un programma d'azione dell'Unione in materia di salute per il periodo 2021-2027 («programma UE per la salute») (EU4Health) e che abroga il regolamento (UE) n. 282/2014, PE/69/2020/REV/1, GU L 107 del 26.3.2021.

legislativo e di soft law che riguarderanno l'utilizzo e la circolazione dei dati sanitari, soprattutto con finalità di ricerca, ed incentiverà lo sviluppo di innovative soluzioni tecnologiche e di nuovi strumenti[3] [Bincoletto 2021b, 388-389].

Le piattaforme di *e-health* inducono a concepire l'intera infrastruttura non solo in base alle esigenze professionali o manageriali dei titolari del trattamento, ma in misura crescente alla luce degli interessi di cui il paziente è portatore. Il principio di autodeterminazione altro non è che lo strumento che permette di dare contenuto giuridico a tali esigenze. Questa nuova tendenza va sotto il nome di «patient empowerment». In concreto ciò si traduce nel fatto che le scelte in ordine a quali informazioni immettere nel sistema, ai livelli di condivisione e alle varie applicazioni che una piattaforma di sanità digitale permette di amministrare possono essere gestite direttamente dal paziente attraverso lo strumento tecnico-giuridico del consenso.

L'avvento di questi nuovi sistemi si accompagna, però, al rischio di disumanizzare il rapporto medico-paziente. La tecnologia informatica irrompe nella loro interazione, che risulta, così, filtrata da strumenti digitali che integrano e a volte sostituiscono segmenti di questo scambio interattivo, un tempo affidato esclusivamente alla comunicazione orale, seguita dalla scrittura in documenti cartacei [Izzo 2000 e Guarda 2011, 120-122]. Se, a prima vista, gli assi sui quali costruire il rapporto medico-paziente non cambiano (un confronto in ambulatorio senza contatto fisico può avvenire attraverso una comunicazione video in remoto; un referto cartaceo illustra i medesimi contenuti quando è originariamente composto in bit), è innegabile che lo scenario digitale acceleri i tempi, arricchisca sensibilmente i possibili contenuti di questo scambio informativo e, soprattutto, introduca una nuova dimensione nella dinamica che accede all'instaurarsi della fiducia.

Evidentemente le questioni regolamentari e giuridiche giocano in tale contesto un ruolo decisivo. In particolare, e per quanto qui ci interessa, la riservatezza, la protezione dei dati e la sicurezza potrebbero essere viste sia come questioni relative alle tecnologie di *e-health* sia come diritti o obblighi stabiliti dalla legge per ridurre al minimo i rischi per i diritti e le libertà degli individui [Bincoletto 2021a, 176-184].

3 Commissione Europea, *A European Strategy for Data*, cit., par. 4.

La privacy nel contesto dell'*e-health* è un concetto complesso e sfaccettato perché protegge un ampio spettro di interessi. Anzitutto può essere intesa come protezione contro il potenziale pregiudizio al diritto al rispetto della vita privata e familiare ai sensi dell'articolo 7 della Carta dei diritti fondamentali dell'UE e dell'articolo 8 della Convenzione europea Diritti umani. Essa è anche strettamente legata al concetto di confidenzialità che rappresenta un principio generale in ambito sanitario: si parla, infatti, di segreto medico sancito, ad esempio nel contesto italiano, nel Codice etico dei medici all'art. 10. Questa previsione richiama più in generale il celebre giuramento di Ippocrate che, nella sua versione antica e originale, così recita:

> Ciò che io possa vedere o sentire durante il mio esercizio o anche fuori dell'esercizio sulla vita degli uomini, tacerò ciò che non è necessario sia divulgato, ritenendo come un segreto cose simili.

Altro aspetto centrale è quello della sicurezza dei dati personali, in special modo in scenari come questi che vedono il trattamento sistematico di dati relativi alla salute che rientrano nella più generale categoria dei dati particolari [vedi → Capitolo 3]. L'accesso non autorizzato e l'uso illecito di dati sanitari sono rischi elevati in questo settore. Secondo la Commissione europea, un'efficace protezione dei dati è un fattore chiave per creare fiducia nell'*e-health* (come ribadito nel già citato «eHealth Action Plan 2012-2020»).

Rilevanza assume, poi, anche il tema della qualità dei dati, che dovrebbe rappresentare una priorità nei sistemi di sanità digitale. I dati sanitari devono essere accurati e aggiornati al fine di garantire un trattamento efficiente ed efficace. L'utilizzo di dati non corretti può, infatti, causare errori terapeutici e medici. Da questa prospettiva, la disciplina in materia di protezione dei dati personali è anche volta a preservare l'efficienza sanitaria e per garantire l'accuratezza dei dati.

Il diritto al rispetto della vita privata, i doveri di riservatezza e le leggi sulla protezione dei dati stabiliscono una serie di obblighi per la tutela dei diritti degli individui. La definizione ed organizzazione dell'intero processo relativo al trattamento dei dati fin dalla sua progettazione rappresenta l'unico modo per prevenire possibili criticità e per ridurre i rischi che sono intrinseci alla sanità digitale [vedi → Capitolo 4].

Infine, merita di essere ricordato che la direttiva 2011/24/UE sui diritti dei pazienti nell'assistenza sanitaria transfrontaliera promuove il diritto di accesso all'assistenza sanitaria e ai dati sanitari personali in qualsiasi Stato membro dell'UE[4]. Nel 2020, inoltre, la Commissione Europea ha presentato il progetto sulla creazione di uno spazio comune nell'area della salute denominato «European Health Data Space» (EHDS) nell'ambito della sua strategia europea per i dati. Secondo la Commissione questo spazio sarà essenziale per i progressi nella prevenzione, individuazione e cura delle malattie, nonché per decisioni informate e basate sull'evidenza per migliorare l'accessibilità, l'efficacia e la sostenibilità dei sistemi sanitari[5]. Da ultimo, la Commissione europea il 3 giugno 2022 ha presentato una proposta di Regolamento sullo spazio europeo dei dati sanitari al fine di: supportare le persone ad assumere il controllo dei propri dati; sostenere l'uso dei dati sanitari per migliorare l'erogazione dell'assistenza sanitaria, la ricerca, l'innovazione e l'elaborazione delle politiche; permettere all'UE di sfruttare le potenzialità offerte da uno scambio, utilizzo e riutilizzo sicuri dei dati sanitari.

Di seguito, senza alcuna pretesa di esaustività, alcuni scenari applicativi paradigmatici tra quelli che abbiamo visto caratterizzare il contesto della sanità digitale.

15.2 Il Fascicolo sanitario elettronico

15.2.1 Le funzionalità e le caratteristiche tecniche

Momento decisivo di tale processo di digitalizzazione è l'implementazione di sistemi di gestione posti in essere dalle aziende sanitarie al fine di potenziare le loro capacità di cura e prevenzione. Questi consistono in infrastrutture informatiche che prendono il nome di «dossier sanitario» e «Fascicolo Sanitario Elettronico» (FSE) [Guarda 2011 e Bincoletto

4 Come approfondimento si veda, European Commission. *Report from the Commission to the European Parliament and the Council on the operation of Directive 2011/24/EU on the application of patients' rights in cross-border healthcare*. European Commission. COM/2018/651 final, 2018.

5 Si veda EDPS, *Preliminary Opinion 8/2020 on the European Health Data Space*, 2020.

2021a, 229-283]. Il FSE rappresenta un importante strumento a disposizione di chi opera nel mondo sanitario ed ospedaliero. Esso si sostanzia in due momenti fondamentali: da un lato, quello dell'archiviazione di una massa di dati ed informazioni; dall'altro, quello della condivisione dei dati così archiviati tra tutti gli operatori del sistema legittimati al trattamento. Il FSE aiuta gli operatori sanitari a gestire meglio il trattamento del paziente con dati accurati, aggiornati e completi, consentendo un rapido accesso a un record digitale, che incorpora diagnosi e prescrizioni. Esso consente lo scambio di dati tra pazienti, operatori sanitari, medici e farmacie al fine di supportare sia gli individui che i medici nell'accesso e nell'erogazione delle cure. Accanto all'esigenza degli operatori sanitari di accedere ai dati del paziente per svolgere al meglio la propria attività diagnostico-curativa, si rende azionabile l'interesse da parte del paziente a svolgere un ruolo attivo nel processo di cura.

Tra le tante proposte nella letteratura scientifica, il FSE può essere definito come [Shabo 2017, 101]:

> a standard-based machine-processable information entity consisting of health data pertaining to an individual and resulting in an exhaustive aggregation of personal health data, which is longitudinal, cross-institutional and multi-modal.

Si possono elencare alcuni requisiti tipici [Bincoletto 2021a, 236-237 e Iakovidis 1988, 107]:

– «accessibilità e disponibilità»: consente l'accesso continuo ai dati del paziente o l'accesso tempestivo ad altre fonti di informazione;
– «affidabilità»: garantisce l'integrità dei dati e la permanenza delle informazioni originali nel formato concordato e per un determinato periodo di tempo;
– «usabilità e flessibilità»: supporta visualizzazioni multiple da parte dell'utente ed interazioni di facile utilizzo con il sistema;
– «integrazione»: consente l'integrazione di diversi sistemi informativi amministrativi e clinici, ad es. dalla farmacia all'ospedale;
– «prestazione»: garantita la fornitura di informazioni normalmente nell'arco di pochi secondi, attraverso sistemi di interrogazione e sorveglianza;

– «riservatezza e verificabilità»: fornisce un modello di controllo atto a documentare le interazioni con il sistema (ovvero l'accesso degli utenti), e utilizza sistemi di autenticazione e autorizzazione per il controllo degli accessi.

Cinque sono, invece, le componenti funzionali che vengono tipicamente implementate [Bincoletto 2021a, 237]:
– visualizzazione integrata dei dati del paziente, ad es. anamnesi, o diagnosi, da fonti diverse;
– sistema di supporto alle decisioni cliniche («clinical decision support system»), atti ad assistere il processo decisionale da parte del medico;
– inserimento di istruzioni da parte del medico, ad esempio relative a prescrizioni di terapie o farmaci;
– accesso a molteplici fonti di dati, come immagini da risultati di laboratorio o test radiologici;
– supporto integrato di comunicazione e refertazione, che consente l'integrazione elettronica dei messaggi nella cartella del paziente e le notifiche dei risultati medici.

Il FSE va, inoltre, tenuto concettualmente distinto dai sistemi informativi ospedalieri che sono deputati a gestire tutte le informazioni socio-sanitarie relative ai processi di cura e che possono semmai essere una delle fonti da cui il FSE collaziona dati. Da tale prospettiva quest'ultimo si pone semmai come una interconnessione logica tra diversi sistemi informativi. Il FSE va anche distinto dai c.d. «Personal Health Record» (PHR), i quali possono anche essere integrati in un ecosistema di FSE, ma rappresentano delle piattaforme di servizi online rivolti al cittadino, che si declinano in un'ampia gamma di applicazioni, modalità di accesso al FSE e di condivisione di dati tramite tale piattaforma, archiviazione diretta da parte del paziente di informazioni di carattere socio-sanitario che li riguardano. Strumento, quindi, che permette di costruire il processo di cura attorno al cittadino: questi, da spettatore passivo di decisioni a lui in larga misura inintelligibili, è messo ora in condizione di partecipare attivamente con una rinnovata autodeterminazione decisionale, la quale si lega a doppio filo ai profili di protezione dei dati personali.

15.2.2 Le implementazioni nazionali e le criticità con riferimento alla protezione dei dati personali

Il FSE è attualmente disponibile e adottato in tutti gli Stati membri dell'Unione europea. Il quadro giuridico con riferimento alla protezione dei dati è allora rappresentato dall'articolo 8 della Carta dei diritti fondamentali dell'UE, dal GDPR e dalla direttiva 2011/24/UE sui diritti dei pazienti nell'assistenza sanitaria transfrontaliera. Inoltre, si possono considerare anche il Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE (c.d. Regolamento eIDAS) e la Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.

Oltre a questo quadro generale, ogni Stato membro può prevedere norme specifiche. Il FSE è stato, infatti, oggetto di apposita regolamentazione nazionale attraverso leggi in ambito sanitario, discipline sui diritti dei pazienti e linee guida sulla protezione dei dati sanitari [Dumortier, Verhenneman 2013, 25-56].

Nel contesto italiano, ad esempio, a lungo il FSE non aveva trovato una definizione a livello legislativo. Tale vuoto era stato prima in parte «tamponato» da alcuni interventi del Garante per la protezione dei dati personali («Linee guida in tema di fascicolo sanitario elettronico (Fse) e di dossier sanitario, 16 luglio 2009»; «Linee guida in tema di referti online, 19 novembre 2009») e dai riferimenti delle linee guida emanate in sede di Conferenza permanente Stato, Regioni e Province Autonome (Intesa 10 febbraio 2011, n. 19/CSR, ai sensi dell'art. 8 comma 6, legge 5 giugno 2003, n. 131, tra il governo, le regioni e le province autonome di Trento e Bolzano sul documento recante «Il fascicolo sanitario elettronico – Linee guida nazionali». Rep. Atti n. 19/CSR del 10 febbraio 2011). Sul tema era intervenuto anche il WP29, «Documento di lavoro sul trattamento dei dati personali relativi alla salute contenuti nelle cartelle cliniche elettroniche (CCE)», adottato il 15 febbraio 2007. Da ultimo è intervenuto l'art. 12, d.l. 18 ottobre 2012, fornendone una prima definizione legislativa [Guarda, Ducato 2014, 397-402]:

> l'insieme dei dati e documenti digitali di tipo sanitario e socio-sanitario generati da eventi clinici presenti e trascorsi, riguardanti l'assistito.

Il FSE deve essere istituito dalle Regioni e dalle Province autonome, nel rispetto della normativa prevista in materia di protezione dei dati personali, per le seguenti finalità: a) prevenzione, diagnosi, cura e riabilitazione; b) studio e ricerca scientifica in campo medico, biomedico ed epidemiologico; c) programmazione sanitaria, verifica della qualità delle cure e valutazione dell'assistenza sanitaria[6].

In Francia, il *Dossier médical partagé* (DMP) archivia la storia medica dei pazienti francesi e consente la raccolta di tutti gli altri dati sanitari personali in aree specifiche in conformità con il *Code de la Santé publique*. Il dossier è popolato da tutti i professionisti abilitati dal paziente. In Lussemburgo, il FSE si chiama, invece, *Dossier de Soins Partagé* (DSP), e i servizi sono raggruppati con il termine *eSanté* [Bincoletto 2021a, 245-246].

I sistemi FSE possono essere centralizzati a livello nazionale o decentralizzati a livello locale [Dumortier, Verhenneman 2013].

Una definizione (giuridica) a livello europeo di FSE è fornita dal Gruppo art. 29 nel «Documento di lavoro sul trattamento dei dati personali relativi alla salute contenuti nelle cartelle cliniche elettroniche (CCE)» del 15 febbraio 2007, il quale ha fornito una prima guida sul quadro giuridico applicabile ai sistemi di FSE, stabilendo alcune essenziali indicazioni sui principi generali da seguire e le tutele da adottare:

---

6 La disciplina del FSE è integrata da decreti attuativi previsti all'art. 12, comma 7, d.l. n. 179/2012, volti a stabilire in particolare: i contenuti del FSE e del dossier farmaceutico; i limiti di responsabilità e i compiti dei soggetti che concorrono all'implementazione del FSE; i sistemi di codifica dei dati, le garanzie e le misure di sicurezza da adottare nel trattamento dei dati personali nel rispetto dei diritti dell'assistito; le modalità e i livelli diversificati di accesso al FSE da parte dei soggetti del Servizio sanitario nazionale e dei servizi socio-sanitari regionali che prendono in cura l'assistito, delle regioni e delle province autonome, nonché del Ministero del Lavoro e delle Politiche sociali e del Ministero della Salute nei limiti delle rispettive competenze attribuite dalla legge; la definizione e le relative modalità di attribuzione di un codice identificativo univoco dell'assistito che non consenta l'identificazione diretta dell'interessato; i criteri per l'interoperabilità del FSE a livello regionale, nazionale ed europeo, nel rispetto delle regole tecniche del sistema pubblico di connettività. V. il Decreto del presidente del Consiglio dei ministri 29 settembre 2015, n. 178, «Regolamento in materia di Fascicolo Sanitario Elettronico».

> Una documentazione medica completa o documentazione analoga sullo stato di salute fisico e mentale, passato e presente, di un individuo, in forma elettronica, e che consenta la pronta disponibilità di tali dati per cure mediche ed altri fini strettamente collegati.

Gli aspetti relativi alla protezione dei dati ed alla riservatezza assumono un ruolo rilevante [Bincoletto 2021a, 248-262].

In primo luogo, è necessario chiarire i soggetti ed i loro ruoli nel trattamento dei dati personali. Ogni operatore sanitario o farmacista persegue la propria finalità (es. fornitura di cure o vendita di farmaci) e di regola determina i propri mezzi per il trattamento (es. il sistema). Pertanto, nell'ambiente FSE potrebbero esserci tanti titolari del trattamento quanti sono gli attori coinvolti. Potremmo poi avere situazioni di contitolarità.

In secondo luogo, vanno svolte alcune considerazioni sulla base legittima del trattamento. Sul punto si dovrebbe poter affermare che ai sensi del GDPR il trattamento dei dati sanitari contenuti nel FSE possa avvenire senza il consenso, stante l'apposita «eccezione sanitaria» prevista all'art. 9, par. 2, lett. h). Questa si applica quando il trattamento di dati è necessario per le finalità ivi elencate e l'attività è svolta da un professionista sanitario o da una persona soggetta al segreto professionale. Va, inoltre, ricordato che ogni Stato membro a livello di diritto nazionale potrà diversamente specificare l'eventuale necessità della richiesta del consenso o di altra base giuridica che legittimi il trattamento posto in essere dal FSE. Tale potere è riconosciuto dal paragrafo 4 dell'art. 9. Ad esempio, in Italia, il già citato d.l. 179/2012 all'art. 12, co. 5, prevedeva la necessità del consenso dell'interessato per l'alimentazione del FSE e la condivisione delle informazioni tra gli operatori sanitari. Durante l'emergenza COVID-19, il d.l. 19 maggio 2020 n. 34 ha modificato l'articolo 12 eliminando il requisito del consenso. Il Garante ha evidenziato che per le finalità sanitarie il consenso non è necessario per il trattamento, ma per quanto riguarda il FSE[7]:

> l'acquisizione del consenso, quale condizione di liceità del trattamento, è richiesta dalle disposizioni di settore, precedenti all'applicazione

7 Si v. Doc-Web 9091942 del 7 marzo 2019, www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9091942. e Doc-Web 9351203 del 25 maggio 2020, www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9351203.

del Regolamento, il cui rispetto è ora espressamente previsto dall'art. 75 del Codice.

Esso rimane, pertanto, richiesto per autorizzare l'accesso alle informazioni da parte degli operatori sanitari e garantire il diritto all'autodeterminazione del paziente [Foglia 2020]. In Francia, invece, ai sensi del «Décret n°2016-914 del 4 luglio 2016 e del Code de la Santé publique», il consenso è necessario per la creazione del DMP e per il livello di accesso dei professionisti[8].

La discrezionalità concessa agli Stati membri potrebbe ostacolare l'accesso a un'assistenza sanitaria transfrontaliera sicura e di alta qualità che è, invece, fortemente promossa dall'UE. Laddove il diritto nazionale non preveda una norma specifica, l'articolo 9, par. 2, lett. h), del GDPR può costituire una base giuridica legittima per la raccolta di dati nel sistema FSE.

Infine, una parte importante giocano anche tutte le garanzie che devono essere adottate nella strutturazione di questo tipo di trattamento di dati: sistemi di autenticazione e autorizzazione, la gestione dei flussi di dati, l'adozione di misure idonee di sicurezza di tipo tecnico ed organizzativo, il concreto riconoscimento dei diritti che il GDPR riconosce in capo all'interessato del trattamento.

15.2.3 L'analisi di un caso

L'ospedale portoghese di Barreiro aveva concesso l'accesso indiscriminato ai dati dei pazienti a livello medico a 985 persone, sebbene in quella struttura operassero solo 296 professionisti. L'Autorità Garante per la protezione dei dati portoghese («Comissão Nacional de Protecção de Dados») CNPD ha applicato una sanzione di 400.000 euro per violazione del GDPR, mancato rispetto della riservatezza del paziente e per la limitazione dell'accesso ai dati dei pazienti[9] [Bincoletto 2021a, 262-264].

Questo un breve schema volto a riassumere gli elementi rilevanti:

8 www.dmp.fr/patient/faq.

9 Deliberação n. 984/2018 https://www.cnpd.pt/umbraco/surface/cnpdDecision/download/121680.

– violazione dell'art. 5, par. 1, lett. c) e f) GDPR in tema di minimizzazione e sicurezza dei dati:
  • a seguito di un sopralluogo, l'autorità ha riscontrato che il sistema per la gestione del paziente non era conforme a questi due principi in quanto l'accesso ai dati personali non era stato limitato;
  • l'ospedale non ha messo in atto misure tecniche e organizzative volte a limitare i sistemi di identificazione ed autenticazione degli utenti in base alle varie categorie di operatori sanitari coinvolti che avrebbero dovuto corrispondere a diversi livelli di accesso (art. 32 GDPR);
  • la sicurezza dei dati personali non era garantita perché le misure di sicurezza adottate non erano adeguate e non era stato previsto alcun processo di audit per i meccanismi di accesso;
  • l'accesso ai dati era garantito in modo del tutto indiscriminato e non invece limitato a casi occasionali e preventivamente giustificati;
– nel valutare l'ammontare della sanzione amministrativa comminata l'Autorità portoghese ha tenuto in considerazione quanto previsto agli artt. 25 e 32 del GDPR considerando la violazione di elevata gravità, in quanto l'ospedale aveva permesso che un gruppo di operatori sanitari con semplice «profilo tecnico» potessero avere invece i privilegi garantiti ai medici:
  • era responsabilità dell'ospedale assicurare il controllo delle contingenti necessità di accesso ai dati e di cancellazione dei profili obsoleti, anche mediante l'adozione di adeguate procedure di audit;
  • si può, quindi, sostenere che non era stata posta in essere una corretta valutazione del rischio e che il sistema di gestione del paziente non era stato progettato correttamente.

15.3 Telemedicina e mobile health

Altro scenario applicativo di rilevante interesse è quello rappresentato dalla c.d. «telemedicina», che rimanda all'utilizzo di tecnologie informatiche, di sistemi informativi e di telecomunicazione nel campo della me-

dicina in contesti nei quali il professionista della salute ed il paziente non sono nello stesso luogo [Bincoletto 2021b e Botrugno 2014][10].

L'Organizzazione Mondiale della Sanità (OMS) definisce la telemedicina come:

> the delivery of health care services, where distance is a critical factor, by all health care professionals using information and communication technologies for the exchange of valid information for diagnosis, treatment and prevention of disease and injuries, research and evaluation, and for the continuing education of health care providers, all in the interests of advancing the health of individuals and their communities[11].

Si enfatizzano così l'importanza che il paziente assuma un ruolo sempre più attivo e centrale nei processi curativi che lo riguardano.

L'emergenza sanitaria da SARS-CoV-2 ha fortemente incentivato l'utilizzo di questi servizi sia per monitorare e contenere il contagio da coronavirus, sia per la teleassistenza di pazienti affetti da particolari patologie, quali le malattie croniche, con ciò favorendo anche lo sviluppo e la sperimentazione di nuove soluzioni[12].

La telemedicina non costituisce un trattamento alternativo, atto a sostituire la tradizionale relazione medico-paziente[13], bensì consiste in uno

---

10 Si v. Commissione delle Comunità Europee, *Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e sociale europeo e al Comitato delle Regioni sulla telemedicina a beneficio dei pazienti, dei sistemi sanitari e della società*, COM(2008)689 definitivo, Bruxelles 4.11.2008, p. 3.

11 Si v. World Health Organization, *Telemedicine: opportunities and developments in Member States: report on the second global survey on eHealth*, 2010, https://apps.who.int/iris/handle/10665/44497. Si v. anche World Health Organization, *WHO Guideline: recommendations on digital interventions for health system strengthening*, 2019, https://apps.who.int/iris/handle/10665/311980.

12 OMS, *Implementing telemedicine services during COVID-19: guiding principles and considerations for a stepwise approach*, maggio 2021, https://iris.wpro.who.int/bitstream/handle/10665.1/14651/WPR-DSE-2020-032-eng.pdf. si v. anche *Indicazioni ad interim per servizi sanitari di telemedicina in pediatria durante e oltre la pandemia COVID-19. Versione del 10 ottobre 2020* dell'Istituto Superiore di Sanità, https://www.iss.it/documents/20126/0/Rapporto+ISS+COVID-19+60_2020.pdf/6b4dfc13-fc37-fadd-3388-b93aef43a15d?t=1602857089054.

13 V. anche Comunicazione COM(2008)689 «*Telemedicina a beneficio dei pazienti, dei sistemi sanitari e della società*»; Parere del CESE sulla telemedicina su

strumento che va a potenziare l'erogazione della prestazione sanitaria, cercando di ridurre i limiti legati alla distanza tra i soggetti coinvolti.

I sistemi di telemedicina riguardano soluzioni tecnologiche sia di tipo hardware che software volte a raccogliere, conservare e scambiare informazioni relative allo stato di salute degli individui al fine di consentire una visita medica e un confronto a distanza tra il medico e il paziente (televisita), o un monitoraggio remoto del paziente affetto da una particolare patologia cronica (telemonitoraggio) [Bincoletto 2021b, 383].

Una nuova frontiera dell'applicazione delle tecnologie digitali all'ambito sanitario è costituita dalle c.d. «m-health app», ovvero il perseguimento degli obiettivi propri del servizio sanitario attraverso l'utilizzo di smartphone e altri strumenti mobile. L'OMS ci fornisce una possibile definizione:

> (…) the Global Observatory for eHealth (GOe) defined mHealth or mobile health as medical and public health practice supported by mobile devices, such as mobile phones, patient monitoring devices, personal digital assistants (PDAs), and other wireless devices[14].

L'uso sempre più massivo e la crescente diffusione presso il pubblico di *app* sanitarie, oltre alla consapevolezza di rischi specifici che tali nuove tecnologie possono ingenerare nel trattamento dei dati personali, hanno portato la Commissione europea a focalizzare la propria attenzione sul fenomeno. Nonostante, infatti, i possibili vantaggi di tale forma di assistenza siano evidenti, diverse e variegate sono le criticità che l'uso di questo tipo di tecnologie sollevano.

A livello europeo l'«eHealth Action Plan 2012-2020»[15] e il «Green Paper on mobile Health»[16] del 2014 avevano fin da subito sottolineato le

---

COM(2008)689, 15 luglio 2009.

14 OMS, *mHealth: New horizons for health through mobile technologies: second global survey on eHealth*, 2011, https://www.who.int/goe/publications/goe_mhealth_web.pdf.

15 Commissione Europea, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions*, *eHealth Action Plan 2012-2020 Innovative healthcare for the 21st century*, COM/2012/0736 final.

16 Commissione Europea, *Green Paper on mHealth*, cit.

potenzialità di cui si caratterizza la telemedicina, proponendo un piano strategico teso ad abbattere le barriere al suo utilizzo.

Il fenomeno delle *mHealth app* è stato studiato con attenzione negli ultimi anni. Nonostante i possibili vantaggi di tale forma di assistenza sanitaria di frontiera, queste tecnologie sollevano varie questioni di conformità con le regole e i principi dell'ordinamento giuridico [Bincoletto 2021b, 385-386 e Mulder 2019]. Da ultimo la Commissione europea nel 2018 ha analizzato, con metodo interdisciplinare, il mercato dei servizi di telemedicina a livello internazionale, mettendo in rilievo come l'utilizzo di questi applicativi sia sempre più diffuso a livello sanitario ma anche come esistono numerose criticità di tipo economico sociale e tecnico, oltre che a barriere regolative e di policy[17].

Venendo, per concludere, al contesto italiano, a partire dagli anni '90 il Consiglio Superiore della Sanità, il Ministero della Salute e le attività di coordinamento con le Regioni e Province autonome hanno prodotto vari documenti di soft law in tema di telemedicina [Botrugno 2014, 639-668 e Bincoletto 2021b, 390-395].

Le «Linee di indirizzo nazionali sulla Telemedicina» del 10 luglio 2012 del Consiglio Superiore della Sanità hanno assunto un ruolo centrale per lo sviluppo dei servizi nell'ambito del Servizio Sanitario Nazionale (SSN), soprattutto a seguito dell'intesa sul documento tra il Governo, le Regioni e le Province autonome di Trento e Bolzano, che è avvenuta nel 2014[18]. Di seguito le finalità essenziali della telemedicina:

– *prevenzione secondaria*, relativa a persone già affette da particolari patologie che richiedono un monitoraggio ai fini di prevenire eventuali complicazioni;
– *diagnosi*, a supporto del tradizionale iter diagnostico;
– *cura*, a supporto di scelte terapeutiche e dell'andamento prognostico, come nel caso di servizi di teledialisi o di interventi chirurgici a distanza;
– *riabilitazione*, nel caso di servizi che avvengono presso il domicilio del paziente;

17 European Commission Consumers, Health, Agriculture and Food Executive Agency, *Provision of a market study on telemedicine*, 2018, https://www.digitalhealthnews.eu/images/stories/pdf/2018_provision_marketstudy_telemedicine_en.pdf.

18 http://www.salute.gov.it/portale/documentazione/p6_2_2_1.jsp?lingua=italiano&id=2129.

– *monitoraggio*, che consisterebbe nella gestione, anche nel tempo, di parametri vitali del paziente, grazie allo scambio di dati tra il soggetto e una postazione di monitoraggio per l'interpretazione dei dati stessi.

I servizi di telemedicina vengono, inoltre, classificati in tre macro-aree[19]:

1. la telemedicina specialistica, relativa ad una specifica disciplina medica, e che comprende la televisita, il teleconsulto (i.e. consulenza a distanza tra più medici) e la telecooperazione sanitaria (i.e. assistenza di un medico ad un altro professionista durante un atto sanitario);
2. la telesalute, che include il telemonitoraggio;
3. la teleassistenza (i.e. sistema socio-assistenziale a domicilio).

La televisita può essere definita come:

> un atto sanitario in cui il medico interagisce a distanza con il paziente. L'atto sanitario di diagnosi che scaturisce dalla visita può dar luogo alla prescrizione di farmaci o di cure. Durante la Televisita un operatore sanitario che si trovi vicino al paziente, può assistere il medico. Il collegamento deve consentire di vedere e interagire con il paziente e deve avvenire in tempo reale o differito[20].

Il telemonitoraggio, invece, riguarda una macrocategoria di servizi di telemedicina che possono

> migliorare la qualità della vita dei pazienti cronici attraverso soluzioni di auto-gestione e monitoraggio remoto, anche ai fini di una de-ospedalizzazione precoce[21].

---

19 Si v. pp. 11-17 delle Linee di indirizzo.

20 Si v. p. 11 delle Linee di indirizzo.

21 Si v. p. 7 delle Linee di indirizzo. Nel 2008 la Commissione Europea ha adottato una nozione più ampia di telemonitoraggio, definendolo come un «servizio di telemedicina il cui obiettivo è di sorvegliare le condizioni di salute dei pazienti a distanza», grazie ad una raccolta di dati che può avvenire o automaticamente tramite l'ausilio di dispositivi di controllo, o tramite la collaborazione attiva del paziente, come nel caso di inserimento di misurazioni di parametri. Si v. Commissione delle Comunità Europee, *Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e sociale europeo e al Comitato delle Regioni sulla teleme-*

Nella visione del Consiglio Superiore di Sanità [Bincoletto 2021b, 391],

> il telemonitoraggio è una *species* del *genus* telesalute, che consiste nell'uso di sistemi e di servizi digitali che collegano i pazienti con il medico che li ha presi in carico. I dati raccolti dai sistemi vengono condivisi con l'operatore sanitario per ottimizzare il trattamento del paziente, ridurre le visite e le ospedalizzazioni e adottare misure correttive tempestive del piano di cura. Questo concetto di monitoraggio è particolarmente utilizzato per pazienti affetti da malattie croniche, come il diabete mellitico e l'insufficienza cardiaca cronica.

Nel 2008 la «Commissione Europea nella Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e sociale europeo e al Comitato delle Regioni sulla telemedicina a beneficio dei pazienti, dei sistemi sanitari e della società» COM(2008)689 definitivo, Bruxelles 4.11.2008 ha proposto una definizione che tratteggia una nozione più ampia di telemonitoraggio, definendolo come

> un servizio di telemedicina il cui obiettivo è di sorvegliare le condizioni di salute dei pazienti a distanza. La raccolta dei dati può avvenire o automaticamente, tramite dispositivi di controllo personale della salute, o tramite la collaborazione attiva del paziente (ad esempio inserendo in uno strumento basato su l web le misurazioni del peso o dei livelli glicemici quotidiani). Una volta elaborati e condivisi con i professionisti della sanità competenti, i dati possono esse re utilizzati per ottimizzare i protocolli di controllo e trattamento del paziente.

Da ultimo il 17 dicembre 2020, la Conferenza Permanente per i rapporti tra lo Stato, le Regioni, e le Province Autonome di Trento e Bolzano ha pubblicato un accordo sul documento «Indicazioni nazionali per l'erogazione di prestazioni di telemedicina»[22] che fornisce ulteriori specifica-

---

dicina a beneficio dei pazienti, dei sistemi sanitari e della società, COM(2008)689 definitivo, Bruxelles 4.11.2008, p. 4.

22 Conferenza Permanente per i rapporti tra lo Stato, le Regioni, e le Province Autonome di Trento e Bolzano, *Accordo sul documento recante "Indicazioni nazionali per l'erogazione di prestazioni in telemedicina"*, 2020, http://www.statoregioni.it/media/3221/p-3-csr-rep-n-215-17dic2020.pdf.

zioni chiave a livello organizzativo e tecnologico, anzitutto classificando i servizi di telemedicina in quattro tipologie di prestazioni sanitarie:

1. prestazioni assimilabili ad una qualsiasi prestazione sanitaria diagnostica e/o terapeutica tradizionale, diventandone un'alternativa di erogazione;
2. prestazioni che non possono in nessun modo sostituire una prestazione sanitaria tradizionale, ma possono invece supportarla e renderla meglio accessibile e/o aumentarne l'efficienza e l'equità distributiva;
3. prestazioni che possono integrare in varia proporzione una prestazione tradizionale e renderla più efficace e più capace di adattarsi in modo dinamico ai cambiamenti delle esigenze di cura;
4. prestazioni che possono completamente sostituire una prestazione sanitaria tradizionale, diventando un nuovo metodo e/o tecnica diagnostica e/o terapeutica, e così creando una nuova prassi assistenziale.

La telemedicina, in tutte le sue declinazioni, rappresenta una chiara sfida da un punto di vista dell'applicazione della privacy. Il ruolo centrale del paziente va gestito ed inserito all'interno di un ecosistema di servizi sanitari avanzati che mettano al primo punto il rispetto della riservatezza e della protezione dei dati personali.

15.4 Sanità digitale ed intelligenza artificiale

Da anni il settore sanitario è fortemente interessato dall'utilizzo di tecnologie basate sull'intelligenza artificiale [vedi → Capitolo 13] [Nicholson Price 2017 e Guarda 2019]. Ciò è stato sicuramente favorito dall'incessante sviluppo di tecnologie basate su sofisticate tecniche di machine learning e dall'enorme disponibilità di informazioni che l'era dei Big Data consente. Le possibili fonti di dati in questo scenario sono le più disparate: FSE, letteratura medica, studi clinici, dati sui sinistri assicurativi, cartelle cliniche, dati inseriti dai pazienti o registrati su fitness tracker, ecc. La confluenza di questi due fattori ha determinato una notevole spinta verso lo sviluppo e il perfezionamento di metodiche di medicina personalizzata [Hoffman, Podgurski 2014].

Ci sono molte aspettative e speranze per l'applicazione delle tecniche di IA in campo medico. Innanzitutto, la possibilità di sviluppare modelli predittivi con evidenti vantaggi in termini di prevenzione. In secondo luogo, la capacità di fornire diagnosi tempestive, al fine di garantire una pronta reazione con le cure più appropriate. Infine, l'affermazione degli ambienti basati su *chatbot* promette di garantire un corretto livello di informazione ai pazienti, accompagnandoli nei loro processi di cura.

L'IA potrebbe essere in grado di risolvere molti problemi in diversi contesti di *e-health*. Gli assistenti virtuali intelligenti, ora integrati anche negli smartphone, negli home speaker o nei dispositivi domestici delle persone (come Amazon Alexa o Google Assistant) sono supportati da sistemi con potenti funzionalità. Questi strumenti rappresentano oggi la frontiera più accattivante dell'uso dell'IA nella vita di tutti i giorni: gli utenti sono, infatti, in grado di porre domande, controllare dispositivi e riprodurre contenuti multimediali tramite la voce, gestendo al contempo altre attività di base come e-mail e calendari con comandi verbali. Ovviamente le criticità privacy e di sicurezza non sono di poco momento [Guarda, Petrucci 2020]. Essi possono, però, rappresentare un valore aggiunto, in special modo se abbinati alle app sanitarie, garantendo un'integrazione nelle applicazioni mediche quotidiane, migliorando così l'efficienza del trattamento. Tutto ciò facilitando anche, ad esempio, una più mirata pianificazione pre-operatoria o supportare le fasi post-operatorie.

Anche condizioni particolari che richiedono piani di trattamento elaborati potrebbero trarre vantaggio dagli strumenti di intelligenza artificiale durante specifiche terapie. Incorporare un sistema di IA in grado di formulare automaticamente piani basati su condizioni specifiche fornirebbe un supporto fondamentale sia ai medici che ai pazienti. È il caso degli ecosistemi progettati per innovare i processi di interazione tra medico e paziente, con un evidente impatto anche sui modelli organizzativi che regolano la prestazione dei servizi sanitari. Questi sistemi intelligenti possono cercare incongruenze, errori e omissioni in un piano di trattamento esistente o possono essere utilizzati per formulare un trattamento basato sulla condizione specifica del paziente e su linee guida terapeutiche condivise. L'agente intelligente può, inoltre, essere utilizzato per trovare informazioni, ad esempio su Internet, rilevanti per una particolare malattia, integrare la conoscenza delle preferenze e dei

bisogni dell'utente in tali ricerche, o per interpretare automaticamente immagini mediche (es. raggi X, angiogrammi, TAC, ecc.). Infine, i sistemi di supporto alle decisioni, programmati per aggregare e archiviare una grande quantità di dati modellati per scopi specifici, possono essere utilizzati con successo nel campo dei dispositivi medici nelle applicazioni di monitoraggio cardiaco ed ECG automatizzato, imaging medico, analisi di laboratorio clinico, e così via.

Uno strumento molto famoso – sebbene sia discussa la sua reale efficacia – è rappresentato in tale contesto da «IBM Watson»[23] [Chung, Zink 2018]. Comunemente descritto come un «sistema esperto», questo utilizza l'IA per risolvere problemi definiti in un'area tematica specializzata. Watson incorpora il software «DeepQA» e dispone di un'architettura informatica che analizza, ragiona ed interagisce con i contenuti inseriti nel sistema. È stato alimentato con informazioni di tipo ontologico provenienti da riviste mediche, opere di approfondimento, protocolli curativi, ecc.: milioni e milioni di pagine di testo che è in grado di studiare ed analizzare al fine di proporre ai medici opzioni terapeutiche, prescrizioni farmacologiche e istruzioni per la somministrazione. Questa capacità grezza di analizzare i dati è combinata con l'addestramento fornito dai medici che operano negli istituti di cura.

Le premesse per usi più estesi dell'IA nell'assistenza sanitaria ci sono tutte. Tuttavia, alcune criticità ne ostacolano la definitiva affermazione. Mancano studi clinici che possano dimostrare affidabilità e maggiore efficacia rispetto ai sistemi tradizionali nel fare previsioni, diagnosi o suggerire terapie appropriate: ciò provoca una certa sfiducia da parte dei medici nei confronti del loro utilizzo e un limite anche per i decisori politici a spingere per la loro definitiva adozione. Inoltre, la questione relativa all'attribuzione di responsabilità in caso di errori medici presenta criticità non ancora del tutto analizzate e risolte dalla dottrina [Schweikart 2021]. Infine, gli aspetti etici giocano un ruolo essenziale, non solo in termini di perdita di posti di lavoro (o meglio di trasformazione di questi), ma soprattutto per gli scenari futuri, e in parte distopici, che l'emergere di queste tecnologie a volte suggerisce [Mittelstadt, Allo, Taddeo, Wachter, Floridi 2016].

23 https://www.ibm.com/watson.

15.5 Caso 15-1

Caso 15-1

Un paziente è sottoposto ad un trattamento di telemedicina. Attraverso una specifica app mobile egli ha la possibilità di inserire nel suo Personal Health Record (PHR) un insieme di informazioni riguardanti il suo stato di salute. Il paziente è in grado di condividere queste informazioni con il Diabetologo che lavora all'interno dell'Azienda sanitaria che lo ha in cura. Lo specialista può così, attraverso una dashboard dedicata, accedere ai dati inseriti dalla paziente e fornirgli le indicazioni mediche e terapeutiche necessarie. Inoltre, il paziente, al fine di avvalersi dell'assistenza di una persona di fiducia nella gestione dei propri dati sanitari, delega l'accesso del proprio PHR (e quindi anche ai dati relativi al trattamento di telemedicina) ad un proprio familiare.
Qual è la base giuridica di questo trattamento?
Qual è l'allocazione corretta dei ruoli privacy?
Quali sono le criticità di questo scenario applicativo?
Quali le misure adeguate da adottare in tale contesto?

CAPITOLO 16.
Privacy e ricerca scientifica

Paolo Guarda

16.1 Protezione dei dati personali e ricerca: la disciplina europea ed italiana

La ricerca scientifica è elemento imprescindibile per garantire lo sviluppo della conoscenza e, più in generale, il progresso della scienza.

Dopo l'entrata in vigore del GDPR, è sorto un acceso dibattito circa l'impatto che la nuova normativa avrebbe avuto sulla ricerca. L'equilibrio tra la tutela dei diritti fondamentali e la libera circolazione dei dati rende, infatti, i ricercatori responsabili di una serie di obblighi per l'intera durata del ciclo di vita della ricerca [Ducato 2020 e Manis 2017].

La Direttiva 95/46/CE già prevedeva una disciplina improntata ad un evidente *favor* per le attività di trattamento di dati personali per finalità di ricerca. Il GDPR non ha cambiato il generale approccio di favore, ma ha sicuramente modificato e ampliato la regolamentazione [Guarda 2021, 134 ss.] creando un regime di deroghe ad alcune regole generali, sempre in presenza di adeguate garanzie.

La norma di riferimento è qui l'art. 89 il quale prevede che:

> 1. Il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici è soggetto a garanzie adeguate per i diritti e le libertà dell'interessato, in conformità del presente regolamento. Tali garanzie assicurano che siano state predisposte misure tecniche e organizzative, in particolare al fine di garantire il rispetto del principio della minimizzazione dei dati. Tali misure possono includere la pseudonimizzazione, purché le finalità in questione possano

essere conseguite in tal modo. Qualora possano essere conseguite attraverso il trattamento ulteriore che non consenta o non consenta più di identificare l'interessato, tali finalità devono essere conseguite in tal modo.

2. Se i dati personali sono trattati a fini di ricerca scientifica o storica o a fini statistici, il diritto dell'Unione o degli Stati membri può prevedere deroghe ai diritti di cui agli articoli 15, 16, 18 e 21, fatte salve le condizioni e le garanzie di cui al paragrafo 1 del presente articolo, nella misura in cui tali diritti rischiano di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità specifiche e tali deroghe sono necessarie al conseguimento di dette finalità.

3. Se i dati personali sono trattati per finalità di archiviazione nel pubblico interesse, il diritto dell'Unione o degli Stati membri può prevedere deroghe ai diritti di cui agli articoli 15, 16, 18, 19, 20 e 21, fatte salve le condizioni e le garanzie di cui al paragrafo 1 del presente articolo, nella misura in cui tali diritti rischiano di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità specifiche e tali deroghe sono necessarie al conseguimento di dette finalità.

4. Qualora il trattamento di cui ai paragrafi 2 e 3 funga allo stesso tempo a un altro scopo, le deroghe si applicano solo al trattamento per le finalità di cui ai medesimi paragrafi.

Per poter trattare i dati personali il titolare del trattamento deve, pertanto, adottare adeguate garanzie e misure di natura tecnica ed organizzativa, valutate sulla base di un'analisi dei concreti rischi e della specificità del contesto applicativo [Wiese Svanber 2020]. Aspetti chiave sono la protezione della sicurezza dei dati ai sensi dell'art. 32 GDPR e l'osservanza del principio di minimizzazione, che richiede che i dati personali siano «adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati» (art. 5, par. 1, lett. c), GDPR).

Le misure di minimizzazione si estrinsecano in concreto in tecniche di anonimizzazione o pseudonimizzazione che limitano i dati personali utilizzabili durante le operazioni di trattamento (Gruppo art. 29, Parere 5/2014) [Tosoni 2020, Foglia 2019 e Stalla-Bourdillon, Knight 2017] [vedi → Capitolo 14]. Le soluzioni tecniche e organizzative adottate dovranno avere un intrinseco carattere dinamico e saranno volte a prevenire rischi di tipo giuridico, etico e sociale.

Il Regolamento europeo ha, in realtà, lasciato ampio spazio e libertà agli Stati membri di derogare i principi e prevedere nuove e specifiche garanzie (Cons. 156) [TIPIK 2021]. Tale possibilità a livello nazionale rappresenta, in qualche modo, un limite rispetto all'intento di uniformare il diritto della disciplina dei dati personali europei. Il settore della ricerca scientifica potrebbe, quindi, essere regolato difformemente negli Stati membri, con piccole e grandi differenze. Ciò potrebbe ricreare quella serie di ostacoli e barriere che si riteneva di voler superare con il nuovo intervento normativo rispetto all'implementazione della direttiva.

L'art. 89 non definisce le finalità di ricerca storica, archiviazione nel pubblico interesse e ricerca scientifica e statistica. I considerando del GDPR offrono, però, alcune indicazioni utili.

Per quanto riguarda la ricerca storica il considerando 160 afferma che:

> Qualora i dati personali siano trattati a fini di ricerca storica, il presente regolamento dovrebbe applicarsi anche a tale trattamento. Ciò dovrebbe comprendere anche la ricerca storica e la ricerca a fini genealogici, tenendo conto del fatto che il presente regolamento non dovrebbe applicarsi ai dati delle persone decedute.

Si segnala un'importante novità rispetto al quadro normativo precedente. Questo tipo di trattamento è, infatti, ora ben distinto dall'archiviazione nel pubblico interesse, di cui si dirà subito sotto, sottolineando così la differenza funzionale tra i due ambiti. Il primo è concettualmente e strutturalmente diverso dal secondo: archiviazione è attività culturale in sé e per sé considerata, semmai, prodromica alla finalità di ricerca [Ducato 2020, 2 e Uda 2019, 560]. L'archiviazione nel pubblico interesse riguarda, pertanto, i servizi effettuati da autorità pubbliche o altri organismi che hanno un obbligo giuridico di (Cons. 158 GDPR)

> acquisire, conservare, valutare, organizzare, descrivere, comunicare, promuovere, diffondere e fornire accesso a registri con un valore a lungo termine per l'interesse pubblico generale.

Ci si riferisce, ad esempio, al trattamento posto in essere da parte degli archivi di stato, archivi storici tenuti da enti pubblici, attività archivistica effettuata da altri organismi culturali cui il diritto nazionale o dell'unione attribuisca tale specifica funzione istituzionale. La distinzione non è di

poco momento da un punto di vista pratico-applicativo: come presto si dirà gli Stati membri potranno, infatti, prevedere limitazioni all'esercizio del diritto di accesso (art. 15), rettifica (art. 17), limitazione (art. 18) e opposizione al trattamento (art. 21) nel caso di ricerca per finalità storica ai sensi dell'art. 89, par. 2. Se, invece, la finalità fosse di archiviazione nel pubblico interesse l'art. 89, par. 3 prevede che le limitazioni possano essere introdotte anche per l'obbligo di notifica per rettifica o cancellazione (art. 19) e per il diritto alla portabilità dei dati (art. 20).

La ricerca scientifica è definita in modo molto ampio fino ad abbracciare qualsiasi attività atta a generare nuova conoscenza e ad avanzare lo stato dell'arte in un determinato settore scientifico. Il considerando 159 ne fornisce alcuni esempi, quali:

> sviluppo tecnologico e dimostrazione, ricerca fondamentale, ricerca applicata e ricerca finanziata da privati. (…). Le finalità di ricerca scientifica dovrebbero altresì includere gli studi svolti nell'interesse pubblico nel settore della sanità pubblica.

In tale categoria non vanno considerate solo le c.d. STEM («Science, Technology, Engineering and Mathematics») ma anche le scienze di carattere sociale e umanistico (Cons. 157).

Per la ricerca statistica, infine, si può fare riferimento al considerando 162 che la identifica in

> qualsiasi operazione di raccolta e trattamento di dati personali necessari alle indagini statistiche o alla produzione di risultati statistici.

I dati derivanti da un processo statistico sono, comunque, di tipo aggregato e quindi il risultato non può consistere in dati che siano riferibili ad un soggetto in particolare. I confini tra la ricerca scientifica e quella statistica non sono sempre così ben delineati. Vengono individuate due caratteristiche peculiari al trattamento per fini statistici: questo è diretto a creare la base di conoscenza per future ricerche (magari in ambito scientifico) ed esclude espressamente una ricaduta personalizzata sugli individui [Guarda 2021, 139 e Ducato 2020, 3].

In presenza delle garanzie richieste dall'art. 89, par. 1, GDPR si applica un regime che consente la deroga ad alcuni principi del trattamento dei dati personali ed all'esercizio di una serie di diritti dell'interessato.

In primo luogo, è consentita una deroga al principio di limitazione delle finalità. L'art. 5, par. 1, lett. b), GDPR così recita:

> un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»).

Per ricerche scientifiche, storiche e statistiche o per archiviazioni nel pubblico interesse sarebbe consentito un ulteriore trattamento dei dati rispetto all'originaria e diversa finalità perseguita dal titolare del trattamento perché considerate ad essa compatibili da una regola generale del medesimo principio (Gruppo art. 29, «Opinion 3/2013 on Purpose limitation», 2 aprile 2013). Il trattamento secondario ai fini di archiviazione nel pubblico interesse, o di ricerca scientifica o storica o a fini statistici dovrebbe essere considerato un trattamento lecito e compatibile, quando il trattamento originario è lecito e tenendo conto del «contesto in cui i dati personali sono stati raccolti», delle «ragionevoli aspettative dell'interessato in base alla sua relazione con il titolare del trattamento con riguardo al loro ulteriore utilizzo», «della natura dei dati personali», «delle conseguenze dell'ulteriore trattamento previsto per gli interessati», e «dell'esistenza di garanzie adeguate sia nel trattamento originario sia nell'ulteriore trattamento previsto» (Cons. 50 GDPR). La deroga al principio di limitazione della finalità per i trattamenti secondari di ricerca e archiviazione semplifica le regole ordinarie e permette il riuso di dati personali che siano già stati legittimamente raccolti per altre finalità. EDPS, nella sua «Opinione preliminare sulla protezione dei dati e ricerca scientifica» del 2020, propende per un'interpretazione restrittiva: non sarebbe possibile considerare di per sé compatibile il riuso dei dati per scopi di ricerca, ma si dovrebbe effettuare in ogni caso il test di compatibilità di cui all'art. 6, par. 4, GDPR, in quanto non sarebbe possibile assimilare le condizioni di legittimità dell'ulteriore trattamento con la de-

terminazione della prima finalità[1]. Tale presunzione di compatibilità dipenderebbe, pertanto, dalla valutazione di alcuni aspetti specifici, quali: 1) la natura dei dati personali, in particolare nel caso in cui siano trattate categorie particolari di dati (art. 6, par. 4, c) GDPR); 2) il collegamento fra lo scopo originario e gli scopi secondari (art. 6, par. 4, lett. a) GDPR); 3) le ragionevoli aspettative dell'interessato in base alla sua relazione con il titolare del trattamento con riguardo al loro ulteriore utilizzo (art. 6, par. 4, lett. d) GDPR); 4) le conseguenze che l'ulteriore trattamento possa produrre (Considerando 50); 5) il contesto nel quale i dati sono stati raccolti (art. 6, par. 4, b) GDPR) [Casonato, Tomasi 2019]. Tale test non è di immediata eseguibilità, ma richiede un'attenta analisi.

La seconda possibile deroga riguarda il principio di limitazione della conservazione dei dati. L'art. 5, par. 1, lett. e) GDPR) così prescrive:

> 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»).

I dati trattati per le finalità di archiviazione e ricerca possono, così, essere conservati in una forma che consenta l'identificazione degli interessati anche oltre il periodo strettamente necessario per il conseguimento dello scopo per cui sono stati originariamente raccolti, previe misure tecniche e organizzative a loro protezione.

Sono previste, inoltre, possibili deroghe ai diritti degli interessati:

– «obblighi informativi»: nel caso in cui la comunicazione delle informazioni richieste prevista dall'art. 14, par. 1 e 2, risulti impossibile, o richieda uno sforzo sproporzionato, o rischi di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità di archiviazione, ricerca scientifica o statistica il titolare del trattamento può

1 Opzione auspicabile, tra l'altro, soprattutto nel caso in cui le informazioni vengano utilizzate a fini di ricerca medica.

essere sollevato dall'obbligo di fornire le informazioni (art. 14, par. 5, lett. b) GDPR). Occorre sottolineare che tale eccezione è stabilita esclusivamente per la lunga lista di informazioni dell'art. 14, e quindi soltanto quando i dati non sono raccolti direttamente dall'interessato (come disciplinato invece dall'art. 13). Se, in caso di dati raccolti presso l'interessato, il titolare scegliesse di non informare, o di farlo solo successivamente, perché una trasparenza sulle finalità del trattamento comprometterebbe il raggiungimento degli scopi che la ricerca si prefigge[2], si potrebbe rilevare che tale pratica risulterebbe controversa da un punto di vista etico e anche giuridico poiché l'interpretazione letterale dell'art. 13 parrebbe non lasciare spazio a possibili eccezioni, come invece già stabilisce l'art. 14;
– «diritto alla cancellazione dei dati»: tale diritto può venir limitato qualora il suo esercizio da parte dell'interessato rischi di rendere impossibile o di pregiudicare gli obiettivi del trattamento a fini di archiviazione, ricerca o statistica (art. 17, par. 3, lett. d), GDPR);
– «diritto di opposizione»: tale diritto può essere esercitato in generale dall'interessato contro il trattamento avente finalità di ricerca «per motivi connessi alla sua situazione particolare», tranne che nell'ipotesi in cui il trattamento sia necessario per l'esecuzione di un compito di interesse pubblico (art. 21, par. 6, GDPR). Di fronte all'interesse superiore di rilevanza collettiva, le ragioni del singolo vengono, pertanto, limitate e il trattamento può proseguire senza alcuna limitazione.

In aggiunta a questi diritti, uno Stato membro potrebbe prevedere regole per la limitazione del diritto di accesso (art. 15), diritto di rettifica (art. 16), diritto di limitazione del trattamento (art. 18) e diritto di opposizione (art. 21), come previsto dall'art. 89, par. 2 GDPR [Ducato 2020, 6 e Staunton et al. 2019].

Con riferimento alla base legittima per il trattamento di dati personali (non particolari), si possono presentare tre principali casistiche previste dall'art. 6 GDPR:

2 Un caso pratico, ad esempio, è quello di una ricerca di carattere psicologico o sociologico volta a determinare il perché del comportamento degli individui o dei gruppi in determinate circostanze. Se ci fosse l'informazione, la validità della ricerca potrebbe essere viziata.

– il consenso dell'interessato, che viene confermato quale strumento per autorizzare il titolare a trattare informazioni di carattere personale (art. 6, par. 1, lett. a), GDPR). Un comune fraintendimento è quello che opera a livello pratico tra il consenso al trattamento dei dati personali, oggetto della presente analisi, ed il consenso, invece, alla partecipazione al progetto che è di regola richiesto da principi di carattere etico. Sebbene da un punto di vista informativo alcuni elementi tendano a sovrapporsi, è opportuno ribadire che questi sono concettualmente, e giuridicamente, molto diversi [Quinn, Quinn 2018, Dove 2018 e EDPB, Linee guida 5/2020]. Il consenso privacy deve essere «inequivocabile» e «specifico» per l'operazione di trattamento che si intende porre in essere; ciò potrebbe perciò rappresentare una sfida per l'attività di un progetto di ricerca, in quanto spesso non è agevole individuare correttamente la finalità del trattamento dei dati personali a fini di ricerca scientifica al momento della raccolta dei dati. A questo proposito, qualora fosse necessario raccogliere il consenso per finalità di ricerca, ma il titolare non potesse individuare pienamente la finalità del trattamento al momento della raccolta dei dati, egli potrà richiedere agli interessati di prestare il consenso a taluni settori della ricerca scientifica, dovendo però rispettare le norme deontologiche in materia di ricerca scientifica (Considerando 33 GDPR). Sebbene ci possa essere una certa flessibilità e granularità in tale contesto, il consenso dell'interessato deve rimanere specifico: ciò significa che non si potrà comunque utilizzare una sorta di «broad consent» in quanto il GDPR non può essere interpretato in modo tale da permettere ad un titolare del trattamento di aggirare uno dei concetti chiave della disciplina relativo alla finalità specifica per la quale il consenso dell'interessato è richiesto (EDPB, Linee Guida 5/2020). Il consenso è sempre revocabile (art. 7 GDPR);
– la seconda casistica riguarda i progetti di ricerca che si possono fondare sulla necessaria esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento (art. 6, par. 1, lett. e) GDPR). Si pensi alle ricerche compiute dalle università (ricerca base o applicata) e dai centri di ricerca;
– altra possibile base giuridica, infine, è rappresentata dall'interesse legittimo del titolare del trattamento o di terzi, «a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'inte-

ressato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore» (art. 6, par. 1, lett. f) e Cons. 47 GDPR; WP29, Parere 6/2014). Questa possibilità è indirettamente prevista dal Considerando 47 e dal Considerando 113 che consente di tener conto delle «legittime aspettative della società nei confronti di un miglioramento delle conoscenze» in caso di finalità di ricerca scientifica o storica o a fini statistici. Dovrà, quindi, essere compiuto un test comparativo tra gli interessi del titolare, di terzi e degli interessati («three step test»). Le autorità pubbliche nell'esecuzione dei loro compiti non possono fondare un trattamento sull'interesse legittimo e pertanto esso sarà una base soltanto per enti privati (art. 6, par. 1, lett. f) GDPR).

Nel caso di trattamento di categorie particolari di dati, entra in gioco quanto previsto all'art. 9 GDPR. Anzitutto vige un divieto generale, che può essere superato solo nel caso in cui operi una specifica eccezione tra quelle elencate al secondo paragrafo. Anche in questo caso si prevede la possibilità di utilizzare il consenso come base legittima, il quale dovrà essere «esplicito» (art. 9, par. 2, lett. a) GDPR). L'art. 9, par. 2, lett. j) GDPR prevede, inoltre, che il trattamento sia legittimo qualora necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità all'articolo 89, par. 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.

Come dicevamo, in materia di ricerca scientifica il legislatore europeo ha lasciato ampio spazio agli Stati membri. Questi possono, infine, adottare particolari previsioni in materia di trattamenti per finalità di ricerca o archiviazione. Prendiamo qui, ad esempio, il contesto applicativo italiano. La disciplina è inserita al Titolo VII, artt. 97-110-*bis* del Codice Privacy, adeguato al GDPR dal d.lgs. 10 agosto 2018, n. 101. La normativa è in larga parte conforme a quella previgente, con l'eccezione di alcune modifiche riguardanti l'adozione di regole deontologiche. Il Garante può, infatti, adottare regole deontologiche per specifici trattamenti, inclusi quelli per scopi di ricerca (art. 2-*quater*).

In generale, l'art. 2-*quinquies*, co. 2, lett. cc) del Codice Privacy inserisce all'interno dei trattamenti di dati particolari per motivi di interesse

pubblico rilevante i trattamenti effettuati a fini di archiviazione o ricerca storica «concernenti la conservazione, l'ordinamento e la comunicazione dei documenti detenuti negli archivi di Stato, negli archivi storici di enti pubblici, o in archivi privati dichiarati di interesse storico particolarmente importante», e i trattamenti per fini di ricerca scientifica e a fini statistici da parte di soggetti del Sistan (Sistema statistico nazionale). L'art. 99 del Codice recepisce poi la possibilità di derogare al principio di limitazione della conservazione per scopi di archiviazione e ricerca e prevede che tali trattamenti possano essere effettuati oltre il periodo di tempo prefissato per conseguire quelle finalità.

Per quanto concerne la disciplina in tema di ricerca storica, è poi necessario richiamare anche il Capo II del Codice Privacy agli artt. 101-103, le Regole deontologiche per il trattamento a fini di archiviazione nel pubblico interesse o per scopi di ricerca storica pubblicate ai sensi dell'art. 20, comma 4, del d.lgs. 10 agosto 2018, n. 101 - 19 dicembre 2018 del Garante; e il d.lgs. 22 gennaio 2004, n. 42 «Codice dei beni culturali e del paesaggio», con particolare attenzione al Titolo II, Capo III «Consultabilità dei documenti degli archivi e tutela della riservatezza», artt. 122-127.

I trattamenti a fini statistici o di ricerca scientifica sono regolati dal Capo III, artt. 104-109 del Codice Privacy. Queste norme richiedono che i trattamenti con questi fini non utilizzino i dati per prendere decisioni o provvedimenti sugli interessati e che siano rese le necessarie informazioni come richiesto dagli artt. 13 e 14 GDPR (art. 105 Codice Privacy). L'informativa non è dovuta soltanto quando richiederebbe uno sforzo sproporzionato rispetto al diritto dell'interessato ad essere informato e vengano poste in essere forme di pubblicità idonee, come previsto dal Garante nelle «Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica» (Regole deontologiche ricerca scientifica) e nelle «Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica effettuati nell'ambito del Sistema statistico nazionale», entrambe pubblicate ai sensi dell'art. 20, comma 4, del d.lgs. 10 agosto 2018, n. 101 - 19 dicembre 2018. Le prime Regole si applicano ai trattamenti effettuati da università enti o istituti di ricerca, società scientifiche e loro ricercatori per scopi statistici e scientifici, con l'esclusione di quelli connessi all'attività di tutela della salute svolte da esercenti delle professioni sanitarie o organismi sanitari e di quei trattamenti che hanno comparabile ricaduta personalizzata sugli interessati (art. 1). Le seconde Regole deontologi-

che, invece, riguardano a) «enti ed uffici di statistica che fanno parte o partecipano al Sistema statistico nazionale»; b) strutture diverse da questi uffici, ma «appartenenti alla medesima amministrazione o ente, qualora i relativi trattamenti siano previsti dal programma statistico nazionale e gli uffici di statistica attestino le metodologie adottate», osservando le disposizioni contenute nel d.lgs 6 settembre 1989, n. 322, nel GDPR, nel Codice Privacy nelle stesse regole deontologiche (art. 1). In entrambi i casi il trattamento dei dati deve essere descritto nei progetti di ricerca.

Con specifico riferimento alla ricerca in ambito medico, biomedico ed epidemiologico rileva l'art. 110 del Codice Privacy. Oltre a tale previsione rimangono applicabili alcune autorizzazioni generali al trattamento pubblicate dal Garante prima del GDPR nel 2016 (Provv. 1/2016, 3/2016, 6/2016, 8/2016 e 9/2016). In particolare l'Allegato 1, punto 5 del Provvedimento del 13 dicembre 2018 contiene le «Prescrizioni relative al trattamento dei dati personali effettuato per scopi di ricerca scientifica (aut. gen. n. 9/2016)» (Prescrizioni ricerca scientifica), le quali riguardano il trattamento effettuato da: a) università, altri enti o istituti di ricerca e società scientifiche, nonché ricercatori che operano nell'ambito di dette università, enti, istituti di ricerca e ai soci di dette società scientifiche; b) esercenti le professioni sanitarie e gli organismi sanitari; c) persone fisiche o giuridiche, enti, associazioni e organismi privati, nonché soggetti specificatamente preposti al trattamento quali designati o responsabili del trattamento (ricercatori, monitor, commissioni di esperti, organizzazioni di ricerca a contratto, laboratori di analisi, ecc.) (artt. 2-*quaterdecies* Codice Privacy e 28 GDPR) (punto 5.1). Tali prescrizioni concernono il trattamento di dati personali per finalità di ricerca medica, biomedica ed epidemiologica effettuati quando: il trattamento è necessario per la conduzione di studi condotti con dati raccolti in precedenza a fini di cura della salute o per l'esecuzione di precedenti progetti di ricerca, ovvero ricavati da campioni biologici prelevati in precedenza per finalità di tutela della salute o per l'esecuzione di precedenti progetti di ricerca; oppure quando il trattamento è necessario per la conduzione di studi effettuati con dati riferiti a persone che, in ragione della gravità del loro stato clinico, non sono in grado di comprendere le indicazioni rese nell'informativa e di prestare validamente il consenso (5.2). Il punto 4 dell'Allegato 1 del suddetto Provvedimento prevede, invece, le «Prescrizioni relative al trattamento dei dati genetici (aut. gen. n. 8/2016)».

Nelle Prescrizioni ricerca scientifica si prevede che la ricerca medica, biomedica ed epidemiologica deve essere svolta (art. 8)

> nel rispetto degli orientamenti e delle disposizioni internazionali e comunitarie in materia, quali la Convenzione sui diritti dell'uomo e sulla biomedicina del 4 aprile 1997, ratificata con legge 28 marzo 2001, n. 145, la Raccomandazione del Consiglio d'Europa R(97)5 adottata il 13 febbraio 1997 relativa alla protezione dei dati sanitari e la dichiarazione di Helsinki dell'Associazione medica mondiale sui princìpi per la ricerca che coinvolge soggetti umani.

Con riferimento ai requisiti di legittimità del trattamento, sia le Prescrizioni ricerca scientifica che le Regole deontologiche ricerca scientifica richiamano il consenso degli interessati come base giuridica del trattamento. L'art. 110 del Codice Privacy, quindi, sul presupposto che tale consenso sia richiesto per condurre una ricerca scientifica in campo medico, biomedico ed epidemiologico, disciplina al primo comma i casi in cui questo non risulta, invece, necessario. Il primo tra questi riguarda la fattispecie relativa al trattamento effettuato in base a disposizioni di legge o di regolamento o al diritto dell'Unione europea. La previsione normativa richiama come base legittima direttamente l'art. 9, par. 2, lett. j) GDPR e menziona espressamente, come esempio paradigmatico, la ricerca rientrante in un programma previsto ai sensi dell'art. 12-*bis* d.lgs. 502/1992 («Riordino della disciplina in materia sanitaria, a norma dell'articolo 1 della legge 23 ottobre 1992, n. 421»). Una ricerca rientrante in questo ambito potrà essere condotta senza il consenso degli interessati, a condizione che sia posta in essere e resa pubblica una DPIA. Il secondo caso di esenzione del consenso è previsto dalla seconda parte del primo comma dell'art. 110 e ricorre qualora «a causa di particolari ragioni, informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca». In queste ipotesi, il punto 5.3 delle Prescrizioni ricerca scientifica stabilisce il titolare del trattamento deve documentare nel progetto di ricerca la sussistenza delle ragioni, considerate del tutto particolari o eccezionali, per le quali informare gli interessati risulta impossibile o implichi uno sforzo sproporzionato, oppure rischi di rendere impossibile o di pregiudicare

gravemente il conseguimento delle finalità della ricerca. Queste ragioni rimandano principalmente a tre tipologie:

– motivi di carattere etico, riconducibili alla circostanza che l'interessato ignori la propria condizione (si pensi, ad esempio, agli studi epidemiologici sulla distribuzione di un fattore che predica o possa predire lo sviluppo di uno stato morboso per il quale non esista un trattamento curativo);
– motivi di impossibilità organizzativa, riconducibili alla circostanza che la mancata considerazione dei dati riferiti agli interessati che non è possibile contattare, rispetto al numero complessivo dei soggetti che si intende coinvolgere nella ricerca, produrrebbe conseguenze significative per lo studio in termini di alterazione dei relativi risultati;
– motivi di salute, riconducibili alla gravità dello stato clinico in cui versa l'interessato a causa del quale questi è impossibilitato a comprendere le indicazioni rese nell'informativa e a prestare validamente il consenso.

Nelle ipotesi di cui alla seconda parte del primo comma dell'art. 110 Codice Privacy il titolare del trattamento è obbligato ad adottare le misure appropriate per tutelare i diritti, le libertà ed i legittimi interessi dell'interessato, dovrà redigere un programma di ricerca oggetto di motivato parere favorevole da parte del competente comitato etico a livello territoriale e dovrà compiere una DPIA, la quale dovrà essere, infine, necessariamente sottoposta in consultazione preventiva al Garante ai sensi dell'art. 36 GDPR.

Il secondo comma dell'art. 110 stabilisce che nel caso in cui l'interessato al trattamento intenda esercitare i diritti di cui all'art. 16 GDPR, l'aggiornamento, la rettificazione e l'integrazione dei dati avvenga senza la modifica dei dati stessi ma con una semplice annotazione, sempre che il risultato di tali operazioni non produca effetti significativi sul risultato della ricerca. Le Regole deontologiche ricerca riprendono questa previsione consentendo, qualora siano necessarie modifiche ai dati che riguardano l'interessato in caso di esercizio dei diritti dell'interessato cui agli art. 15 e ss. del GDPR, al titolare del trattamento di annotare, in appositi spazi o registri, le modifiche richieste dall'interessato, senza variare i dati originariamente immessi nell'archivio (art. 12).

A chiusura del Titolo VII del Codice Privacy è stato inserito un articolo dedicato al trattamento ulteriore (secondario) di dati personali da parte di terzi per finalità di ricerca scientifica o a fini statistici, che si inserisce nella previsione dell'art. 89 GDPR. Questa tipologia di trattamento può essere direttamente autorizzata dal Garante, anche in caso di utilizzo di dati particolari, per soggetti terzi che svolgono «principalmente» tali attività di ricerca[3] quando, a causa di particolari ragioni, informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità, a condizione che siano adottate misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, in conformità all'articolo 89 GDPR, incluse forme preventive di minimizzazione e di anonimizzazione dei dati (art. 110-*bis*, co. 1, Codice Privacy). Questa autorizzazione può essere rilasciata su richiesta entro quarantacinque giorni, decorsi i quali la mancata pronuncia del Garante equivale ad un rigetto; con tale autorizzazione o anche successivamente, se compiute ulteriori verifiche, l'autorità stabilirà le condizioni e le misure, anche di sicurezza, che sono necessarie ad assicurare adeguate garanzie (co. 2). Il Garante, peraltro, può autorizzare queste tipologie di trattamenti anche mediante provvedimenti generali adottati d'ufficio e pubblicati in Gazzetta Ufficiale. Tali autorizzazioni generali potranno riferirsi a determinate categorie di titolari e di trattamenti, stabilire le condizioni del trattamento secondario e prescrivere le misure necessarie per assicurare adeguate garanzie a tutela degli interessati (co. 3). Dalla previsione dell'art. 110-*bis* devono ritenersi esclusi i trattamenti per l'attività clinica a fini di ricerca, effettuati da istituti di ricovero e cura a carattere scientifico, pubblici e privati, dal momento che la loro attività è strumentale all'assistenza sanitaria (co. 4). Qualunque progetto di riutilizzo dei dati per finalità di ricerca per essere sottoposto al vaglio del Garante dovrà perciò dimostrare preventivamente di aver predisposto tutte le misure adeguate a protezione dei dati. L'adozione di questi idonei accorgimenti dovrà, inoltre, essere comprovata e documentata. Tutto ciò in

3 Una lettura sistematica delle norme consiglierebbe di individuare i destinatari dell'articolo tra quelli indicati nell'Allegato 5 al Codice privacy Regole deontologiche ricerca.

piena conformità al principio della responsabilizzazione, come sancito dagli articoli 5, par. 2, e 24, par. 1, GDPR.

Si ricorda che durante l'elaborazione e l'esecuzione di un progetto di ricerca ogni attività dovrà essere considerata distintamente per la definizione delle misure di accountability (art. 24 GDPR), di data protection by design e by default (art. 25 GDPR) [vedi → Capitolo 4], per la predisposizione del registro delle attività di trattamento (art. 30 GDPR), per l'implementazione delle misure di sicurezza del trattamento (art. 32 GDPR), per la redazione, infine, della valutazione di impatto sulla protezione di dati (art. 35 GDPR).

16.2 Ricerca scientifica e privacy negli Stati Uniti d'America

La disciplina in tema di protezione dei dati personali nell'ordinamento statunitense si presenta frammentata e appare come un'intricata combinazione di varie forme di protezione di rango costituzionale, leggi federali e statali, *tort* [Solove, Hartzog 2014 e Pagallo 2008]. Coloro i quali trattano i dati fanno spesso affidamento su autoregolamentazioni che riguardano contesti specifici [Klitou 2104, 42]. Non esiste, quindi, nulla di paragonabile al GDPR ed al suo approccio uniforme e onnicomprensivo. Il legislatore statunitense interviene solo in modo circoscritto e mirato e quando la regolazione legislativa appare strettamente necessaria [vedi → Capitolo 1].

Lo stesso concetto, poi, di «Personally Identifiable Information» (PII) non è definito in modo uniforme in questo sistema giuridico [Burdon 2020, 155-170]. È stato sottolineato come le PII siano in gran parte circoscritte alle sole informazioni relative ad un soggetto direttamente identificabile, con un approccio quindi molto più limitato di quello previsto dal GDPR [Solove, Schwartz 2021, 820-832].

Occorre, quindi, individuare e delimitare il contesto applicativo per cercare di offrire la descrizione del quadro regolativo e per proporre uno spaccato che possa essere funzionale ed utile ad una comparazione con il modello europeo. Prendiamo a riferimento il tema dell'accesso ai dati sanitari per finalità di ricerca [Hintze 2019].

Molte leggi federali e statali riguardano la privacy medica. Nessuna di queste, tuttavia, fornisce ai pazienti una protezione completa e, nel complesso, sono presenti numerose lacune.

La prima disciplina che viene ad evidenza è l'«Health Insurance Portability and Accountability Act» del 1996 (HIPAA)[4]. La privacy medica è garantita per tipologia di dato e di «custode». Le Privacy Rules proteggono le c.d. «Protected Health Information» (PHI), indipendentemente dal formato in cui esse sono state memorizzate; mentre le Security Rules si applicano alle sole PHI trattate in formato elettronico (e-PHI). Le informazioni sanitarie vengono eventualmente anonimizzate secondo gli standard indicati dall'HIPAA stesso. Questa disposizione normativa si applica solo alle c.d. «covered entity», ossia ai fornitori di servizi sanitari, agli enti che coprono i costi dei servizi sanitari stessi, centri di compensazione sanitari o da chiunque utilizzi o divulghi PHI per svolgere o fornire servizi per una «covered entity». Tale approccio con riferimento all'ambito di applicazione è stato oggetto di critiche in quanto questa sarebbe troppo ristretta e molti soggetti che elaborano informazioni sanitarie operano al di fuori delle condizioni HIPAA, creando così una ampia lacuna normativa [Solove, Schwtarz 2021, 531-564].

Le HIPAA Privacy Rules stabiliscono le condizioni in base alle quali le PHI possono essere utilizzate o divulgate dalle entità coperte a fini di ricerca. Si prevede che le informazioni sanitarie possano essere utilizzate a fini di ricerca senza l'autorizzazione dell'interessato solo nel caso in cui sia stato ottenuto un «waiver» documentato ed approvato da un «Institutional Review Board» (IRB) o dal «Privacy Board» dell'entità coperta che pone in essere l'attività di divulgazione (Section 164.512(i)(1) HIPAA).

4 Per più di 25 anni, l'HIPAA ha stabilito lo standard per governare lo scambio elettronico, la privacy e la sicurezza delle informazioni sanitarie. Sebbene pionieristico ai suoi tempi, l'HIPAA non è più in grado di gestire gli attuali scenari tecnologici. Nel febbraio 2022 è stata proposta l'adozione di una nuova disposizione normativa chiamata «Health Data Use and Privacy Commission Act», a firma congiunta dei senatori Tammy Baldwin e Bill Cassidy, al fine di avviare una modernizzazione della disciplina in materia. Si prevede, tra le altre cose, la creazione di una Commissione per la salute e la privacy che condurrà ricerche e formulerà raccomandazioni su come modernizzare le attuali leggi sulla privacy dei dati sanitari. L'obiettivo dichiarato dovrebbe essere quello di stabilire nuovi standard per la protezione della privacy dei pazienti, consentendo al contempo agli operatori sanitari di accedere alle tecnologie e agli strumenti di comunicazione di cui hanno bisogno per fornire il miglior standard di cura.

Affinché un IRB o un comitato per la privacy approvi una deroga all'autorizzazione devono essere soddisfatti tre criteri:

1. l'utilizzo o la divulgazione di PHI comporta solo un rischio minimo per la privacy delle persone, basato sulla presenza degli elementi indicati alla Section 164.512(i)(1)(ii)[5];
2. la ricerca non potrebbe essere condotta senza il «waiver»;
3. la ricerca non potrebbe essere condotta senza l'accesso alle informazioni sanitarie protette ed il loro utilizzo.

In assenza di questi criteri, il trattamento dei dati per finalità di ricerca dovrà, quindi, necessariamente essere basato sull'autorizzazione scritta degli interessati (Section 164.508-510 HIPAA). In questo caso l'HIPAA incoraggia l'adozione di «data use agreement» in merito al trattamento delle informazioni sanitarie che, sebbene non completamente de-identificate, siano state comunque oggetto della rimozione di alcuni identificatori diretti (Section 164.514(e) HIPAA).

Una covered entity può, invece, sempre utilizzare o divulgare a fini di ricerca informazioni sanitarie che siano state de-identificate (in conformità con quanto stabilito alle Section 164.502 (d) e 164.514 (a) - (c) HIPAA Privacy Rules).

Il concetto di «de-identificazione» diviene, pertanto, cruciale. Le Privacy Rules stabiliscono che le informazioni sanitarie sono da considerarsi anonimizzate: 1) se un esperto qualificato determina che esiste solo un rischio «molto basso» che i dati possano essere nuovamente identificati; 2) se l'esperto documenta la propria analisi (Section 164.514(b)(1) HIPAA). Questo criterio è noto come HIPAA «standard statistico». In alternativa, le informazioni sono considerate de-identificate qualora vengano rimossi i seguenti diciotto identificatori (Section 164.514(b)(2) HIPAA):

5 L'esistenza di: un piano adeguato per proteggere gli identificatori da usi e divulgazioni impropri; un piano adeguato per distruggere gli identificatori alla prima occasione coerente con lo svolgimento della ricerca, a meno che non vi sia una giustificazione sanitaria o di ricerca per conservare gli identificatori o tale conservazione sia altrimenti richiesta dalla legge; adeguate garanzie scritte che le informazioni sanitarie protette non saranno riutilizzate o divulgate a nessun'altra persona o entità, ad eccezione di quanto richiesto dalla legge, per la supervisione autorizzata del progetto di ricerca, o per altre ricerche per le quali l'uso o la divulgazione di informazioni sanitarie protette sarebbe comunque consentito.

(A) Names;
(B) All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the cur-rent publicly available data from the Bureau of the Census: (1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000;
(C) All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
(D) Telephone numbers;
(E) Fax numbers;
(F) Electronic mail addresses;
(G) Social security numbers;
(H) Medical record numbers;
(I) Health plan beneficiary numbers;
(J) Account numbers;
(K) Certificate/license numbers;
(L) Vehicle identifiers and serial numbers, including license plate numbers;
(M) Device identifiers and serial numbers;
(N) Web Universal Resource Locators (URLs);
(O) Internet Protocol (IP) address numbers;
(P) Biometric identifiers, including finger and voice prints;
(Q) Full face photographic images and any comparable images; and
(R) Any other unique identifying number, characteristic, or code.

Infine, vengono anche definite le modalità attraverso le quali i soggetti saranno informati degli usi e della divulgazione delle loro informazioni mediche a fini di ricerca e dei loro diritti di accesso.

Il Privacy Act è, invece, una legge federale che regola la raccolta, l'archiviazione, l'uso e la divulgazione di informazioni da parte del governo federale [Solove, Schwartz 2021, 685-688; vedi → Capitolo 1]. Si prevede che il governo non possa divulgare i dati senza l'autorizzazione dell'interessato, a meno che non si applichino specifiche eccezioni. Di conse-

guenza, tale disposizione normativa permette la diffusione da parte del governo di informazioni anonime tramite il portale «HealthData.gov» o altri siti Web.

Infine, a livello statale, il diritto alla privacy è generalmente riconosciuto e disciplinato dalla common law o tramite un apposito *statute* che regola la materia. Tra tutti ricordiamo il «California Consumer Privacy Act» (CCPA) [Solove, Schwartz 2021, 970-973 e Determann 2018; vedi → Capitolo 1] il quale definisce e circoscrive la nozione di ricerca alle sole attività orientate all'interesse pubblico (Section 1798.140(s) CCPA):

> scientific, systematic study and observation, including basic research or applied research that is in the public interest and that adheres to all other applicable ethics and privacy laws or studies conducted in the public interest in the area of public health.

Lo *statute* afferma, inoltre, che possono essere trattate a fini di ricerca, a condizione che siano soddisfatte determinate condizioni:

> personal information that may have been collected from a consumer in the course of a consumer's interaction with a business's service or device for other purposes.

Tra queste condizioni si ricordano: la compatibilità degli scopi di ricerca con quelli aziendali per i quali le informazioni sono state raccolte; l'adozione di misure di sicurezza che impediscano la reidentificazione dei consumatori o garantiscano quantomeno la pseudonimizzazione delle stesse. Si vieta, infine, espressamente l'uso di dette informazioni a fini commerciali.

16.3 Casi 16-1, 16-2, 16-3

Caso 16-1

Il Dr. Carter medico cardiologo lavora presso l'azienda sanitaria Alfa e intende effettuare una ricerca sui dati raccolti tramite i pace-maker «impiantati» sui suoi pazienti cronici per valutare la precisione ed efficacia

degli strumenti scelti e per supportare l'azienda nella gestione dei futuri trend sui ricoveri ospedalieri. Per fare ciò si propone di combinare i dati ricavati da tali strumenti con gli altri dati presenti nei fascicoli sanitari elettronici dei pazienti. In particolare, i sistemi di pace-maker raccolgono automaticamente i dati che vengono, poi, salvati in cloud.
Chi è il titolare del trattamento? Chi è l'eventuale responsabile?
Quali dati sono oggetto di trattamento?
Qual è la base giuridica del trattamento?

Caso 16-2

Il dottor Casa che lavora presso l'Azienda sanitaria Asclepio contatta il centro di ricerca Futuristic per porre essere un'attività di ricerca volta allo sviluppo di un'applicazione che, tramite algoritmi di machine learning, possa interpretare immagini radiologiche di pazienti e individuare più rapidamente ed efficacemente l'eventuale presenza di rischi tumorali. Al caricamento di un'immagine nel sistema, l'applicazione dovrebbe essere in grado di rispondere con un esito positivo o negativo della possibile presenza di un tumore. Al fine di poter sviluppare un'applicazione realmente affidante, il centro di ricerca Futuristic dovrebbe poter addestrare il suo algoritmo con dataset di immagini radiologiche provenienti da reali pazienti del dottor Casa (precedentemente refertate con esito positivo o negativo circa la presenza di un tumore).
Chi è il titolare del trattamento? Chi è l'eventuale responsabile?
Quali dati sono oggetto di trattamento?
Qual è la base giuridica del trattamento?
Quali le peculiari regole giuridiche applicabili a questo scenario?

Caso 16-3

Un Consorzio di imprese e istituti di ricerca sta portando avanti un progetto nell'ambito delle «città intelligenti». L'Università Alfa è il coordinatore dell'attività del Progetto che si propone di studiare la mobilità dei cittadini. Per raggiungere questo obiettivo, i ricercatori raccoglieranno informazioni sulle loro preferenze rispetto ai servizi offerti dal Comune Beta e sui loro dati di geolocalizzazione (attraverso questionari e dati «sensoriali» derivanti da un'app installata sui cellulari dei partecipanti). Questi dati verranno analizzati insieme alle condizioni meteorologiche, agli eventi sul territorio e alle segnalazioni dei cittadini, correlandoli per ottenere informazioni a valore aggiunto. I dati sono archiviati in un cloud storage fornito da una società privata. Il Consorzio vuole sviluppare un sistema capace di: da un lato, prevedere il traffico e anticipare

in che modo questo possa essere influenzato da eventi come i cantieri stradali; dall'altro, progettare servizi di mobilità in grado di sfruttare al meglio tutte queste informazioni.
Quale è la finalità del trattamento?
Quali dati sono oggetto di trattamento?
Come gestire l'allocazione dei ruoli privacy?

CAPITOLO 17.
Privacy e Blockchain[1]

Paolo Guarda

17.1 Premesse

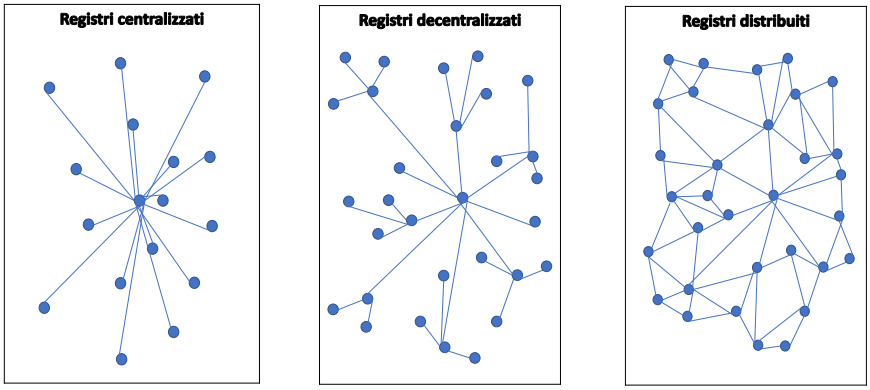
Il mondo del diritto è intrinsecamente legato a quello delle innovazioni tecnologiche. Ogni qual volta una nuova tecnologia si afferma (o meglio diventa di uso diffuso) e si pensa di adottarla nei vari scenari applicativi, la prima domanda che sorge spontanea è se essa sia ancora conforme alle norme di legge previste o se rappresenti una rottura rispetto al quadro stabilito [Pascuzzi 2020, 17-30 e 249-250].

Nel contesto digitale, il dato normativo è spesso vittima della sua precoce obsolescenza. I giuristi devono, allora, cimentarsi nel difficile compito di trovare una soluzione che si inserisca in una tradizione giuridica caratterizzata da principi fondamentali e regole di dettaglio. Sono chiamati a mettere in mostra la loro «creatività», pur restando nell'ambito di un sistema rigorosamente codificato e tipizzato [Pascuzzi 2013].

L'avvento della c.d. blockchain conferma quanto appena sostenuto [Finck 2019, Pascuzzi 2020, 279-288 e Arisi, Guarda 2020]. Si tratta, infatti, di una soluzione tecnologica, a dire il vero già nota da anni ad una ristretta cerchia di «esperti», che promette di superare alcuni dei problemi tipici delle applicazioni digitali centralizzate. Da sistemi di archiviazione centralizzati si è quindi passati a modelli decentralizzati, fino a giungere a soluzioni totalmente distribuite, dove non vi è più un centro organizzativo ma va considerato il ruolo di tutti i soggetti coinvolti. In-

1 Il presente capitolo è stato scritto grazie alla collaborazione e confronto con Marta Arisi.

dividuiamo questo approdo tecnologico con l'espressione «distributed ledger». Architetture di questo tipo prevedono che la banca dati non si trovi più fisicamente su un unico server, ma risieda effettivamente su più computer contemporaneamente, tutti perfettamente sincronizzati[2].



L'ecosistema blockchain [Arisi, Guarda 2020, 479-480 e nt. 11] promette alcuni affascinanti vantaggi: l'immutabilità del registro (o almeno la tendenziale immutabilità dello stesso per i motivi che verranno discussi in seguito); la totale tracciabilità delle transazioni, con evidenti benefici in termini di trasparenza dei processi; la sicurezza, basata anzitutto su tecnologie crittografiche; il decentramento, tipico di un sistema distribuito, che riduce il rischio di perdita o alterazione di dati; la regola del «consenso», un nuovo concetto di «fiducia» ma forse anche una nuova forma di «democrazia».

La possibile adozione di sistemi basati sulla blockchain solleva numerose criticità nell'incontro con la disciplina in materia di protezione dei dati personali. Le problematiche non sono di poco momento. In questo Capitolo si cercherà di evidenziare i nodi più rilevanti e di sciogliere le questioni più spinose.

2 L'elaborazione originale di questa schematizzazione si deve a Baran 1964, 2.

17.2 Blockchain in pillole

La blockchain va inserita all'interno del movimento c.d. *Cypherpunk*: alla fine degli anni Ottanta i *crypto rebel* si battevano per l'uguaglianza sociale e il diritto alla privacy nell'era elettronica. Le loro «armi» erano la crittografia ed il codice [Arisi, Guarda 2020, 479 e Levy 1993]. Satoshi Nakamoto, l'anonimo e mitico inventore di Bitcoin[3], può essere considerato il genio del *cypherpunk* [Nakamoto 2009]. Questo non solo per il grande successo della criptovaluta, forse tutt'ora la più popolare al mondo, ma soprattutto perché Bitcoin ha rappresentato una sorta di rivoluzione per l'affermarsi, soprattutto nel periodo più recente, di nuove architetture digitali caratterizzate da decentramento, trasparenza e resistenza alle manomissioni [Tapscott, Tapscott 2016].

La blockchain è una implementazione di tecnologie basate su registri distribuiti e strutturati come una catena di blocchi contenenti le transazioni e la cui validazione è affidata a un meccanismo di consenso, distribuito su tutti i nodi della rete, ossia su tutti i «soggetti» che sono autorizzati a partecipare al processo di validazione delle transazioni da includere nel registro. Le principali caratteristiche delle tecnologie blockchain, come dicevamo, sono l'immutabilità del registro, la tracciabilità delle transazioni e la sicurezza basata su tecniche crittografiche.

Una possibile definizione di riferimento è rinvenibile negli standard ISO[4]:

> distributed ledger with confirmed blocks organized in an append-only, sequential chain using cryptographic links.

Una definizione giuridica è, invece, rinvenibile nell'art. 8-ter del d.l. 14 dicembre 2018, n. 135 «Disposizioni urgenti in materia di sostegno e semplificazione per le imprese e per la pubblica amministrazione», come convertito dalla legge 11 febbraio 2019, n. 12:

---

3 https://bitcoin.org/it/.

4 ISO/TR 23455:2019 *Blockchain and distributed ledger technologies. Overview of and interactions between smart contracts in blockchain and distributed ledger technology systems*. Definizioni rinvenibili su https://www.iso.org/obp/ui#iso:std:iso:22739:dis:ed-1:v1:en.

> Si definiscono «tecnologie basate su registri distribuiti» le tecnologie e i protocolli informatici che usano un registro condiviso, distribuito, replicabile, accessibile simultaneamente, architetturalmente decentralizzato su basi crittografiche, tali da consentire la registrazione, la convalida, l'aggiornamento e l'archiviazione di dati sia in chiaro che ulteriormente protetti da crittografia verificabili da ciascun partecipante, non alterabili e non modificabili.

Il decentramento, o distribuzione, ha un ruolo fondamentale: mentre a un livello più ampio si può affermare che nei database centralizzati, anch'essi tipicamente proprietari, un'autorità centrale convalida tutte le informazioni, le blockchain possono definirsi «distribuite» perché è «la catena di blocchi» che identifica la soluzione di archiviazione dei dati e certifica le transazioni. Il meccanismo del «consenso» diviene, pertanto, la nozione centrale per comprendere questa «architettura», in quanto permette ai nodi di «andare d'accordo»:

> agreement among DLT nodes that 1) a transaction is validated and 2) that the distributed ledger contains a consistent set and ordering of validated transactions (ISO/TR 23455:2019).

Il consenso serve, pertanto, a validare una transazione affinché possa essere aggiunta alla «catena»; raggiungendo il consenso, i nodi si impegnano nella convalida dei dati indipendentemente da un comando centrale all'interno della rete. Esistono diversi tipi di consenso: *Proof-of-Work* (PoW), *Proof-of-Stake* (PoS), *Proof-of-Identity* (PoI), *Delegated Proof-of-Stake* (DPoS) [Aggarwal et al. 2019, 17]. Poiché tali meccanismi presentano delle differenze, anche in termini di per così dire «costi» – soprattutto, in termini di calcolo computazionale – essi influenzano anche la cd. scalabilità delle blockchain, cioè la capacità di cambiarne le dimensioni. La scalabilità è una proprietà considerata vitale per gli sviluppi futuri delle diverse blockchain esistenti, date le diverse soluzioni adottate, e il loro successo.

Concretamente, la blockchain può essere rappresentata come una serie di blocchi che archiviano un insieme di transazioni validate e correlate da un marcatore temporale (*timestamp*). Ogni blocco include l'*hash* (una funzione algoritmica informatica non invertibile che mappa una stringa di lunghezza arbitraria in una stringa di lunghezza predefinita) che

identifica il blocco in modo univoco. L'inclusione, in ogni nuovo blocco, dell'hash del blocco precedente permette il dispiegarsi della «catena». Componenti basilari sono:

– *nodo*: sono i partecipanti alla blockchain e sono costituiti fisicamente dai server di ciascun partecipante. Si parla di *miner* quando l'utente contribuisce attivamente alla validazione delle informazioni e dei blocchi;
– *transazione*: è costituita dai dati che rappresentano i valori oggetto di «scambio» e che necessitano di essere verificati, approvati e poi archiviati;
– *blocco*: è rappresentato dal raggruppamento di un insieme di transazioni che sono unite per essere verificate, approvate e poi archiviate dai partecipanti alla blockchain;
– *ledger*: è il registro pubblico nel quale vengono «annotate» con la massima trasparenza e in modo immutabile tutte le transazioni effettuate in modo ordinato e sequenziale. Il ledger è costituito dall'insieme dei blocchi che sono tra loro incatenati tramite una funzione di crittografia e grazie all'uso di hash;
– *hash*: è una operazione (non reversibile) che permette di mappare una stringa di testo e/o numerica di lunghezza variabile in una stringa unica ed univoca di lunghezza determinata. L'*hash* identifica in modo univoco e sicuro ciascun blocco.

Altra distinzione fondamentale per capire le diversità dell'ecosistema è quella tra blockchain privata e pubblica [Buterin 2015 e Arisi, Guarda 2020, 480-481].

Le blockchain *permissionless* o pubbliche non richiedono alcuna autorizzazione per poter accedere alla rete, eseguire delle transazioni o partecipare alla verifica e creazione di un nuovo blocco. Chiunque può divenire un nodo. Gli esempi più famosi sono sicuramente Bitcoin ed Ethereum[5]. Si tratta di una struttura completamente decentralizzata, in quanto non esiste un ente primario che gestisce le autorizzazioni di accesso, le quali sono condivise tra tutti i nodi allo stesso modo. Nessun utente ha privilegi sugli altri, nessuno può esercitare il controllo sulle informazioni che vengono memorizzate su di essa, modificarle o eliminar-

5 https://ethereum.org/it/.

le, o può alterare il protocollo che determina il funzionamento di questa tecnologia.

Dall'altro lato troviamo sempre più esempi di c.d. blockchain private, dove le autorizzazioni di scrittura e modifica dei blocchi sono centralizzate, mentre quelle di lettura sono pubbliche o limitate ad un gruppo specifico di utenti. Esse sono di regola *permissioned*, cioè soggette ad un'autorità centrale che determina chi possa accedervi. Oltre a definire chi è legittimato a far parte della rete, tale autorità definisce quali sono i ruoli che un utente può ricoprire all'interno della stessa, definendo anche regole sulla visibilità dei dati registrati. Le blockchain *permissioned* introducono il concetto di centralizzazione in una rete che nasce come sostanzialmente decentralizzata e distribuita. Di regola al vertice di tali sistemi si trovano istituti finanziari o agenzie governative che definiscono chi possa accedere o meno alla rete (si veda, ad esempio, «Chain»[6]).

Possiamo, infine, avere casi «ibridi» quali le Blockchain pubbliche permissioned (come ad esempio Ripple e Hyperledger Fabri): una rete che opera per conto di una comunità che condivide un interesse comune e dove l'accesso al ruolo di miner è limitato ad un numero esiguo di individui ritenuti fidati. Il livello di lettura del registro e partecipazione nella generazione di nuove transa-zioni può essere soggetto a limitazioni a seconda dell'organizzazione che controlla la Blockchain.

I libri mastri sono sin dai tempi antichi utilizzati per rappresentare dati e raggiungere un accordo sulla validità delle informazioni in essi contenuti. La blockchain rappresenta un nuovo approccio alla costituzione e gestione di un registro [Davidson, Filippi, Potts 2018, 642-643 e Werbach 2018, 33]. La vera caratteristica innovativa risiede nel fatto che qui ci si basa su di un registro globale condiviso e affidante anche in assenza di un'autorità centrale che lo valida e lo garantisce, attraverso il meccanismo del consenso. Si tratta di un nuovo concetto di fiducia o addirittura di un sistema senza fiducia [Arisi, Guarda 2020, 482].

Un'ultima definizione utile per circoscrivere il contesto è quella di «smart contract» [Bompezzi 2021 e Pardolesi, Davola 2019]. Per semplicità e chiarezza possiamo allora richiamare quella proposta dal legislatore italiano all'art. 8-ter, co. 2, D.L. 135/2018:

6 https://chain.com/.

> Si definisce «smart contract» un programma per elaboratore che opera su tecnologie basate su registri distribuiti e la cui esecuzione vincola automaticamente due o più parti sulla base di effetti predefiniti dalle stesse (…).

17.3 Blockchain e disciplina in materia di protezione dei dati personali

Nella loro applicazione pratica le blockchain possono essere potenzialmente oggetto di diverse regole giuridiche. L'Unione europea ha cercato di accogliere i progressi tecnologici nel mercato unico digitale, considerando la blockchain una parte integrante di questa sfida[7]. È di tutta evidenza come la disciplina in materia di protezione dei dati personali, per caratteristiche intrinseche a queste nuove tecnologie, possa rappresentare uno dei contesti più problematici [Bompezzi, Gambino 2019 e Moerel 2018].

Di seguito si evidenzieranno le maggiori criticità che l'applicazione del GDPR comporta con riferimento all'adozione di una blockchain.

17.3.1 Ambito materiale, definizione di dato personale e ambito territoriale

La prima questione da affrontare è quella relativa all'ambito di applicazione materiale (art. 2 GDPR) e, di conseguenza, alla definizione di dato personale.

Affinché il GDPR si applichi, l'ambito materiale richiede che vengano trattati dati personali. Nel Capitolo 4 abbiamo avuto modo di proporre le definizioni di dato personale (art. 4, pt. 1) e nel Capitolo 12 diffusamente trattato la questione relativa ai concetti di anonimizzazione e pseudonimizzazione. Per applicare queste regole occorre analizzare lo scenario che caratterizza l'utilizzo di una blockchain.

Nell'ambito di una blockchain il trattamento di dati personali può interessare due specifici momenti. Anzitutto quello relativo all'esecu-

7 Si veda, ad esempio, la Risoluzione del Parlamento europeo del 3 ottobre 2018 sulle tecnologie di registro distribuito e blockchain: creare fiducia attraverso la disintermediazione (2017/2772(RSP)).

zione del protocollo, a cui sono indispensabili firme e chiavi pubbliche (o la loro forma crittografata o hash). In secondo luogo, la fase c.d. di «payload» (ovvero il «carico utile», la parte di dati trasmessi effettiva che è destinata all'utilizzatore) all'interno di una transazione. Questi dati vengono forniti come input dagli utenti, attraverso un client; vengono successivamente elaborati dai miner e convergono nei blocchi della catena, che saranno, infine, condivisi ed archiviati tra tutti i nodi dell'ecosistema. Stesse considerazioni valgono nel caso degli smart contract [Sater 2017, 19 e Fischer, Grechenig, Niemeier, Schmelz, Zhu 2018, 224-225].

I dati della transazione da includere nel blocco generalmente contengono la chiave pubblica dell'autore della richiesta, il contenuto della transazione, la chiave pubblica del destinatario e una firma crittografica. Il blocco contiene le transazioni più alcuni altri dati, come l'intestazione del blocco e quella del blocco precedente. I dati nei blocchi assumono forme diverse a seconda delle esigenze di esecuzione del protocollo, di efficienza nel funzionamento del sistema o di accessibilità e riservatezza: alcuni dati possono essere «in chiaro» e altri possono essere trasformati grazie alla crittografia. Questo aspetto è cruciale con riferimento alla definizione di dato personale, in quanto l'utilizzo di tecniche crittografiche andrà vagliato attraverso la lente dei concetti di pseudonimizzazione e anonimizzazione. Le definizioni qui diventano fluide e la loro applicabilità dipende in larga misura dal contesto tecnologico (in costante e rapida evoluzione).

Un'altra considerazione chiave è che l'uso di una blockchain può implicare la connessione alla rete attraverso l'uso di un indirizzo IP, il quale può essere rintracciato, nonostante l'adozione di tecniche di anonimizzazione della navigazione (ad es. attraverso Tor o simili).

Le caratteristiche dei dati delle transazioni non possono essere a priori descritte in modo completo, in quanto dipendono fortemente dal caso d'uso e dalle peculiarità a questo intrinseche. Più in generale, si pensi ai contenuti estremamente vari che possono essere oggetto di trattamento da parte degli smart contract. Di conseguenza, la presenza di dati personali all'interno del contenuto delle transazioni, unitamente alle potenziali misure di crittografia applicate a tali dati, deve essere valutata caso per caso.

Ad ogni modo, la presenza di chiavi pubbliche per indicare i soggetti delle transazioni – riferendosi quindi, di regola, direttamente ad un soggetto (individuo o persona giuridica) – rimane essenziale per il funzionamento della blockchain. Inoltre, indipendentemente dal fatto che il contenuto delle transazioni sia o meno qualificabile come un dato personale, da un punto di vista più generale si può ritenere che la presenza stessa di interazioni tra attori all'interno della blockchain possa rappresentare di per sé un'informazione rilevante.

Si noti infine che un comune suggerimento al fine di rendere la blockchain maggiormente conforme alla disciplina in materia di protezione dei dati personali è quello di prevedere l'archiviazione dei dati personali fuori dalla catena (off-chain), lasciando all'interno i soli «puntatori» ai dati originali [Zyskind, Nathan, Pentland 2015]. Tali soluzioni cd. off-chain però non sono del tutto esenti dal rischio che l'ampia nozione di identificabilità e il restrittivo approccio al concetto di anonimizzazione porti a dover considerare anche questi dati e metadati come dati personali. Argomenti analoghi valgono per le c.d. side-chain, le quali consistono in blockchain separate che vengono collegate a quella principale.

La questione è complessa e merita approfondimenti che non possono essere sviluppati nell'ambito di un manuale. Un ecosistema blockchain normalmente tratta dati personali ai sensi dell'art. 4 (generalmente in forma pseudonimizzata). La disciplina in materia di protezione dei dati personali sarà quindi di regola applicabile.

Per concludere con l'ambito territoriale, questo dipende fortemente dall'allocazione dei vari ruoli privacy all'interno della struttura blockchain di cui si tratterà nel prossimo paragrafo [Arisi, Guarda 2020, 486-487]. In prima approssimazione si può, comunque, supporre che, poiché esiste una rete peer-to-peer, indipendentemente dal livello di decentramento e distribuzione, e quindi se la blockchain sia pubblica o privata (o, ancora, ibrida), la transnazionalità rappresenta una caratteristica intrinseca di questo scenario [Finck 2019, 102]. È, dunque, probabile che il GDPR si applichi alle blockchain in modo estensivo: semmai può diventare elemento critico e, talvolta, di difficile gestione quello del trasferimento di dati verso paesi terzi.

17.3.2 Principi in materia di protezione dei dati personali

L'art. 5 del GDPR codifica i principi fondamentali per il trattamento dei dati personali. Alcuni tra questi rivestono una posizione rilevante nel contesto blockchain.

Anzitutto i dati devono essere trattati in modo lecito, corretto e trasparente (art. 5, par. 1, GDPR). In particolare, la liceità richiede di individuare una base giuridica per il trattamento dei dati sulla blockchain. Come già introdotto nel Capitolo 5, l'art. 6 prevede alcune condizioni alternative. Tra queste può sicuramente rilevare nel nostro scenario applicativo il consenso al trattamento, ex art. 6, par. 1, lett. a). La regola è ricalcata, con alcune peculiarità specifiche, nell'art. 9, par. 2, lett. a), con riferimento al trattamento di categorie particolari di dati. In una blockchain, tuttavia, la prestazione del consenso si estrinsecherebbe, di regola, in un comportamento di tipo passivo, derivante dalla scelta di fatto di utilizzare la blockchain da parte dell'utente; ciò con chiare criticità con riferimento alle caratteristiche del consenso previste all'art. 7. Lo stesso diritto di revocare il consenso, inoltre, non risulterebbe sempre facilmente esercitabile [Courcelas, Lyons, Timsit 2019, 25].

Altra possibile condizione è quella prevista all'art. 6, par. 1, lett. b) relativa alla necessità del trattamento per l'esecuzione di un contratto di cui l'interessato è parte. Anche tale previsione presenta alcune incertezze applicative fintantoché non vi sia un accordo o una definizione precisa della governance. Da ultimo, potrebbe entrare in gioco anche quanto sancito all'art. 6, par. 1, lett. f) GDPR che legittima il trattamento di dati qualora sia necessario per il perseguimento di un legittimo interesse da parte del titolare, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato[8]. Tale regola richiede, però, un attento vaglio prima di poterne confermare la sua applicabilità.

I principi di correttezza e trasparenza appaiono, invece, meno problematici, nonostante la potenziale asimmetria informativa [Ianez, O'Hara, Simperl 2018, 6]. La realizzazione di tali principi si lega inscindibilmente all'insieme dei diritti in materia di comunicazione, informazione e accesso di cui agli artt. 12-15 GDPR e a quanto ribadito dal Considerando 39.

8 Si v. Gruppo art. 29, *Parere 6/2014 sul concetto di interesse legittimo del responsabile del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE*, 9 aprile 2014.

Sebbene non sia del tutto chiaro quali soggetti debbano fornire queste informazioni e con quali modalità, soprattutto in riferimento agli ambienti pubblici, è evidente come tale divulgazione di informazioni possa davvero svolgere un ruolo chiave nel fornire consapevolezza agli utenti di una blockchain. Inoltre, ciò interseca la questione relativa al come debba essere considerata la «scelta informata» dell'utente-nodo-interessato: questo problema può essere affrontato adeguatamente solo una volta definita la governance dell'intero processo di trattamento [Arisi, Guarda 2019, 491].

Il rispetto del principio della limitazione della finalità (art. 5, par. 1, lett. b)) appare in linea teorica rispettato tenuto conto del fatto che il trattamento dei dati in una blockchain persegue normalmente un protocollo e una funzione specifici. In realtà, però, l'impossibilità di esercitare il controllo sulla diffusione e l'utilizzo dei dati, se resi pubblicamente disponibili, renderebbe in alcuni scenari impraticabile la conformità con tale principio [Fink 2019, 104].

Inoltre, il fatto che tutti i nodi elaborino le informazioni, caratteristica intrinseca della tecnologia, può essere considerato in contrasto con il principio di minimizzazione dei dati di cui alla lettera c), che impone di limitare il trattamento ai soli dati strettamente necessari al raggiungimento della finalità per la quale sono trattati [Ibanez, O'Hara, Simperl 2018, 6-8]. La presenza di dati personali potrebbe essere sostanzialmente limitata, anche se non completamente evitata, sin dalla progettazione, con l'applicazione di soluzioni volte a limitare la presenza di dati stessi nella blockchain, o comunque a tutelarne la confidenzialità (si veda la pseudonimizzazione o le altre tecniche di crittografia) [Arisi, Guarda 2020, 491-492 e De Filippi, Wright 2018, 115-116].

Simili considerazioni possono essere svolte con riferimento al rispetto del principio di limitazione della conservazione (art. 5, par. 1, lett. e)). Il tempo per il quale le informazioni vengono conservate non può essere facilmente determinato in una blockchain, ma le soluzioni di cui sopra si faceva cenno possono essere opportunamente ponderate attraverso una valutazione legale del rischio di re-identificazione. Il limite di conservazione si riferisce, infatti, ai dati «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 (…)».

Il fatto che i dati non possano essere modificati o cancellati in una blockchain (o che tali operazioni siano tecnicamente talmente gravose da apparire non realizzabili) porta a dover considerare il principio di accuratezza di cui all'art. 5, par. 1 lett. d), strettamente connesso ai diritti di rettifica (art. 16), cancellazione (art. 17), nonché limitazione del trattamento (art. 18). Da una prospettiva più ampia, l'accuratezza dei dati è una delle idee centrali della blockchain perché il registro stesso viene creato al fine di permettere agli utenti l'accesso allo stato aggiornato delle transazioni. Ciò sebbene la blockchain stessa non garantisca che ogni informazione in essa registrata sia di per sé corretta, ma piuttosto l'avvenuta transazione. Tuttavia, se si verifica una rettifica, i record pertinenti rimarrebbero nel registro distribuito, poiché i dati sulla blockchain non possono essere modificati.

Infine, ai sensi del principio di integrità e riservatezza di cui all'art. 5, par. 1, lett. f), i dati devono essere trattati in modo tale da garantirne la sicurezza: ciò significa che il rischio di trattamento non autorizzato o illecito, e di perdita, distruzione o danneggiamento accidentali deve essere mitigato mercé l'applicazione di misure tecniche e organizzative adeguate. Da un lato, la tecnologia blockchain è generalmente nota per la sua resilienza e sicurezza, sebbene non immune dai cd. «attacchi». La blockchain è sempre stata raccontata come una tecnologia robusta e infallibile, in quanto concepita con tecniche avanzate di consenso distribuito, fiducia consolidata e informazioni sempre verificabili. Occorre prestare attenzione alla sicurezza dell'infrastruttura blockchain e attacchi di tipo DDoS (*Direct Denial of Service*) non sono infrequenti: si tratta di un tentativo di paralizzare il nodo di una blockchain, inondandolo con un volume elevato di traffico. D'altra parte, dal punto di vista della protezione dei dati personali la garanzia di protezione contro un possibile trattamento non autorizzato (o illecito) costituisce una criticità in special modo nel caso di blockchain pubbliche, dove i dati sono apertamente accessibili e pubblicamente disponibili. Anche per l'applicazione di tale principio molto dipenderà dalle scelte di design che si porranno in essere allorquando si deciderà di utilizzare una blockchain per trattare dati personali.

Da ultimo, il principio di accountability stabilito al paragrafo 2 dell'art. 5 GDPR rappresenta un punto fondamentale nell'applicazione della disciplina in materia di protezione di dati personali. Al netto delle difficoltà

più volte palesate di individuare chiaramente i soggetti impegnati nel trattamento dei dati, l'allocazione delle responsabilità deriverà anche dalle valutazioni poste in essere con riferimento ai rischi che i diversi scenari applicativi possono presentare e dalle misure di sicurezza adottate al fine di mitigarne l'impatto.

17.3.3 Gestione dei ruoli privacy

Una questione preliminare a molte altre è quella dell'attribuzione dei ruoli privacy in una blockchain. Questo rappresenta un aspetto decisivo nell'applicazione della totalità delle regole del GDPR ed in linea con il principio di accountability a cui si è fatto subito sopra cenno.

Nel Capitolo 3 abbiamo già introdotto la definizione dei vari attori che entrano in gioco nella governance del trattamento di dati: titolare del trattamento, responsabile del trattamento, autorizzato, ecc. Di seguito si declineranno queste regole generali sul nostro peculiare contesto applicativo, consapevoli del fatto che fare riferimento ad uno «scenario blockchain» rappresenta una semplificazione: poiché si parla di blockchain per descrivere una tecnologia generica o, almeno, un ampio cambio di paradigma, è molto difficile identificare l'utilità della blockchain in un unico modello di business.

Una premessa necessaria è che, come è stato per Internet, la blockchain potrebbe non determinare l'eliminazione di tutti gli intermediari, ma potrebbe comportare forti cambiamenti negli intermediari esistenti, implicando eventualmente un'ibridazione dei ruoli e l'emergere di nuove figure [De Filippi, Wright 2018, 279 e Moerel 2018, 834]. Di conseguenza, anche l'interazione dell'utente con l'ecosistema sarebbe complessa e poliedrica. Come afferma Michèle Finck [Finck 2019, 101]:

> Whereas, in the early stages of the technology's development, many Data subjects have directly engaged with the network itself, this may become exceptional in the future, as Data subjects are more likely to communicate only with the application layer. This is easier for GDPR purposes, because it reintroduces the central entity the legislation was crafted for.

Inoltre, la definizione dei ruoli interseca ovviamente il tema della differenza tra blockchain pubbliche e private. L'importanza di queste classificazioni sta nella possibilità di definire sistemi aperti a cui tutti possono accedere, o ambienti chiusi riservati solo ad attori identificati e autorizzati, oltre alla possibilità di impegnarsi nella scrittura di transazioni nella blockchain e/o partecipare all'attività di validazione o creazione di blocchi. Partendo da tale prospettiva, appare chiaro come nel caso di blockchain pubblica ci sarebbero utenti indefiniti e la cui identità potrebbe anche essere sconosciuta; scenario completamente diverso è quello che caratterizza, invece, una blockchain privata dove l'accesso e la partecipazione sono soggetti a identificazione (e autorizzazione).

Considerando i principali «attori» in questo contesto tecnologico, gli sviluppatori giocano un ruolo fondamentale. La loro categoria è una delle più discusse rispetto alla governance blockchain. In questo ampio termine possono rientrare molti contributori diversi: gli autori del protocollo di rete, coloro che partecipano alla creazione della pluralità di strumenti implementati sulla blockchain, gli autori di smart contract. Anche il contesto in cui operano è fondamentale alla definizione del loro ruolo e quindi è possibile differenziare tra la figura classica e tradizionale dei partecipanti a comunità collaborative e progetti open source e quanti operano, invece, dietro compenso per grosse società.

I c.d. nodi, o peer, sono i principali partecipanti alla blockchain. In sostanza, i nodi convalidano le transazioni, secondo diversi meccanismi di consenso[9]. Tuttavia, essi sono essenzialmente macchine, computer: la loro attività è automatizzata. Gli altri attori rilevanti da citare, infatti, sono i soggetti che si avvalgono di queste macchine: gli utenti finali.

La letteratura sull'argomento è copiosa e le diverse sfumature tra gli autori potrebbero essere apprezzate solo attraverso uno studio approfondito [Arisi, Guarda, 2020, 485 e Finck 2019, 100-102][10]. Si discute an-

9 C'è incertezza sulla completa giustapposizione del ruolo di nodo e miner nella blockchain Bitcoin: quest'ultimi, infatti, normalmente gestiscono un nodo completo, ma partecipano anche alla creazione di blocchi e agiscono per la propria ricompensa.

10 Si veda anche *Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data,* Report of Commission Nationale de l'Informatique et des Libertés (CNIL), French Data Protection Authority, 2018, 1-4, https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data.

zitutto se sia possibile rinvenire la figura del titolare del trattamento e quella del responsabile del trattamento in un contesto blockchain. Tale ruolo in capo agli sviluppatori di protocolli o ai creatori di smart contract è dibattuto. Alcuni commentatori suggeriscono, poi, che, tenuto conto dell'attività svolta, i nodi stessi potrebbero essere qualificati titolari del trattamento, o anche come contitolari in un ecosistema così complesso. Si sostiene anche che il funzionamento tecnico della blockchain pubblica implichi che i vari nodi siano da considerarsi responsabili del trattamento.

Nel complesso, la soluzione più efficace di conformità alla disciplina in materia di protezione dei dati personali appare più agevole per gli ambienti privati e/o autorizzati, alla luce di potenziali accordi *ad hoc* per l'assegnazione dei ruoli e del fatto che il trattamento dei dati personali potrebbe essere disciplinato a livello applicativo. Da altra prospettiva, l'obbligo relativo ad una struttura trasparente per l'allocazione delle responsabilità di cui al GDPR appare in diretta contraddizione con ciò che l'avvento delle blockchain mirava ad eliminare. Tale obbligo potrebbe poi essere meno impegnativo e stringente a seconda del contesto normativo di riferimento.

17.3.4 I diritti dell'interessato

Come noto, il GDPR agli articoli 12 e seguenti stabilisce una serie di diritti in capo all'interessato del trattamento. La possibilità del loro esercizio in un contesto blockchain merita un approfondimento.

Vi sono diritti che non presentano particolari criticità, che possono essere definiti come compatibili con la tecnologia qui in oggetto e per i quali non svolgeremo un approfondimento specifico: il diritto ad ottenere informazioni, comunicazioni trasparenti (artt. 12-14); il diritto d'accesso (art. 15); il diritto alla portabilità dei dati (art. 20).

Sicuramente più difficile appare, invece, garantire l'applicabilità del diritto di rettifica, di cancellazione e di opposizione ad un processo automatizzato.

Il diritto alla cancellazione sancito all'art. 17 può essere attivato in diverse circostanze, tra le quali, ad esempio, qualora i dati non siano più necessari per il raggiungimento della finalità (par. 1, lett. a)) o nel caso di revoca del consenso (par. 1, lett. b)). Vengono, poi, elencati, al para-

grafo 3, i motivi per i quali, invece, esso non è applicabile; tra gli altri si ricordano: l'adempimento di un obbligo legale, l'esecuzione di un compito svolto nel pubblico interesse o nell'esercizio di pubblici poteri (lett. b)); il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente (lett. c)); l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria (lett. d)).

Questo argomento è sicuramente tra quelli più controversi e ha suscitato il maggior clamore nel dibattito circa la presunta incompatibilità tra GDPR ed una tecnologia, quale quella blockchain, che fa dell'immutabilità del dato una delle sue peculiarità principali. Sebbene alcuni autori contestino il fatto che tale diritto sia assoluto e affermano che esso deve comunque essere oggetto di un bilanciamento di interessi e quindi di una valutazione caso per caso [Moerel 2018, 846], è innegabile che qualora venga avanzata una richiesta di cancellazione dei dati in una blockchain, il problema da un punto di vista tecnico si porrebbe sicuramente. Le stesse criticità emergono evidentemente anche con riferimento all'esercizio del diritto di rettifica (art. 16) e di limitazione del trattamento (art. 18), in quanto presentano simili esigenze di intervenire sui dati trattati.

Alcuni vedono nella off-chain la soluzione alla cancellazione. Tuttavia, anche se i dati personali possono essere cancellati da questa, il problema si sposta sui metadati on-chain e continua a riguardare le chiavi pubbliche [Finck 2019, 107]. Uno dei temi più discussi è se la crittografia possa essere d'aiuto, in quanto i dati sarebbero in caso crittografati nella blockchain ma la chiave di crittografia verrebbe distrutta. Nell'ambito dell'attuale quadro giuridico, la risposta sulla cancellazione appare comunque essere negativa, in quanto non esiste al momento una tecnica che possa azzerare completamente il rischio di re-identificazione delle informazioni [vedi → Capitolo 12] [Fink 2019, 107].

Il paragrafo 2 dell'art. 17 potrebbe presentare indicazioni utili ad adattarne l'applicazione alla realtà blockchain:

> 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.

Questa previsione potrebbe aprire a soluzioni alternative tenuto conto delle peculiarità della blockchain anche nella sua versione pubblica. Il titolare sarebbe quindi obbligato ad adottare tutte le misure ragionevoli, comprese le misure tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta al fine di eliminare eventuali collegamenti ai dati o copie o repliche degli stessi, ma tenendo conto della tecnologia disponibile e dei costi di attuazione [Finck 2019, 107].

La stessa natura del diritto alla cancellazione potrebbe venire in soccorso [vedi → Capitolo 8]. La norma può essere oggetto di interpretazione e gli autori ritengono che ci possa essere spazio per esplorare diverse soluzioni di cancellazione che potrebbero superare le carenze delle blockchain [Fink 2019, 108 e Moerel 2018, 845-846]. Al riguardo si può richiamare l'esempio tedesco: in caso di impossibilità o di sforzo sproporzionato nella cancellazione, a causa di specificità nelle modalità di conservazione, l'art. 35 della Bundesdatenschutzgesetz opta allora per la limitazione del trattamento (salvo che il trattamento sia illecito). Soluzioni di questo tipo sembrano di superare le carenze tecniche delle blockchain e la presunta incompatibilità assoluta con il GDPR [Arisi, Guarda 2020, 493].

Infine, merita di essere citato quanto previsto dall'art. 22 GDPR. Nel Capitolo 13 abbiamo già avuto modo di affrontare la portata applicativa di questo diritto dell'interessato a non esser oggetto ad una decisione basata unicamente su un processo decisionale automatizzato che produca un effetto giuridico che lo riguarda o che incida in modo significativo sulla sua persona. Non è chiaro se questa norma possa trovare applicata in una blockchain: mentre non si esclude che i dati in una blockchain pubblica possano portare alla profilazione attraverso il raggruppamento e il riconoscimento di pattern, si discute se il suo funzionamento stesso implichi un processo decisionale automatizzato. La questione viene sollevata rispetto ai già citati smart contract [Fink 2019b]. Stante il loro ipotizzabile utilizzo in scenari applicativi dove possono divenire strumenti adatti a modificare lo stato giuridico dell'interessato al trattamento, determinando una serie di operazioni automatiche che esitano in conseguenze dalla rilevanza giuridica, gli smart contract possono configurarsi

come idonei all'applicabilità dell'art. 22 GDPR e, quindi, il loro design e scrittura necessita di essere pensato in modo conforme alla disciplina in oggetto fin dalle prime fasi di progettazione.

17.4 Caso 17-1

Caso 17-1

Un'impresa di servizi logistici che contribuisce a commercializzare prodotti sanitari e per la cura della persona, ivi inclusi prodotti attinenti alla sfera sessuale, su tutto il territorio nazionale, nonché in Svizzera, decide di gestire tutti i passaggi delle merci e le operazioni dei propri dipendenti tramite una blockchain privata, e così esercitare un controllo più certo sui propri flussi informativi. L'impresa prescrive che ad ogni operazione (ad esempio di trasporto, manipolazione, consegna, etc.) il proprio dipendente o il dipendente dell'impresa a cui ha delegato determinate operazioni registri nella blockchain la transazione, inserendone i dati (ivi incluso il nome, cognome e ID lavoratore, eventuali dati del cliente finale, risultato dell'operazione, ID operazione, luogo e data dell'operazione). L'impresa chiede ad una società che offre servizi di risorse umane di effettuare controlli a campione su questi dati, anche per verificare l'adempimento dei turni di lavoro assegnati ai propri dipendenti e assegnare così le ferie o prescrivere eventuali visite mediche che si rendano necessarie, nonché verificare il rispetto dei contratti conclusi con altre imprese, specialmente quelle che operano fuori dal territorio nazionale.
Quali sono i dati personali trattati?
Qual è l'organizzazione dei ruoli nell'ambito del trattamento di dati?
Qual è la base giuridica di questo trattamento?
Quali sono le criticità di questo scenario applicativo?
Quali sono le misure adeguate da adottare in tale contesto?

CAPITOLO 18.
Sorveglianza e controllo

Giorgia Bincoletto

18.1 Dal Panopticon al Surveillance Capitalism

Il concetto di sorveglianza può essere declinato in diverse accezioni [Comandè 2021, 341-346]. Secondo una prospettiva filosofica, nel diciottesimo secolo Jeremy Bentham ha elaborato il concetto di Panopticon: una prigione ideale a forma radiale in cui un numero limitato di guardie - posizionate all'interno di una torre di osservazione al centro della struttura - è in grado di controllare costantemente le celle dei prigionieri, i quali non hanno la certezza che qualcuno li stia osservando proprio in quel momento, ma la cui sola possibilità ciò avvenga li porta a conformarsi alle regole, a non tentare l'evasione [Bentham 1983]. Questa è oggi la più conosciuta metafora di sorveglianza. Un altro famoso autore, Michel Foucault, nel secolo successivo ha poi spiegato che il Panopticon si basa su un sistema gerarchico, permanente e funzionale di sorveglianza in cui i soggetti non sono e non saranno liberi di agire perché il loro subconscio, condizionato dal contesto, li costringerà a cambiare comportamento, adattandosi a quanto richiesto dal controllore [Foucault 1975]. Gli individui così si conformano ai valori dell'ordine sociale.

Adottando un diverso punto di vista, questa volta letterario, George Orwell ha presentato una società distopica in cui l'unico grande occhio (*Big Brother*) sorveglia ogni aspetto della vita dei cittadini, privandoli di libertà e privacy [Orwell 2017]. Nel mondo di 1984 le telecamere controllate dal partito unico trasmettono la propaganda e riprendono ogni attività.

Con il termine sorveglianza, perciò, si può intendere l'attenzione assidua da parte di qualcuno per una determinata finalità.

Di per sé la sorveglianza è un concetto neutro e rappresenta un fenomeno diffuso. L'accezione negativa del termine potrebbe emergere in ambito giuridico quando essa viene compiuta in modo pervasivo, in violazione della vita privata e familiare e/o della protezione dei dati personali degli individui e di altri diritti e libertà fondamentali.

Nel 1966 il professore statunitense Alan Westin individuava quattro passi fondamentali per l'uso di dispositivi o processi di sorveglianza, al di là della tipologia di strumento coinvolto [Westin 1966]:

1. stabilire regole per limitare i soggetti che possono effettuare la sorveglianza;
2. stabilire norme dettagliate per l'ambito, la durata e il funzionamento del controllo;
3. creare un'agenzia generale per stabilire degli standard, monitorare gli utilizzi e valutare la loro compliance e quanto necessario sanzionare le violazioni delle regole;
4. formulare regole per disciplinare la divulgazione e l'uso delle informazioni ottenute, come ad esempio durante un processo.

I progressi tecnologici degli ultimi decenni hanno reso possibile aumentare la sorveglianza sia nel settore pubblico, ad esempio per finalità di pubblica sicurezza e controllo della criminalità, che nel settore privato, per la tutela di beni aziendali o della sicurezza personale, anche tramite sistemi di riconoscimento facciale che utilizzano l'intelligenza artificiale.

Come scritto da Rodotà, i cambiamenti resi possibili dalla tecnologia hanno creato trasformazioni profonde che favoriscono la nascita di una società della sorveglianza, del controllo, della classificazione, della selezione sociale, operanti in modo generalizzato [Rodotà 2009]. Si è di fronte ad un moderno modello di Panopticon, così descritto dallo stesso Rodotà:

> La sorveglianza si trasferisce dall'eccezionale al quotidiano, dalle classi 'pericolose' alla generalità delle persone. La folla non è più solitaria e anonima. La digitalizzazione delle immagini, le tecniche di riconoscimento facciale consentono di estrarre il singolo dalla massa, di individuarlo e di seguirlo. Il data mining, l'incessante ricerca di

> informazioni sui comportamenti di ciascuno, genera una produzione continua di 'profili' individuali, familiari, di gruppo: ancora una volta, la sorveglianza non conosce confini. Non è arbitrario, quindi, analizzare quest'insieme di mutamenti dal punto di vista di un modello di Panopticon che, distaccandosi dall'originaria sua matrice carceraria, investe l'insieme delle relazioni sociali. Qui emerge con particolare nettezza il fatto che la sorveglianza genera nuovi assetti dei poteri, modificando la condizione di ogni soggetto.

Questa sorveglianza «di massa» raccoglie dati personali su larga scala ed è compiuta sia da attori pubblici che privati. Rispetto al Panopticon di Bentham, la sorveglianza è rafforzata sia sul piano del controllo governativo (*Big Government*), che di grandi aziende private (*Big Business*) [Faini 2019].

La questione fondamentale è cercare un punto di equilibro tra l'istanza individuale di privacy (qui intesa come riservatezza e protezione dei dati personali) e quella di sicurezza, che può essere collettiva o anch'essa singolare. I due concetti sono stati posti spesso in modo antagonista anche alla luce di quanto è successo l'11 settembre 2001, avvenimento da cui è conseguito un incremento dei poteri di sorveglianza in capo agli organi esecutivi, prima degli Stati Uniti e poi anche di altri stati [Guarda 2004]. Un maggiore livello di sicurezza pubblica implicherebbe così una minore tutela degli individui.

Al contempo, la normativa in materia di protezione dei dati personali utilizza oggi un concetto di sicurezza diverso che riguarda l'implementazione di misure tecniche e organizzative al fine di tutelare l'integrità e la confidenzialità delle informazioni. In questo caso, quindi, maggiore è la sicurezza, maggiore è la protezione del dato personale e per sua estensione della sfera giuridica del singolo.

Diversi sono i contesti in cui emerge ancora la tensione tra forme di sicurezza e privacy.

Il problema della sorveglianza come invasione della riservatezza rileva soprattutto in relazione al controllo dei lavoratori da parte del datore di lavoro con sistemi audiovisivi [vedi → Capitolo 9] e in presenza di installazione di videocamere, che avviene abitualmente e soprattutto in luoghi pubblici, ma può riguardare anche ambienti privati, quali abitazioni e condomini.

Come si vedrà in questo capitolo l'utilizzo di tali sistemi comporta anche la gestione dei dati personali raccolti. Se da un lato si avranno esigenze di protezione della sicurezza di beni e persone, dall'altro è necessario trovare un bilanciamento con la salvaguardia dei diritti alla riservatezza e alla protezione dei dati personali.

La sorveglianza può anche operare attraverso il controllo del traffico e dei dati personali su Internet. Come anticipato nel Capitolo 6 sui trasferimenti internazionali di dati, un sistema di pervasiva sorveglianza di massa è stato denunciato da parte di Edward Snowden con riferimento alle attività operate dalle agenzie federali statunitensi. Lo scandalo «Datagate» è strettamente legato alle misure che gli Stati Uniti hanno adottato a seguito degli attacchi terroristici dell'11 settembre 2001. Questa sorveglianza «pubblica» opera attraverso la raccolta e l'analisi di grandi quantità di dati personali riferiti a persone di tutto il mondo con la finalità di sicurezza e prevenzione di rischi per la democrazia. Un controllo così costante ed invasivo, tuttavia, si traduce in una violazione sistematica del diritto alla protezione dei dati personali, dell'autodeterminazione dei singoli e dei valori fondanti di una società democratica.

Il monitoraggio delle attività online è anche svolto dalle grandi piattaforme che trattano dati personali su larga scala e hanno a disposizione i cd. Big Data [Richards 2013, 1939]. L'espressione suggestiva «liquid surveillance» è stata così proposta per indicare le nuove dinamiche della sorveglianza che nella società moderna si diffondono in modo fluido e dinamico, anche nei confronti dei consumatori [Bauman, Lyon 2012].

Zuboff elabora la teoria del «capitalismo della sorveglianza» [Zuboff 2019]. Secondo l'autrice, il capitalismo proprio dell'era digitale si appropria dell'esperienza umana per utilizzarla come materia prima da trasformare in dati sui comportamenti attuali e futuri degli individui. I dati ottenuti durante l'uso di prodotti e servizi, inclusi i dati personali, sono utilizzati per generare un surplus di informazioni in grado di testare e alimentare modelli predittivi che possono determinare cosa gli individui faranno in un prossimo e lontano futuro. Si crea così il «mercato dei comportamenti futuri» con cui i capitalisti della sorveglianza si arricchiscono per i loro stessi prodotti e servizi o tramite lo scambio dei risultati delle predizioni con altri portatori di interessi. Non solo i dati comportamentali sono usati per predire l'attività umana, ma anche per formarla, condizionarla e modificarla. Zuboff ritiene che questo potere sia fondato

su processi automatizzati che sempre più sono in grado di controllare l'esperienza umana senza limiti e ostacoli, con rischi concreti per la sopravvivenza della società democratica. Come scrive Zuboff rimane una speranza (pp. 533-534):

> La democrazia è vulnerabile a quel che non ha precedenti, ma la forza delle istituzioni democratiche è l'orologio che determina quanto tali ferite siano gravi e durature. In una società democratica il dibattito e il contesto garantito dalle istituzioni ancora solide può orientare l'opinione pubblica contro forme inattese di oppressione e ingiustizia, per mostrare la strada a leggi e giurisprudenza.

Tramite i meccanismi della sorveglianza delle piattaforme la persona è ridotta a materia prima e «datificata» da chi la controlla [Caso 2021, 340].

La tematica della sorveglianza nell'era digitale richiede l'analisi di molti contesti applicativi che i diversi sistemi giuridici possono decidere di governare in modo differente. Di recente, la pandemia ha, peraltro, creato nuove forme di controllo che, seppur temporanee, hanno richiesto attente riflessioni giuridiche.

Nelle prossime sezioni verranno affrontati due tradizionali problemi di sorveglianza, l'attività di controllo delle comunicazioni da parte dell'autorità pubblica e la videosorveglianza tramite l'installazione di dispositivi audiovisivi, e due nuove questioni emerse a seguito dell'emergenza sanitaria, l'uso di sistemi online per l'insegnamento a distanza e lo sviluppo di tecnologie per il tracciamento dei contatti. Con riferimento ai primi si è scelto di presentare le esperienze di specifici ordinamenti giuridici, rispettivamente gli Stati Uniti e l'Italia, dal momento che la regolazione in questi campi avviene a livello nazionale; con riferimento ai secondi, invece, si è preso a riferimento l'ordinamento dell'UE, fornendo poi un esempio di applicazione di app di tracking nel contesto italiano.

18.2 La sorveglianza elettronica nell'ordinamento statunitense

Un contesto tipico in cui la tutela della privacy si scontra con la dimensione della sicurezza è l'utilizzo di tecnologie di controllo da parte del potere pubblico, come le forze dell'ordine, per finalità di contrasto alla criminalità.

Quando il mezzo di comunicazione era il telefono «di rete fissa», l'attività di sorveglianza di comunicazioni era compiuta con congegni installati sulle linee telefoniche; con il passaggio alle nuove forme di comunicazione, quali telefoni cellulari ed e-mail, le operazioni invece iniziano ad essere effettuate attraverso tecnologie di intercettazione di tipo informatico [Guarda 2004, 329-334].

Questa moderna intercettazione, in particolare, può avvenire direttamente sul flusso delle comunicazioni o indirettamente attraverso i dati di traffico conservati nelle banche dati dei servizi di telecomunicazione o di contenuti multimediali, come è stato riscontrato con riferimento alle attività delle agenzie di intelligence durante i programmi di sorveglianza di massa [Resta 2015, 25].

Negli Stati Uniti la *law enforcement surveillance* è stata regolata sia grazie all'interpretazione della Costituzione sia tramite l'adozione di speciali *statute* a livello federale o statale [Solove, Schwartz 2021]. Peraltro, secondo Richards, un principio generale del diritto statunitense è che la sorveglianza è legittima, a meno che non vi sia una regola che la proibisca [Richards 2013].

Il primo riferimento è il Quarto Emendamento che prevede che le perquisizioni e i sequestri («searches and seizures») su un oggetto, un documento o una persona possano legittimamente avvenire solo a seguito dell'emissione di uno specifico mandato basato su una «probable cause». Con tale ultima espressione si può intendere l'esistenza di informazioni sul compimento o il probabile avvenimento di un'*offence* e non un mero sospetto [Solove, Schwartz 2021, 271].

Nel famoso caso *Katz v. United States* [vedi → Capitolo 1], la Corte Suprema ha così ritenuto che l'uso di un sistema di intercettazione (un telephone bug) da parte dell'FBI fosse illegittimo e violasse la «reasonable expectation of privacy» del cittadino perché avvenuto in assenza di un valido mandato.

Nel successivo caso *United States v. United States District Court*, 407 U.S. 297 (1972), la medesima Corta ha chiarito che il Quarto Emendamento si applica ai casi di sorveglianza con finalità di prevenzione e repressione dei dati, la cd. «domestic security» nel contesto del «law enforcement», e non a quella di tutela della sicurezza nazionale («foreign intelligence»).

L'Electronic Communications Privacy Act (ECPA) del 1986 è stato emanato a seguito dell'iniziale diffusione dei computer per fornire delle regole sulle comunicazioni elettroniche a livello federale. Questo Act è composto da tre parti che riguardano diverse tipologie di comunicazioni:
– il Wiretap Act, sulle intercettazioni;
– lo Stored Communications Act, sugli archivi elettronici;
– e il Pen Register Act, sui dispositivi che registrano i numeri di chiamata.

Con il «Communications Assistance for Law Enfocement Act» del 1994 è stato imposto alle società di telecomunicazione di sviluppare dei sistemi per rendere disponibili all'autorità di *law enforcement*, qualora richiesto in relazione a una «criminal investigation», delle intercettazioni delle comunicazioni elettroniche come disciplinate dall'ECPA. Tuttavia, tale *statute* federale non si applica alle e-mail [Solove, Schwartz 2021, 383].

A seguito degli attacchi alle torri gemelle l'Uniting and Strengthening America By Providing Appropriate Tools Required To Intercept and Obstruct Terrorism Act o «USA Patriot Act» ha disciplinato la sorveglianza di informazioni per esigenze di sicurezza nazionale contro il terrorismo. Questo *statute* consente alle autorità di *law enforcement* di rivolgersi ad un giudice per procedere ad una perquisizione o sequestro con una «delayed notice» rispetto al mandato richiesto dal Quarto Emendamento, qualora ci sia il rischio che un avviso comprometta l'indagine o la prova.

La sorveglianza elettronica è disciplinata anche a livello statale. La legislazione è spesso più protettiva della «federal electronic surveillance law». In molti casi, infatti, la normativa richiede il consenso di tutte le parti presenti per la registrazione di una comunicazione, oppure l'emissione di un mandato per l'installazione di uno strumento tecnologico [Solove, Schwartz 2021, 386-389].

Con riferimento alla videosorveglianza è possibile affermare che essa non è oggetto di regolamentazione da parte della «federal electronic suirveillance law», trovando applicazione solo il Quarto Emendamento. Per tale ragione e sulla base del famoso detto «who will watch the watchers?», Solove ha proposto cinque linee guida per la videosorveglianza nel contesto statunitense [Solove 2011]:

> 1. Accountability and transparency. All video surveillance should be subjected to oversight and review. Data should be kept about the per-

> formance and effectiveness of the surveillance, as well as of any abuses and problems.
> 2. Strong penalties for abuses. Any leaks or misuses of video surveillance information should be subject to strong penalties.
> 3. Deletion of old data. Video surveillance data shouldn't be maintained indefinitely. It should be deleted after a period of time. This prevents future misuse.
> 4. Prevention of mission creep. «Mission creep» refers to the phenomenon of a task's growing beyond its original parameters. In the case of video surveillance, it means data collected for one purpose coming to be used for other purposes, or technologies installed for one purpose later being used for another. The purposes of surveillance should be specified in advance, and data collected via surveillance should be used only for those purposes. Any new uses of the data must be approved by a court, and only after the government demonstrates that the benefits of the uses outweigh any harms to privacy and civil liberties.
> 5. Protection of First Amendment rights. Video surveillance data involving speech, protest, political association, religion, and the exploration of ideas and knowledge should be subject to the most stringent of protections. The government must avoid using this data except under the most compelling circumstances.

Per quanto riguarda, invece, il controllo elettronico per finalità di sicurezza nazionale, è necessario compiere ulteriori brevi precisazioni.

Il «Foreign Intelligence Surveillance Act» (FISA) del 1978 ha stabilito «standards and procedures» per l'uso di informazioni di sorveglianza elettronica per finalità di «foregin intelligence». Perciò, mentre l'ECPA si riferisce al «domestic law enforcement», il FISA crea un regime per l'attività delle agenzie federali di intelligence. A differenza del regime del Quarto emendamento, non è necessaria per la sorveglianza una «probable cause» di attività illecita. La regola costituzionale si applica, invece, anche ai sistemi di videosorveglianza richiedendo un order da parte del giudice per procedere alla raccolta delle informazioni. Il Patriot Act del 2001 ha modificato il FISA per ampliare i poteri di controllo. Nel 2008 e nel 2012 il FISA è stato nuovamente emendato per aumentare le possibilità di sorveglianza con l'aggiunta però di alcune cautele per la privacy per i soli cittadini statunitensi che si trovano all'estero [Solove e Schwartz 2021, 449-450].

Com'è noto, i programmi di sorveglianza di massa posti in essere a seguito degli attacchi terroristici di inizio secolo per esigenze di sicurezza pubblica prevedono la raccolta di informazioni personali su larga scala sia di utenti statunitensi che stranieri. A differenza di quanto qui sopra illustrato, le operazioni di questi programmi non avvengono in modo mirato su un determinato individuo, ma seguono la logica dei Big Data [Resta 2015, 25]. Le informazioni, infatti, sono raccolte in maniera automatica a partire da esistenti banche dati e poi analizzate per ricavare inferenze statisticamente rilevanti per le ricerche delle agenzie di intelligence.

18.3 I sistemi di videosorveglianza: l'esperienza italiana

La videosorveglianza consiste nell'installazione di impianti per esterno o per interno con telecamere e/o microfoni in grado di sorvegliare e registrare informazioni e con la finalità di sicurezza dei beni e delle persone che si trovano in un'abitazione privata, un'attività commerciale, un luogo di lavoro o un'area pubblica. Solitamente, i sistemi sono posizionati per sorvegliare specifiche aree e archiviano le immagini e/o i suoni in una memoria locale o direttamente in un cloud.

Se da un punto di vista tecnico è necessario valutare la tipologia e le caratteristiche dell'impianto, come la posizione dei sensori o la qualità di risoluzione dell'immagine, la modalità di registrazione, da una prospettiva giuridica è opportuno conoscere le regole specifiche in materia di telecamere di sicurezza.

In Italia in tema di videosorveglianza occorre tenere conto delle regole del GDPR, del Codice Privacy e delle indicazioni specifiche fornite dal Garante per la protezione dei dati personali. Fin dai primi anni Duemila l'autorità garante ha pubblicato linee guida per rendere compatibile l'installazione di telecamere con il diritto alla protezione dei dati personali, sia per il settore pubblico che privato[1].

In generale, l'installazione era considerata lecita solo se proporzionata alle finalità perseguite e le videocamere avrebbero dovuto raccogliere

1 Si v. le regole del 2004 in https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/1006052.

dati personali solo qualora non fosse possibile utilizzare dati anonimi. Secondo il Garante, le riprese avrebbero dovuto essere attive quando altre misure di protezione dei beni e delle persone non fossero sufficienti o attuabili (ad es., allarmi, controlli del personale). L'informativa poteva essere fornita anche con un modello semplificato (si ricordi il segnale ormai familiare con l'icona della telecamera e la scritta «area videosorvegliata»). I dati personali raccolti dovevano essere conservati per un tempo limitato. In alcuni casi, veniva richiesta un'autorizzazione per l'installazione dei vari sistemi.

A seguito dell'applicazione del GDPR e delle modifiche al Codice Privacy, è possibile affermare quali attività di trattamento di dati personali, il titolare che installa un sistema di videosorveglianza (VVS) dovrà:

- definire e mappare i ruoli del trattamento, delegando eventualmente un responsabile e nominando un DPO, rispettando il principio di accountability;
- determinare una valida base giuridica e una specifica finalità, che deve essere esplicita e legittima (principi di legalità, correttezza e trasparenza, limitazione della finalità);
- determinare i tempi di conservazione dei dati e così delle immagini registrate (principio di limitazione della conservazione);
- adempiere ai doveri di informazione e trasparenza mediante il rilascio di un'informativa ai sensi degli artt. 12-14 del GDPR e di una segnaletica di avvertimento (c.d. informazioni di primo livello);
- scegliere sistemi che minimizzino la raccolta dei dati personali (principio di minimizzazione);
- implementare misure tecniche e organizzative a proteggere i dati fin dalla progettazione e per impostazione predefinita, oltre alle misure di sicurezza (art. 25 e art. 32 GDPR che protegge l'integrità e la riservatezza dei dati personali);
- quando necessario, redigere un registro delle attività di trattamento (art. 30 GDPR) e la valutazione di impatto sulla protezione dei dati (art. 35 GDPR);
- consentire all'interessato l'esercizio dei diritti, tra cui il diritto di accesso. Tuttavia, tale accesso non dovrà ledere i diritti di altri soggetti.

Sulla necessità di minimizzare la raccolta dei dati personali il Garante aveva già indicato, in un decalogo sulla videosorveglianza del 2000, che

andrebbero registrate solo le immagini indispensabili, limitando l'angolo visuale delle videocamere ed evitando riprese dettagliate o ingrandite[2]. Quale misura organizzativa, peraltro, l'accesso alle riprese dovrebbe essere limitato a specifici soggetti autorizzati e le finalità secondarie o ulteriori dovrebbero essere valutate con attenzione. Le riprese, comunque, non dovrebbero essere diffuse dal momento che contengono dati personali. Potranno eventualmente essere rese disponibili all'autorità giudiziaria o di polizia in presenza di adeguati presupposti e nel contesto di un'attività investigativa in corso.

L'informativa, in aggiunta, dovrà essere collocata nei luoghi ripresi o nelle immediate vicinanze e dovrà essere chiara, visibile e comprensibile. Nel 2020 il Garante ha reso disponibile un nuovo modello semplificato che segue le Linee Guida 3/2019 dell'EDPB sul trattamento dei dati personali attraverso dispositivi video. Oltre all'icona di una telecamera è richiesta indicazione di varie informazioni: dove sia accessibile l'informativa completa; chi effettua la registrazione e i contatti del responsabile della protezione dei dati, se presente; il tempo di conservazione delle immagini; la finalità della videosorveglianza; i contatti per l'esercizio del diritto di accesso e degli altri diritti riconosciuti dalla normativa. Non è necessario indicare la collocazione precisa di una telecamera; tuttavia, dovrà essere evidente la zona soggetta al controllo in modo da consentire ai soggetti di adeguare il loro comportamento.

Non è attualmente richiesta alcuna autorizzazione da parte del Garante Privacy per l'installazione, ma seguendo il principio di proporzionalità e responsabilizzazione il titolare dovrà valutare con attenzione l'opportunità di utilizzare sistemi per le riprese. Con gli stessi principi dovrà essere determinato il periodo di conservazione, a meno che non vi siano regole specifiche derivanti da disposizioni di legge. Il Garante sul punto suggerisce di prevedere meccanismi automatici di cancellazione dopo pochi giorni[3].

Con riferimento all'installazione di sistemi di videosorveglianza da parte di persone fisiche in ambito privato o domestico e a tutela della si-

2 Il decalogo del 2000 è disponibile in https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/46822.

3 Si v. la FAQ n. 5 sulla videosorveglianza del 2022 in https://www.gpdp.it/temi/videosorveglianza.

curezza di persone o beni, il Garante Privacy ha individuato altre precise regole da seguire per evitare di incorrere nel reato di interferenze illecite nella vita privata (art. 615-*bis* c.p.)[4]. Non è necessaria un'autorizzazione o altra formalità se:

– le telecamere riprendono solo le aree di propria esclusiva pertinenza;
– misure tecniche per oscurare porzioni di immagini vengono attivate in tutti i casi in cui, per tutelare adeguatamente la sicurezza propria o dei propri beni, sia inevitabile riprendere parzialmente anche aree di terzi;
– viene acquisito formalmente il consenso del soggetto titolare di una servitù di passaggio nei casi in cui sulle aree riprese insista tale diritto. Il consenso può anche essere rilasciato una tantum;
– aree condominiali comuni o di terzi, quali cortili, pianerottoli, scale, parti comuni delle autorimesse, non sono oggetto di ripresa;
– aree aperte al pubblico, quali strade pubbliche o aree di pubblico passaggio, non sono oggetto di ripresa;
– le riprese non sono oggetto di comunicazione a terzi o comunque le immagini non sono diffuse.

All'interno dell'abitazione gli individui possono legittimamente installare delle cd. *smart cam* senza dover applicare la normativa in materia di protezione dei dati personali perché tale attività è effettuata «da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico» (art. 2, par. 2, lett. b) GDPR). Al contempo, se lavoratori, quali babysitter o collaboratori domestici frequentano questa abitazione, dovranno essere informati delle videocamere[5]. Il Garante suggerisce di evitare la loro collocazione in ambienti che potrebbero ledere la dignità dei soggetti ripresi, quali i bagni, e di adottare misure di sicurezza al fine di evitare la diffusione delle immagini su Internet.

In caso di installazione di telecamere in un condominio, sarà necessaria l'autorizzazione da parte dell'assemblea condominiale ai sensi

4 Si v. l'infografica del gennaio 2022 disponibile in https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9737891.

5 Si v. la FAQ n. 12 sulla videosorveglianza del 2022 in https://www.gpdp.it/temi/videosorveglianza.

dell'art. 1136 c.c. e con una maggioranza dei millesimi dei presenti. Anche in questo contesto, servirà un'informativa su appositi cartelli. Sul termine di conservazione delle immagini il Garante individua sette giorni come tempo congruo[6].

Il trattamento di dati personali realizzato da soggetti pubblici mediante sistemi di videosorveglianza può essere svolto per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri. Tra queste finalità potrebbero rientrare le installazioni in scuole e università, ospedali, sulla pubblica via. Non si applicherà la disciplina in materia di protezione dei dati personali a telecamere spente o non funzionanti e ad attività di ripresa ad alta quota con droni che non consentono l'identificabilità nemmeno indiretta di persone fisiche[7]. Per quanto riguarda l'attività di videosorveglianza a scuola, in cui spesso si trovano minori, l'autorità ha specificato che l'utilizzo deve essere limitato a casi di stretta indispensabilità per tutelare il patrimonio da atti vandalici e quindi le riprese dovranno essere indirizzate a limitate aree di interesse[8].

Con riferimento ai comuni è necessario che venga stipulato un «patto per la sicurezza urbana tra Sindaco e Prefettura» ai sensi dell'art. 5 del d.l. 20 febbraio 2017, n. 14 «Disposizioni urgenti in materia di sicurezza delle città». In presenza di azioni di prevenzione e di contrasto alle forme di illegalità presenti nel territorio e di promozione del rispetto del decoro urbano un comune può installare sistemi di videosorveglianza previo accordo con la competente prefettura con cui si determinano le specifiche aree, si istituisce una cabina di regia e si definiscono i tempi e le modalità di intervento. I comuni che utilizzano sistemi di videosorveglianza in luoghi pubblici aperti al pubblico devono peraltro conformarsi all'art. 6, co. 8 del d.l. 23 febbraio 2009, n. 11, che prescrive che:

6 Si v. la FAQ n. 11 sulla videosorveglianza del 2022 in https://www.gpdp.it/temi/videosorveglianza.

7 Si v. la FAQ n. 11 sulla videosorveglianza del 2022 in https://www.gpdp.it/temi/videosorveglianza.e il Parere 3/2019 dell'EDPB disponibile in https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_it.pdf.

8 Si v. la FAQ n. 14 su scuola e privacy in https://www.garanteprivacy.it/home/faq/scuola-e-privacy.

> la conservazione dei dati, delle informazioni e delle immagini raccolte mediante l'uso di sistemi di sorveglianza è limitata a sette giorni successivi alla rilevazione, fatte salve esigenze di ulteriore conservazione.

In caso di videosorveglianza su larga scala di una zona accessibile al pubblico è sempre necessaria la valutazione di impatto o DPIA (art. 35, par. 3, lett. c) del GDPR).

Le telecamere possono anche essere «intelligenti» e dedurre informazioni da quanto registrato. Il Garante Privacy ha recentemente specificato che attualmente, e comunque fino al 31 dicembre 2023, in Italia non sono consentiti l'installazione e l'uso di sistemi di riconoscimento facciale tramite dati biometrici, eccetto il caso in cui il trattamento dei dati personali non sia effettuato per indagini della magistratura o prevenzione e repressione dei reati[9]. In presenza di queste finalità, peraltro, si applicheranno le regole della Direttiva 2016/680 e del d.lgs. 51/2018 [vedi → Capitolo 7]. La legge di conversione del decreto capienze del 2021 ha infatti previsto una moratoria all'impiego di sistemi di videosorveglianza con riconoscimento facciale in luoghi pubblici e aperti al pubblico. In particolare, all'art. 9 si prevede che:

> 9. In considerazione di quanto disposto dal regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, nonché dalla direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, e dell'esigenza di disciplinare conformemente i requisiti di ammissibilità, le condizioni e le garanzie relativi all'impiego di sistemi di riconoscimento facciale, nel rispetto del principio di proporzionalità previsto dall'articolo 52 della Carta dei diritti fondamentali dell'Unione europea, l'installazione e l'utilizzazione di impianti di videosorveglianza con sistemi di riconoscimento facciale operanti attraverso l'uso dei dati biometrici di cui all'articolo 4, numero 14), del citato regolamento (UE) 2016/679 in luoghi pubblici o aperti al pubblico, da parte delle autorità pubbliche o di soggetti privati, sono sospese fino all'entrata in vigore di una disciplina legislativa della materia e comunque non oltre il 31 dicembre 2023.

9 Si v. il doc-web n. 9823282 del 14 novembre 2022 https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9823282.

10. La sospensione di cui al comma 9 non si applica agli impianti di videosorveglianza che non usano i sistemi di riconoscimento facciale di cui al medesimo comma 9 e che sono conformi alla normativa vigente.
11. In caso di installazione o di utilizzazione dei sistemi di cui al comma 9, dalla data di entrata in vigore della legge di conversione del presente decreto e fino al 31 dicembre 2023, salvo che il fatto costituisca reato, si applicano le sanzioni amministrative pecuniarie stabilite dall'articolo 166, comma 1, del codice di cui al decreto legislativo 30 giugno 2003, n. 196 e dall'articolo 42, comma 1, del decreto legislativo 18 maggio 2018, n. 51, in base al rispettivo ambito di applicazione.
12. I commi 9, 10 e 11 non si applicano ai trattamenti effettuati dalle autorità competenti a fini di prevenzione e repressione dei reati o di esecuzione di sanzioni penali di cui al decreto legislativo 18 maggio 2018, n. 51, in presenza, salvo che si tratti di trattamenti effettuati dall'autorità giudiziaria nell'esercizio delle funzioni giurisdizionali nonché di quelle giudiziarie del pubblico ministero, di parere favorevole del Garante reso ai sensi dell'articolo 24, comma 1, lettera b), del medesimo decreto legislativo n. 51 del 2018.

18.4 Sorveglianza e pandemia: l'uso di sistemi di remote teaching

L'emergenza sanitaria ha richiesto riflessioni sulle esigenze di bilanciamento tra la protezione della privacy e altri diritti e libertà, cercando di rispettare i valori democratici [Comandè et al. 2020]. Durante la pandemia di Covid-19, in tutto il mondo, università di diverse dimensioni e tipologie e altri istituti scolastici sono stati costretti a passare al software e ad altri servizi digitali per l'insegnamento e per esaminare gli studenti da remoto [Pievatolo 2022]. La tecnologia della sorveglianza è stata così largamente utilizzata nel contesto pandemico all'interno di ambienti educativi per consentire la prosecuzione delle attività quando non era possibile svolgerle in presenza [Karagianni, Papakonstantinou 2022].

Con l'espressione «emergency remote teaching» si intende, quindi, la modalità di insegnamento da remoto che comprende sia i sistemi di formazione a distanza o videoconferenza che quelli di «e-proctoring», software intelligenti volti a sorvegliare gli studenti durante gli esami online per evitare copiature o assunzione di comportamenti vietati. Le soluzioni sono state per la maggior parte fornite da piattaforme private

tramite licenze [Pascault et al. 2020]. I fornitori dei servizi, in aggiunta, erano per lo più stabiliti al di fuori dello Spazio Economico Europeo, solitamente negli Stati Uniti.

Il rispetto del diritto alla protezione dei dati personali in questo contesto non è stato solo necessario per esigenze di conformità con l'ordinamento giuridico, ma anche per assicurare, tramite la corretta gestione dei dati, la libertà di istruzione, di ricerca e il benessere digitale [Angiolini et al. 2020].

Le questioni più rilevanti sollevate in materia di protezione dei dati personali dall'uso di tecnologie di *remote teaching* hanno riguardato la definizione dei ruoli, la trasparenza sulle finalità del trattamento, la presenza di un'adeguata base giuridica, l'esistenza di modalità per l'esercizio dei diritti da parte degli interessati al trattamento, e l'applicazione delle regole in materia di trasferimento transfrontaliero di dati personali.

In primo luogo, nel caso in cui l'infrastruttura fosse fornita da un terzo soggetto diverso dall'università o dall'ente scolastico, il primo era considerabile il responsabile del trattamento, mentre il secondo il titolare, determinando la finalità e avendo scelto il mezzo. I docenti e gli insegnanti non risultavano titolari, ma meri autorizzati al trattamento. Tra titolare e responsabile dovevano essere conclusi accordi dettaglianti secondo le regole dell'art. 28 del GDPR. In alcuni casi ente scolastico e piattaforma hanno tuttavia regolato i ruoli con accordi di contitolarità. In ogni caso, gli studenti potevano essere considerati gli interessati al trattamento.

Con riferimento alla finalità di trattamento, oltre a quella primaria di fornire un servizio per scopi educativi, varie informative dei servizi di *remote teaching* menzionavano ulteriori finalità di miglioramento delle funzionalità o di marketing svolte, in concreto, dai responsabili del trattamento. La prima espressione non sembrava rispettare il dovere di determinatezza e trasparenza richiesto dalla normativa per la finalità; la seconda, invece, appariva non compatibile con gli scopi propri dell'insegnamento perseguiti dai titolari (art. 5, par. 1, lett. b) GDPR). In aggiunta, quando la base giuridica prescelta era il consenso, veniva raramente fornita la possibilità di modulare l'accettazione delle funzionalità, con l'esito di dover accettare anche utilizzi ulteriori dei dati personali rispetto a quelli educativi. In generale, non veniva frequentemente specificato quale fossero le condizioni di validità per il trattamento dei dati partico-

lari, quali i dati biometrici raccolti dalle webcam dei dispositivi. Avrebbe, infatti, dovuto applicarsi il secondo paragrafo dell'art. 9 del GDPR.

Complesso risultava l'esercizio dei diritti da parte degli interessati, sia per difficoltà di accesso a tutti i dati raccolti, sia per poca trasparenza su quali pretese fossero in concreto invocabili (ad es., se si applicasse o meno il diritto alla cancellazione dell'art. 17).

Durante la pandemia, come anticipato [vedi → Capitolo 6], è stato invalidato l'accordo Privacy Shield da parte della CGUE con la sentenza Schrems II. In assenza di un'altra decisione di adeguatezza da parte della Commissione europea per il trasferimento di dati verso gli Stati Uniti è stato necessario individuare rapidamente le nuove basi giuridiche per la prosecuzione dei servizi di *remote teaching* [Angiolini et al. 2020, 58-63]. La scelta è principalmente ricaduta su clausole contrattuali tipo, con la necessità di individuare appropriate garanzie a protezione dei dati e di dover contrattare con le piattaforme quali fossero le condizioni per gestire nel modo più corretto i dati personali raccolti. Si è immediatamente notato lo sbilanciamento tra le posizioni di potere contrattuale tra i soggetti privati che fornivano i servizi e gli enti educativi.

Varie autorità di controllo hanno sanzionato trattamenti di dati eseguiti tramite sistemi di *e-proctoring* da parte delle università. Si segnalano:

- la decisione dell'autorità di controllo greca che ha riconosciuto illegittimo l'uso di Webex per varie violazioni della normativa, tra cui la mancanza di necessarie garanzie per il trasferimento di dati personali al di fuori dell'UE (decisione n. 50/2021 del 16 novembre 2021);
- il provvedimento del Garante per la protezione dei dati sul trattamento dell'Università Bocconi tramite il software Respondus (provv. N. 317 del 16 settembre 2021), le cui operazioni, tra le molte violazioni, non rispettavano i doveri di trasparenza, anche sulla logica dell'algoritmo, non prevedevano una corretta base giuridica per i dati biometrici e per la profilazione, e non rispettavano il principio di protezione della vita privata fin dalla progettazione;
- e infine la decisone dell'autorità portoghese che sempre su Respondus ha sanzionato la mancanza di adeguate garanzie per i trasferimenti di dati (Deliberação/2021/622).

I sistemi di *e-proctoring* raccoglievano dati personali tramite la webcam ed il microfono dei dispositivi ed erano in gradio di prendere decisio-

ni automatizzate. L'informativa di questi sistemi con intelligenza artificiale avrebbe sempre dovuto specificare chiaramente la logica algoritmica, come richiesto dal GDPR quando sono presenti processi automatizzati di trattamento (art. 5, par. 1, lett. a) e 13 GDPR), dal momento che l'effetto di una segnalazione o di un blocco dell'esame poteva essere significativo per gli interessati [Bincoletto 2021c].

Più in generale è possibile affermare che la scelta tra gli strumenti di remote teaching dovrebbe essere compiuta tenendo conto di ogni aspetto del trattamento dei dati, dall'esistenza di un corretto fondamento giuridico per le categorie di dati al periodo di conservazione degli stessi. L'analisi dei rischi rappresenta un utile strumento a supporto delle valutazioni. In questo settore emerge l'esigenza che il principio di data protection by design sia implementato dal titolare, ma anche dal responsabile del trattamento, quale soggetto che in concreto gestisce gli aspetti tecnologici e può modificare i sistemi.

18.5 Sorveglianza e pandemia: le applicazioni per il tracking

Fin dall'inizio della pandemia è altresì emersa la possibilità di utilizzare le tecnologie al fine della gestione del contagio. In questo contesto la sorveglianza è di tipo epidemiologico, essendo volta a gestire la diffusione di una malattia attraverso il monitoraggio capillare ed efficace dei singoli individui e dei loro contatti.

Con i termini «contact tracing» e «tracking» si intendono, in generale, vari e diversi meccanismi volti a tracciare, rispettivamente manualmente o digitalmente, gli spostamenti degli individui per identificare i precedenti contatti dei soggetti risultati sierologicamente positivi al test su un virus e così coloro che potenzialmente sono a rischio di contagio. Prima dello sviluppo dei vaccini, il tracciamento e il controllo dei contatti, e così degli spostamenti degli individui, e l'inevitabile sorveglianza ad essi collegata, risultavano le strategie più importanti ed efficaci contro il Covid-19, come indicato nel rapporto del 2020 intitolato «Sorveglianza territoriale e tutela della salute pubblica: alcuni aspetti etico-giuridici» del Gruppo di Lavoro Bioetica Covid-19 dell'Istituto Superiore di Sanità[10].

10 https://www.iss.it/rapporti-covid-19/-/asset_publisher/btw1J82wtYzH/content/

Tuttavia, sull'utilizzo di strumenti di sorveglianza per il monitoraggio del contagio è sorto un acceso dibattito sia a livello politico che accademico [Hondius et al. 2021 e Poletti 2021]. Innanzitutto, è stato sottolineato che le decisioni sui meccanismi di tracciamento, sia politiche che, successivamente, legislative, avrebbero dovuto essere il frutto di scelte adeguatamente ponderate risultando, inevitabilmente, chiari precedenti per il futuro. Era innegabile che la situazione in cui si trovavano gli stati si riferiva ad un'inaudita emergenza, ma era altrettanto comprensibile che il tracciamento e le tecnologie a suo supporto, una volta diffuse, avrebbero potuto essere utilizzate anche e successivamente per altri scopi, allora nemmeno previsti. Il tracciamento degli spostamenti avrebbe potuto *de facto* e *pro-futuro* legittimare un'attività di sorveglianza capillare e sistematica degli individui. Perciò, è stato necessario fin da subito adottare strette misure di salvaguardia per proteggere i diritti fondamentali, tra cui la riservatezza e la protezione dei dati personali, e così evitare abusi da parte delle autorità pubbliche, ma anche di soggetti privati coinvolti nello sviluppo delle soluzioni tecnologiche.

In secondo luogo, è emerso che il controllo del contagio cosiddetto manuale («contact tracing») era tradizionalmente già utilizzato per prevenire e contenere la diffusione di malattie infettive sulla base di una serie di procedure che seguivano le linee guida dell'Organizzazione Mondiale della Sanità (WHO)[11]. La principale metodologia consisteva nell'effettuazione di interviste con i soggetti risultati positivi alla malattia per avere contezza dei loro precedenti contatti e così delle persone a rischio di contagio. Tali operazioni venivano compiute dall'autorità sanitaria e richiedevano molte risorse umane e il tempo necessario a contattare i vari individui. Il controllo digitale, o «tracking», invece, poteva risultare più rapido, diffuso e meno dispendioso, ma implicava diversi e ulteriori problemi in quanto più pervasivo. Perciò, mentre il tracciamento manuale è stato immediatamente considerato «accettabile» nell'ambito di un bilanciamento che premiava la necessità di protezione dell'interesse alla salute pubblica - sempre se svolto nella cornice delle linee guida riconosciute a livello internazionale - il tracciamento digitale ha richiesto mag-

rapporto-iss-covid-19-n.-34-2020-sorveglianza-territoriale-e-tutela-della-salute-pubblica-alcuni-aspetti-etico-giuridici.-versione-del-25-maggio-2020.

11 https://www.paho.org/en/contact-tracing-knowledge-hub.

gior attenzione perché l'intensità e la portata del controllo sugli individui apparivano inevitabilmente maggiori.

Allo stesso tempo, i benefici del tracking venivano così riassunti: (i) supplire i possibili vuoti di memoria del soggetto potenzialmente contagioso sugli individui che aveva incontrato nei giorni precedenti; (ii) far emergere i vari contatti sconosciuti al soggetto potenzialmente contagioso, che potevano comunque essere a rischio; (iii) comunicare rapidamente il rischio di contagio alla rete di contatti; (iv) creare un sistema che richiedesse minori oneri organizzativi per gli stati e per le autorità sanitarie, rispetto al controllo manuale [Poletti 2021, Resta 2020 e Poletti 2020].

In aggiunta, alcuni lamentavano che la privacy e la protezione dei dati personali non avrebbero dovuto essere un freno alla tecnologia e all'innovazione e non avrebbero dovuto nemmeno impedire soluzioni a vantaggio della salute pubblica. In realtà, il contrasto tra privacy e sicurezza o privacy e salute rappresentano dicotomie in gran parte superate. Come già sottolineato in questo manuale, il diritto alla riservatezza e alla protezione dei dati personali possono essere posti in bilanciamento con altri diritti e interessi. Il diritto alla salute pubblica e il principio di solidarietà possono legittimamente rappresentare interessi da porre in bilanciamento. Ciò che però non deve essere dimenticato è che tutelare il dato personale e l'auto-determinazione dell'individuo non significa soltanto proteggere una singola informazione o aspetti della personalità, ma anche proteggere la dignità dell'interessato e per estensione dell'intera comunità.

È così emerso che il tracciamento digitale non doveva essere proibito di per sé, ma avrebbe dovuto porre al centro delle soluzioni le persone e la tutela della loro dignità, interessi esistenti nell'ordinamento giuridico tanto quanto quello individuale e collettivo alla salute, alla vita e alla sanità pubblica. La protezione della dignità è il simbolo di un paese democratico, come insegnato da Rodotà [Rodotà 2012]. Ogni limitazione alle libertà e ai diritti fondamentali deve peraltro essere giustificata e limitata in termini di tempo, spazio e contenuto. Il sistema costituzionale nazionale ed europeo e l'articolo 52 della Carta di Nizza forniscono gli strumenti per il bilanciamento dei diritti. Nel contesto del contact tracing e del tracking, rilevava, pertanto, sia la necessità di proteggere la dignità

del singolo sia quella di tutelare la salute, la vita e gli interessi del gruppo e della società.

Con riferimento alla protezione del diritto alla protezione dei dati personali e l'utilizzo di sistemi di tracking si può sottolineare quanto segue.

Il Considerando 46 del GDPR sancisce la liceità del trattamento dei dati quando mirato a tenere sotto controllo l'evoluzione di epidemie e la loro diffusione. L'articolo 23 del GDPR poi prevede la possibilità per gli Stati membri di limitare i singoli diritti dell'interessato (artt. 15-22) e gli obblighi del titolare del trattamento (artt. 24 e ss.) mediante misure legislative nazionali che rispettino «l'essenza dei diritti e delle libertà fondamentali» qualora siano necessarie e proporzionate per salvaguardare vari interessi, tra cui «importanti obiettivi di interesse pubblico generale», come la sanità pubblica e la sicurezza sociale.

Il trattamento dei dati personali in applicazioni di tracking poteva dunque essere attuato secondo la previsione dell'art. 23 perché in atto una situazione emergenziale. Propria questa ha rappresentato la base giuridica per tutte le misure legislative adottate durante l'emergenza da parte degli Stati membri dell'UE. Oltre al GDPR, ad alcune attività di trattamento di dati personali in questo contesto si doveva applicare la Direttiva *e-privacy* vista la presenza di comunicazioni elettroniche.

Il tracking è stato principalmente sviluppato tramite applicazioni mobile che, una volta installate dagli individui sui propri dispositivi, potevano raccogliere sia dati personali comuni, che dati particolari, come quelli in grado di rivelare lo stato di salute di una persona. I moderni smartphone sono dotati di sensori che possono tracciare gli spostamenti degli utenti ed i soggetti con i quali questi entrano in contatto. In generale, le applicazioni di tracking potevano monitorare i movimenti dei soggetti generando dati di prossimità in occasione di incontro grazie a sistemi di rilevamento a corto raggio e poi pseudonimizzare tali informazioni. Con alcune informazioni aggiuntive su chi fosse risultato positivo al virus, l'applicazione poteva avvisare del rischio di contagio implementando a sistemi di alert. Varie autorità hanno segnalato quali dovessero essere i principi da seguire per garantire il rispetto della disciplina in materia di protezione dei dati personali.

Di seguito un elenco di fonti ed una tabella volta ad illustrare i diversi principi ricordati, con l'indicazione della loro definizione e l'autorità o l'organismo che ne ha ribadito l'applicazione:

– Commissione Europea, Comunicazione intitolata «Orientamenti sulle app a sostegno della lotta alla pandemia di covid-19 relativamente alla protezione dei dati» del 17 aprile 2020 e «Raccomandazione (UE) 2020/518 della Commissione dell'8 aprile 2020 relativa a un pacchetto di strumenti comuni dell'Unione per l'uso della tecnologia e dei dati al fine di contrastare la crisi Covid-19 e uscirne, in particolare per quanto riguarda le applicazioni mobili e l'uso di dati anonimizzati sulla mobilità»;
– Consiglio d'Europa, «Joint Statement on Digital Contact Tracing» di Alessandra Pierucci, Chair of the Committee of Convention 108 e Jean-Philippe Walter, Data Protection Commissioner dello stesso Consiglio, del 30 marzo 2020;
– European Data Protection Board, «Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak» del 21 aprile 2020, che elenca i principi per ogni fase di attività delle applicazioni;
– Garante per la protezione dei dati personali, «Parere sulla proposta normativa per la previsione di una applicazione volta al tracciamento dei contagi da COVID-19» del 29 aprile 2020;
– Commission Nationale Informatique et des libertés, «Deliberation N°. 2020-046 of April 24, 2020 delivering an opinion on a proposed mobile application called «StopCovid»»;
– National Security Commission on Artificial Intelligence (NSCAI) degli Stati Uniti, «Privacy and Ethics Recommendations for Computing Applications Developed to Mitigate COVID-19».

Principio	**Definizione**	**Autorità**
Effettività	Il tracking doveva essere la scelta residuale rispetto ad alternative meno invasive nella sfera giuridica degli individui	CE, CoE, EDPB, Garante
Limitazione delle finalità	Il tracking doveva essere volto e limitato al controllo dell'emergenza, le finalità determinate e precise	CE, CoE, EDPB, Garante
Volontarietà	L'utilizzo dello strumento doveva essere volontario, senza meccanismi premiali per chi lo scegliesse. Volontarietà non significava necessariamente consenso come base giuridica per il trattamento dei dati	CE, CoE, EDPB, NSCAI, Garante

Differenziazione del consenso	Se previsto, il consenso doveva essere modulare per le varie operazioni compiute dalle applicazioni	CE, EDPB, Garante
Temporaneità	I dati personali raccolti dovevano essere conservati solo per il periodo necessario al controllo dell'epidemia e poi cancellati o anonimizzati	CE, CoE, EDPB, CNIL, NSCAI, Garante
Trasparenza e accessibilità	La modalità di trattamento doveva essere chiara e trasparente, il sistema comprensibile ed accessibile e il codice della tecnologia aperto	CE, CoE, EDPB, CNIL, NSCAI, Garante
Minimizzazione	Dovevano essere raccolti soltanto i dati personali strettamente necessari al conseguimento della finalità di controllo	CE, CoE, EDPB, CNIL, NSCAI, Garante
Non completa automatizzazione del trattamento	Il trattamento non poteva essere interamente automatizzato	CE, CoE, EDPB, Garante
Analisi d'impatto e privacy by design e by default	Il trattamento doveva essere valutato tramite una preventiva analisi dei rischi e l'implementazione doveva rispettare i principi di protezione fin dalla progettazione e per impostazione predefinita	CE, CoE, EDPB, CNIL, Garante
Anonimizzazione o pseudonimizzazione	I dati raccolti dovevano essere aggregati in forma anonima o pseudonimizzata per escludere o limitare la de-identificazione degli utenti	CE, CoE, EDPB, NSCAI, Garante
Sicurezza	Il tracking doveva includere sistemi di sicurezza protettivi dei dati personali, come la crittografia	CE, CoE, EDPB, CNIL, NSCAI, Garante
Geolocalizzazione	La geolocalizzazione doveva essere esclusa per i dati di prossimità, si dovevano preferire tecnologie bluetooth, meno invasive della sfera personale	CE, CoE, EDPB, Garante
Centralizzazione o decentralizzazione	I dati potevano essere archiviati in un server centrale o potevano essere decentralizzati sui dispositivi degli utenti	Centralizzazione: Cina, Francia, Germania, Istraele, Regno Unito. Decentralizzazione: Italia e Singapore
Audit	Il tracking doveva essere sottoposto a meccanismi esterni di verifica e controllo	CE, CoE, EDPB, CNIL, NSCAI, Garante

Sulla base di tali principi sono state create varie applicazioni in tutto il mondo e in particolare 28 nell'UE (ad es., «Coronalert» in Belgio, «TousAntiCovid» in Francia, «Radar Covid» in Spagna) [Poillot et al. 2021]. Tra queste, ritroviamo l'italiana «Immuni», la cui base giuridica è costituita dall'articolo 6 del d.l. 30 aprile 2020, n. 28 e dall'art. 9 co. 2 lett. (i) e (j) GDPR (sanità pubblica e finalità di ricerca).

Immuni è stata sviluppata dalla società Bending Spoons S.p.A. in open source grazie ad una task force guidata dal Ministero dell'Innovazione. L'applicazione, attiva da inizio giugno 2020 sia per ambienti IoS che Android, funzionava tramite tecnologia bluetooth-low-energy (bluetooth a bassa energia) e un sistema di trasmissione di dati su frequenze radio a corto raggio *peer-to-peer*. Perciò, non veniva utilizzato il GPS, evitando così la geolocalizzazione degli utenti.

Gli individui potevano liberamente scaricare Immuni dagli *store* dei dispositivi se con età maggiore dei 14 anni. I soggetti circolavano e con essi i propri dispositivi, i quali, se attivi e con Immuni installata, generavano dati di prossimità, poi conservati per un tempo limitato e in modalità crittografata. Si trattava di un'applicazione per la notifica di esposizione a situazione di rischio Covid-19. In particolare, l'applicazione creava codici alfanumerici in stringhe di 128 bit ogni 10 minuti a partire da una chiave giornaliera associata all'utente. Il registro del singolo operava per 14 giorni registrando i propri codici e i codici incontrati a distanza ravvicinata per un certo periodo di tempo (meno di 2 metri, per almeno 15 minuti). Dopo 14 giorni, i dati venivano cancellati. In ogni caso tutte le comunicazioni (scambi di codici) tra i dispositivi erano crittografate e rese possibili grazie ad un modello di interoperabilità e comunicabilità delle interfacce (API) messo a disposizione da Apple e Google a inizio 2020.

I codici generati rimanevano nel dispositivo dell'utente e venivano inviati al server centrale di backend solo nel momento in cui, a seguito di responso microbiologico, un utente risultava positivo. I sanitari, infatti, dopo il risultato di un tampone potevano chiedere al paziente se avesse scaricato Immuni e volesse mettere a disposizione i codici generati dal suo dispositivo nei 14 giorni precedenti. Se il soggetto avesse accettato, avrebbe potuto accedere ad una funzionalità di One Time Password (OTP) all'interno dell'applicazione e comunicare i dieci caratteri generati dal sistema al sanitario. Solo dopo questo passaggio si potevano caricare i codici riferiti al soggetto negli ultimi 14 giorni sul server centrale. In questo modo il server risultava decentralizzato. Tutte le versioni di Immuni operavano un controllo con il server in backend per verificare se avessero incontrato un codice divenuto successivamente associato ad un soggetto positivo. I contatti di quest'ultimo ricevano tramite Immuni una notifica di esposizione al rischio dal testo «il giorno X sei stato vicino a un caso Covid-19 positivo». La soglia di rischio era calcolata dall'ap-

plicazione sulla base di un algoritmo basato su modelli probabilistici. A questo punto, il soggetto allertato veniva invitato dall'applicazione a contattare il proprio medico di medicina generale. Il server centrale non poteva identificare l'utente con il codice temporaneo perché veniva rinnovato ogni 10 minuti. Il server riceva solo i codici di un utente positivo e non quelli dei suoi contatti. Il sistema di tracking, perciò, si basava sulla auto-responsabilità nel singolo a contattare il medico e sottoporsi ad un tampone. A seguito di una modifica tecnica effettuata nel 2021 gli utenti hanno potuto scegliere di caricare i propri codici nel server senza dover effettuare il passaggio con un'autorità sanitaria.

Il titolare del trattamento di dati effettuato tramite Immuni era il Ministero della Salute, che si coordinava con i soggetti operanti nel Servizio nazionale della protezione civile, i soggetti attuatori dell'ordinanza del Capo del Dipartimento della protezione civile n. 630 del 3 febbraio 2020, con l'Istituto Superiore di Sanità, con le strutture pubbliche e con le strutture private accreditate che operavano nell'ambito del Servizio sanitario nazionale. Responsabili del trattamento erano Sogei S.p.a., società pubblica, e il Ministero dell'economia e delle finanze per gestire il server di backend.

L'utilizzo di Immuni avveniva su base volontaria e si fondava sullo stesso principio anche l'eventuale attivazione della notifica di esposizione. L'utilizzo di Immuni aveva comunque una base normativa su fonte primaria e il consenso dell'interessato era necessario solo per le funzionalità tecniche relative al bluetooth. Le forze di polizia o dell'ordine, o altri soggetti esterni, non potevano utilizzare i dati di prossimità. I dati aggregati, tuttavia, se anonimizzati, potevano essere usati per finalità di sanità pubblica, profilassi, fini statistici o di ricerca scientifica. Per Immuni è stata realizzata una valutazione di impatto sottoposta ad approvazione al Garante per la protezione dei dati personali, che ne ha ribadito il rispetto dei principi di protezione della vita privata fin dalla progettazione e per impostazione predefinita[12]. Tra le misure tecniche è possibile segnalare

12 Si v. Garante per la protezione dei dati personali, "Provvedimento di autorizzazione al trattamento dei dati personali effettuato attraverso il Sistema di allerta Covid-19 - App Immuni", doc. web n. 9356568 del 1° giugno 2020 e la "Valutazione d'impatto sulla protezione dei dati personali presentata dal Ministero della Salute relativa ai trattamenti effettuati nell'ambito del sistema di allerta Covid-19 denominato Immuni", registrata tramite doc. web n. 9357972 del 3 giugno 2020.

la pseudonimizzazione (crittografia e creazione di ID randomici), la pianificazione puntuale dei tempi di conservazione e l'anonimizzazione per le finalità secondarie. Peraltro, il codice sorgente era ed è disponibile in open source con licenza aperta sul portale GitHub.

L'analisi del caso Immuni dà adito ad alcune considerazioni. La volontarietà per la sua installazione ha avuto come controindicazione un utilizzo dello strumento tecnologico non del tutto soddisfacente [Poillot et al. 2021, 75-76], ma ha lasciato all'individuo la possibilità di auto-determinarsi. A dicembre 2022 risultavano 21.922.401 download, 91.916 utenti dichiarati positivi e 196.114 notifiche di esposizione al rischio[13]. Non tutti i soggetti poi disponevano dei mezzi (telefoni compatibili) e delle capacità necessarie (sufficiente digitalizzazione) per scaricare ed utilizzare una tale applicazione. Ci si domanda perciò se ciò abbia fatto sorgere discriminazioni o disuguaglianze. Una volta ricevuto l'alert per la prossimità, ci si è chiesti se fossero stati previsti abbastanza test diagnostici per valutare la positività da Covid-19 dei contatti a rischio. Il sistema sanitario doveva inevitabilmente essere potenziato sia da un punto di vista tecnologico che organizzativo. E ciò al di là della digitalizzazione del tracciamento dei contatti. Secondo autorevole dottrina, anche altri fattori hanno contribuito a risultati non brillanti dell'applicazione: la mancanza di una strategia di comunicazione coerente, persuasiva ed efficace da parte del Governo; il lancio dell'applicazione in un momento in cui era superato il picco della prima ondata dei contagi; l'esistenza di altre applicazioni a livello regionale; l'invecchiamento della popolazione e le competenze digitali insufficienti; la non ottimale integrazione con gli interventi di assistenza sanitaria e il ritardo nella prenotazione dei tamponi [Poillot et al. 2021, 75 e Poletti 2021].

Dal 31 dicembre 2022 Immuni non è più attiva ed è stata eliminata dagli store. Il problema della sorveglianza di tipo epidemiologico tramite gli strumenti di tracking non può essere risolto da risposte nette («app sì» o «app no») ma con un approccio possibilista e critico, volto a trovare una soluzione di compromesso e bilanciamento, implementando nella tecnologia i principi e le regole «by design».

13 Si v. i dati sempre aggiornati nel sito ufficiale in https://www.immuni.italia.it/dashboard.html.

18.5 Casi 18-1, 18-2, 18-3

Caso 18-1

Il sindaco del Comune Alfa propone al suo Consiglio di installare delle videocamere «intelligenti» nella piazza principale per esigenze di sicurezza urbana, che consentano il riconoscimento facciale. Vista la perplessità di alcuni assessori, il sindaco di rivolge al DPO dell'ente per avere delle delucidazioni sulla legittimità di tale installazione.
Quale sarà la base legittima del trattamento?
Quali obblighi per il titolare del trattamento?
Quali gli ulteriori requisiti necessari a rendere lecito tale trattamento di dati personali?

Caso 18-2

La libreria Beta vuole proteggere la vetrata dopo aver subito atti di vandalismo e decide di installare delle telecamere dirette ad entrambe le direzioni della strada, sia verso l'accesso che il parcheggio delle automobili, condiviso con altri esercizi commerciali e una telecamera all'interno.
Tale trattamento è legittimo?
Quale sarà la base legittima del trattamento?
Quali obblighi per il titolare del trattamento?
Quali gli ulteriori requisiti necessari a rendere lecito tale trattamento di dati personali?
Il proprietario del locale adiacente e i lavoratori della libreria possono lamentare alcunché?

Caso 18-3

L'università italiana Gamma utilizza il sistema di *e-proctoring* intelligente X della società Zeta in grado di bloccare lo schermo degli studenti durante un esame scritto. In tale modo gli studenti non hanno la possibilità di navigare su Internet per cercare le risposte al compito. La società Zeta ha sede legale negli Stati Uniti, ma fornisce servizi in tutto il mondo. Il sistema raccoglie dati biometrici e dati personali comuni degli studenti. In particolare, il sistema scatta fotografie in modo randomico e registra un video dell'esame. Se il software rileva un'attività o un movimento sospetto segnala l'evento con una bandierina gialla. Le registrazioni sono poi rese disponibili al docente previo l'utilizzo di apposite credenziali.
Tale trattamento è legittimo?
Quale sarà la base legittima del trattamento?
Quali obblighi per il titolare del trattamento?
Quali gli ulteriori requisiti necessari a rendere lecito tale trattamento di dati personali?

Conclusioni

Privacy e protezione dei dati personali rappresentano materie che hanno gradualmente guadagnato attenzione ed interesse. Da istituti giuridici di (relativa) nicchia approfonditi da pochi, essi sono divenuti argomento centrale per governare i dinamici fenomeni e processi che riguardano la nostra società.

La privacy, nella sua accezione più ampia, rappresenta un diritto fondamentale per l'esercizio di molti altri diritti nella vita «reale», ma soprattutto in quella digitale. Essa tutela l'individuo in tutte le sue dimensioni; ne protegge anzitutto la dignità che permette ad un uomo di essere tale nei vari contesti dove opera.

Questi temi sono oramai centrali nella preparazione di un giurista. Corsi che trattano il diritto della privacy e della protezione dei dati personali sono via via stati attivati nelle varie università italiane. Si potrebbe, anche, ritenere che un insegnamento su queste materie si debba considerare essenziale per la preparazione di base e, quindi, assurgere a rango di corso «fondamentale».

La protezione dei dati personali è, poi, sempre più spesso volano di opportunità professionali, altre rispetto alle tradizionali figure giuridiche: responsabile della protezione dei dati, giurista d'impresa, consulente su temi di diritto e tecnologia, collaboratore in gruppi di lavoro interdisciplinare volti allo sviluppo di piattaforme informatiche, ecc.

Questo libro vorrebbe rappresentare un contributo alla formazione di giovani giuristi. Uno strumento che li aiuti ad apprendere i rudimenti della «navigazione», fuori e dentro la Rete, nella privacy. È sicuramente un punto di partenza per più attenti ed approfonditi studi sui temi che qui vengono giocoforza solo tratteggiati. Permette, però, di avere una visione d'insieme dei vari fenomeni in atto da una prospettiva comparata ed interdisciplinare, probabilmente unico vero approccio affidante per governare scenari caratterizzati dalle istanze di protezione dei dati personali.

Siamo consapevoli che il rapporto tra diritto e tecnologia è travagliato, essendo il primo obbligato ad inseguire le novità e gli sviluppi del secondo. Alcuni capitoli di questo libro, pertanto, sono condannati ad una inesorabile obsolescenza. Se questo progetto incontrerà il favore del

pubblico a cui è rivolto, le prossime edizioni imporranno modifiche e costanti aggiornamenti.

Il giurista deve continuare ad essere in grado di gestire fenomeni complessi, bilanciare interessi anche molto diversi tra di loro, costruire ponti tra i saperi, risolvere problemi. Speriamo con questo libro di aver incoraggiato in qualche modo lo sviluppo della curiosità e dello spirito critico che dovrebbero caratterizzare l'insegnamento universitario e favorire la formazione delle prossime generazioni di giuristi.

Paolo Guarda
Giorgia Bincoletto

Bibliografia

Aggarwal S., Chaudhary R., Sing Aujla G., Kumar N., Choo K.K.R., Zomaya A.Y. [2019], *Blockchain for Smart Communities: Applications, Challenges and Opportunities*, in *Journal of Network and Computer Applications*, Vol. 144, n. 15, 13-18

Ajunwa I. [2017], *Limitless Workplace Suirveillance*, in *California Law Review*, vol. 105, n. 3, 735-776

Alpa G., Resta G. [2019], *Le persone fisiche e i diritti della personalità*, 2 ed., Milano, Utet Giuridica

Alvino I. [2021], *Commento al Titolo VIII Trattamenti nell'ambito dei rapporti di lavoro. Artt. 111, 111-bis, 112, 113 del Codice Privacy*, in R. D'Orazio, G. Finocchiaro, O. Pollicino, G. Resta (a cura di) [2021], *Codice della privacy e data protection*, Milano, Giuffrè Francis Lefebvre, 1381-1393

Anelli F., Granelli C., Schlesinger P., Torrente A. [2019], *Manuale di diritto privato*, Milano, Giuffrè

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

Antani R. [2015], *The Resistance of Memory: Could the European Union's Right to Be Forgotten Exist in the United States?*, in *Berkeley Technology Law Journal*, Vol. 30, 1173-1210

Arisi M., Guarda P. [2020], *Blockchain and eHealth: seeking compliance with the General Data Protection Regulation*, in *Biolaw journal - Rivista di Biodiritto*, n. 2, 477-496, https://teseo.unitn.it/biolaw/article/view/1559

Ashton K. [2009], *That "Internet of Things" Thing*, in *RFID Journal*, 22 giugno 2009, http://www.itrco.jp/libraries/RFIDjournal-That%20Internet%20of%20Things%20Thing.pdf

Baran P. [1964], *On distributed communications: I. Introduction to distributed communication networks*, Rand Corp Santa Monica Calif., https://www.rand.org/content/dam/rand/pubs/research_memoranda/2006/RM3420.pdf

Barbas S. [2012], *The Sidis Case and the Origins of Modern Privacy Law*, in *Columbia Journal of Law & the Arts*, Vol. 36, No. 1, Fall 2012, SUNY Buffalo Legal Studies Research Paper No. 2013-011, https://ssrn.com/abstract=2151880

Barfield W., Pagallo U. [2020], *Advanced introduction to Law and Artificial Intelligence*, Cheltenham-Northhampton, Elgar Publishing

Bauman Z., Lyon D. [2012], *Liquid Surveillance: a Conversation*, Cambridge, Polity Press

Bentham J. [1983], *Panopticon, ovvero la casa d'ispezione*, Padova, Marsilio

Bholasing J. [2022], *How technological Advances in the Big Data Era Make it Impossible to Define the 'Personal' in GDPR's 'Personal Data'*, in *European Data Protection Law Review*, Vol. 8, n. 3, 346-361

Bignami F., Resta G. [2015], *Transatlantic privacy regulation: Conflict and cooperation*, in *Law and Contemporary Problems*, Vol. 78, n. 4, 231-266.

Bincoletto G. [2019], *La privacy by design. Un'analisi comparata nell'era digitale*, Ariccia, Aracne editrice

Bincoletto G. [2020], *European Union – EDPB Guidelines 4/2019 on Data Protection by Design and by Default*, in *European Data Protection Law Review*, Vol. 6, n. 4, 574-579

Bincoletto G. [2021a], *Data protection by design in the e-health care sector. Theoretical and applied perspectives*, Luxembourg Legal Studies, Baden-Baden, Nomos Verlagsgesellschaft mbH & Co. KG

Bincoletto G. [2021b], mHealth app *per la televisita e il telemonitoraggio. Le nuove frontiere della telemedicina tra disciplina sui dispositivi medici e protezione dei dati personali*, in *BioLaw Journal - Rivista di BioDiritto*, n. 4, https://doi.org/10.15168/2284-4503-2054 , 381-407

Bincoletto G. [2021c], *E-Proctoring During Students' Exams: Emergency Remote Teaching at Stake*, in *European Data Protection Law Review*, Vol. 7, n. 4, 586-591

Bincoletto G., Guarda P. [2021], *A proactive GDPR-compliant solution for fostering medical scientific research as a secondary use of personal health data*, in *Opinio Iuris in Comparatione*, n. 1, 43-76

Bolognini L., Pellino E. [2019], *Codice della disciplina privacy*, Milano, Giuffrè Francis Lefebvre

Bomprezzi C. [2019], *I trattamenti in ambito giudiziario, difesa e sicurezza dello stato*, in G. Finocchiaro (a cura di) [2019], *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna, Zanichelli, 295-317

Bomprezzi C. [2021], *Implications of Blockchain-Based Smart Contracts on Contract Law*, Baden-Baden, Nomos

Bomprezzi C., Gambino A.M. [2019], *Blockchain e protezione dei dati personali*, in *Dir. informazione e informatica*, n. 3, 619-646

Bonzagni G. [2019], *Le comunicazioni elettroniche*, in G. Finocchiaro (a cura di) [2019], *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna, Zanichelli, 972-996

Borgman C.L. [2015], *Big Data, Little Data, No Data*, Cambridge, MIT Press

Botrugno C. [2014] *La diffusione dei modelli di cura a distanza: verso un diritto alla telesalute*, in *BioLaw Journal – Riv. di BioDiritto*, n. 1, 161-177

Brock C. [2015], *Where we're going, we don't need drivers: the legal issues and liability implications of automated vehicle technology*, in *Umkc L. Rev*., Vol. 83, 770-773

Burdon M. [2020], *Digital Data Collection and Information Privacy Law*, Cambridge, Cambridge University Press

Burrell J., *How the Machine "Thinks": Understanding Opacity in Machine Learning Algorithms*, in *Big Data & Soc'Y*, 2016, vol. 3, 1-5

Buterin V. [2015], *On public and private blockchains,* https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/

Bygrave L.A. [2014], *Data Privacy Law, an International Perspective*, Oxford, Oxford University Press

Bygrave L.A. [2020a], *Article 22. Automated individual decision-making including profiling*, in C. Kuner, L.A. Bygrave, C. Docksey, L. Drechsler (a cura di) [2020], *The EU General Data Protection Regulation: a Commentary*, Oxford, Oxford University Press, 522-542

Bygrave L.A. [2020b], *Article 25. Data protection by design and by default*, in C. Kuner, L.A. Bygrave, C. Docksey, L. Drechsler (a cura di) [2020], *The EU General Data Protection Regulation: a Commentary*, Oxford, Oxford University Press, 571-581

Bygrave L.A., Tosoni L. [2020], *Article 4(2). Personal data*, in C. Kuner, L.A. Bygrave, C. Docksey, L. Drechsler (a cura di) [2020], *The EU General Data Protection Regulation: a Commentary*, Oxford, Oxford University Press, 103-115

Bygrave, L. A. [2017], *Hardwiring privacy*, in E. Scotford, K. Yeung (a cura di) [2017], *The Oxford Handbook of the Law and Regulation of Technology*, Oxford, Oxford University Press, 754-775

Calisai F. [2019], *I diritti dell'interessato*, in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di) [2019], *I dati personali nel diritto europeo*, Torino, Giappichelli, 327-351

Caso R. [2008] *Digital Rights Management. Il commercio delle informazioni digitali tra contratto e diritto d'autore*, Padova, Cedam

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

Casonato C., Tomasi M. [2019], *Diritti e ricerca biomedica: una proposta verso nuove conoscenze*, in *BioLaw Journal – Rivista di BioDiritto*, n. 1, 343-358

Cavallaro M.C., Smorto G. [2019], *Decisione pubblica e responsabilità dell'amministrazione nella società dell'algoritmo*, in *Federalismi.it*, 4 settembre, www.federalismi.it

Cavoukian, A. [2010], *Privacy by design: the definitive workshop. A foreword by Ann Cavoukian, Ph. D*, in *Identity in the Information Society*, Vol. 3, n. 2, 247-251

Cavoukian, A. [2012], *Operationalizing privacy by design: A guide to implementing strong privacy practices*, Information and privacy commissioner of Ontario, Canada, https://gpsbydesigncentre.com/wp-content/uploads/2021/08/Doc-5-Operationalizing-pbd-guide.pdf

Cendon P. (a cura di) [2008], *Famiglia e Persone*, Milano, Utet Giuridica

Chander A., Kaminski M. E., McGeveran W. [2021], *Catalyzing Privacy Law*, in *Minn. L. Rev.*, Vol. 105, 1733-1802

Chang H. [2018], *Is Distributed Ledger Technology Built for Personal Data?*, University of Hong Kong Faculty of Law Research Paper No. 16, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3137606

Charnetski W. A., Flaherty P., Robinson J. [2001], *The Personal Information Protection and Electronic Documents Act. A Comprehensive Guide*, Canada Law Book

Chiara P. G. [2022], *The Balance Between Security, Privacy and Data Protection in IoT Data Sharing: A Critical to Traditional "Security&Privacy" Surveys*, in *European Data Protection Law Review*, n. 1, 18-30

Chung J., Zink A. [2018], *Hey Watson—can I sue you for malpractice? Examining the liability of artificial intelligence in medicine*, in *Asia Pac J Health Law Ethics*, Vol. 11, n. 2, 51-80

Ciucciovino S. [2021], *Commento all'art. 88. Trattamento dei dati nell'ambito dei rapporti di lavoro*, in R. D'Orazio, G. Finocchiaro, O. Pollicino, G. Resta (a cura di) [2021], *Codice della privacy e data protection*, Milano, Giuffrè Francis Lefebvre, 947-956

Comandè G. (a cura di) [2022], *Elgar Encyclopedia of Law and Data Science*, Cheltenham, Edward Elgar Publishing

Comandè G., Amram D., Malgieri G. [2020], *The democracy of emergency at the time of the coronavirus: the virtues of privacy*, in *Opinio Iuris in Comparatione*, n. 1, 1-7

Comandè G., Malgieri G. (a cura di) [2018], *Guida al trattamento ed alla sicurezza dei dati personali. Le opportunità e le sfide del Regolamento UE e del codice italiano riformato*, Gruppo24ore, Milano

Cooley T. M. [1888], *Law of Torts*, Callaghan & Company

Courcelas L., Lyons T., Timsit K. [2019], *Blockchain and the GDPR*, Thematic Report of the European Union Blockchain Observatory and Forum, 2018, https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf

Cowie M.R. et al. [2016], *e-Health: a position statement of the European Society of Cardiology*, in *European Heart Journal*, Vol. 37, n.1, 63–66

Cuffaro V., D'Orazio R., Ricciuto V. (a cura di) [2019], *I dati personali nel diritto europeo*, Giappichelli, Torino

Custers B., Dechesne F., Sears A. M., Tani T., van der Hof S. [2017], *A Comparison of Data Protection Legislation and Policies Across the EU*, in *Computer Law & Security Review* e disponibile su SSRN: https://ssrn.com/abstract=3091040

Custers B., Sears A. M., Dechesne F., Georgieva I., Tani T., van der Hof, S. [2019], *EU Personal Data Protection in Policy and Practice*, vol. 29, The Hague, T.M.C. Asser Press

D'Acquisto, G., Naldi, M. [2017], *Big Data e privacy by design. Anonimizzazione Pseudonimizzazione Sicurezza*, Torino, Giappichelli Editore

D'Agata C. [2018], *L'Autorità Garante e la circolazione dei dati personali dentro e fuori l'UE*, in G. Comandè, G. Malgieri (a cura di) [2018], *Guida al trattamento*

ed alla sicurezza dei dati personali. Le opportunità e le sfide del Regolamento UE e del codice italiano riformato, Gruppo24ore, Milano, 127-146

D'Orazio R., Finocchiaro G., Pollicino O., Resta G. (a cura di) [2021], *Codice della privacy e data protection*, Milano, Giuffrè Francis Lefebvre

Dannemann G. [2019], *Comparative law: study of similarities or differences?*, in M. Reinmann, R. Zimmermann (a cura di) [2019], *The Oxford Handbook of Comparative Law*, Oxford, Oxford University Press, II ed., 391-422

Davidson S., De Filippi P., Potts J. [2018], *Blockchain and the economic institutions of Capitalism,* in *Journal of Institutional Economics*, Vol. 4, n. 14, 642-643

Davis, J., Nathan L. P [2015], *Value sensitive design: Applications, adaptations, and critiques*, in J. van den Hoven, P. E. Vermaas, I. van de Poel (a cura di) [2015], *Handbook of Ethics, Values, and Technological Design: Sources, Theory, Values and Application Domains*, Dordrecht, Springer, 11-40

De Cupis A. [1952], *La verità nel diritto (Osservazioni in margine a un libro recente)*, in *Foro it*., IV, 223-224

De Cupis A. [1954], *Il diritto alla riservatezza esiste*, in *Foro it*., IV, 89-98

De Filippi P., Wright A. [2018], *Blockchain and the Law: the rule of code,* Cambridge, Massachusetts

De Mauro A., M. Greco, M. Grimaldi [2016], *A formal definition of Big Data based on its essential features*, in *Library Review*, vol. 65, n. 3, 122-135

De Terwangne C. [2020], *Article 5. Principles relating to processing of personal data*, in C. Kuner, L.A. Bygrave, C. Docksey, L. Drechsler (a cura di) [2020], *The EU General Data Protection Regulation: a Commentary*, Oxford, Oxford University Press, 309-320

Determann L, Sprague R. [2011], *Intrusive Monitoring: Employee Privacy Expectations Are Reasonable in Europe, Destroyed in the United States*, in *Berkeley Tech. L.J.*, Vol. 26, 979-1036

Determann L. [2018], *New California Law against Data Sharing*, in *The Computer & Internet Lawyer*, Vol. 35, 1-10

DeVries W. [2003], *Protecting Privacy in the Digital Age*, in *Berkeley Technology Law Journal*, Vol. 18, n. 1, 283-311

Di Federico G., Negri S. [2020], *Unione Europea e salute*, Milano, Cedam

Ducato R. [2020a], *Data protection, scientific research and the role of information*, in *Computer Law and Security Review*, 2020, Vol. 37, https://www.sciencedirect.com/science/article/pii/S0267364920300170, 1-16

Dumortier J., Verhenneman G. [2013], *Legal regulation of electronic health records: a comparative analysis of Europe and the US*, in G. Carlisle, D. Whitehouse, P. Duquenoy (a cura di) [2013], *eHealth: Legal, Ethical and Governance Challenges*, Heidelberg, Springer, 25-56

Durante M. [2019], *Potere computazionale. L'impatto delle ICT su diritto, società, sapere*, Sesto San Giovanni, Meltemi Editore

Edwards L., Veale M. [2017], *Slave to the algorithm? Why a 'right to explanation' is probably not the remedy you are looking for*, in *Duke L. & Tech. R.*, Vol. 16, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2972855

Errani G. [2019], *Il trattamento di dati relativi a condanne penali e reati*, in G. Finocchiaro (a cura di) [2019], *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna, Zanichelli, 275-294

Errani G. [2021], *Commento art. 2 octies Codice Privacy*, in R. D'Orazio, G. Finocchiaro, O. Pollicino, G. Resta (a cura di) [2021], *Codice della privacy e data protection*, Giuffré, Milano, 1062-1078

Esposito M. S. [2021], *Commento art. 32 GDPR*, in R. D'Orazio, G. Finocchiaro, O. Pollicino, G. Resta (a cura di) [2021], *Codice della privacy e data protection*, Giuffré, Milano, 502-514

Faini F. [2019], *Data society*. *Governo dei dati e tutela dei diritti nell'era digitale*, Giuffrè Francis Lefebvre

Falce V. [2021], *Commento art. 20 GDPR*, in R. D'Orazio, G. Finocchiaro, O. Pollicino, G. Resta (a cura di) [2021], *Codice della privacy e data protection*, Giuffré, Milano, 348-366

Famiglietti G. [2005], *Il diritto alla riservatezza o la riservatezza come diritto. Appunti in tema di riservatezza ed intimità sulla scorta della giurisprudenza della Corte costituzionale e del Tribunal Constitucional*, in A. D'Aloia (a cura di) [2005], *Biotecnologie e valori costituzionali. Il contributo della giustizia costituzionale*, Torino, Giappichelli, 299-324

Ferrara Santamaria M. [1937], *Il diritto dell'illesa intimità privata*, in *Riv. dir. priv.*, n. 1, 168-191

Finck M. [2019a], *Blockchain regulation and governance in Europe*, Cambridge, Cambridge University Press

Finck M. [2019b], *Smart Contracts as a Form of Solely Automated Processing under the GDPR*, Max Planck Institute for Innovation and Competition Research Paper No. 01, 2019, n. 9, disponibile in https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3311370

Finck M., Pallas F. [2020], *They who must not be identified - distinguishing personal from non-personal data under the GDPR*, in *Int. Data Priv. Law*, Vol. 10, n. 1, 11–36

Finocchiaro G. [2012], *Privacy e protezione dei dati personali. Disciplina e strumenti operativi*, Bologna, Zanichelli

Finocchiaro G. [2019], *Il quadro d'insieme sul regolamento europeo sulla protezione dei dati personali*, in G. Finocchiaro (a cura di) [2019], *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna, Zanichelli, 1-26

Finocchiaro G. [2021], *Commento art. 17 GDPR*, R. D'Orazio, G. Finocchiaro, O. Pollicino, G. Resta (a cura di) [2021], *Codice della privacy e data protection*, Giuffré, Milano, 327-335

Fischer G., Grechenig T., Niemeier P., Schmelz D., Zhu L. [2018], *Towards Using Public Blockchain in Information-Centric Networks: Challenges Imposed by the European Union's General Data Protection Regulation*, Proceedings of the 1st IEEE International Conference on Hot Information-Centric Networking, http://hdl.handle.net/20.500.12708/57739, 223-228

Floridi L. [2012], *La rivoluzione dell'informazione*, trad. it., Torino, Codice

Floridi L. (a cura di) [2015], *The onlife Manifesto. Behind Human in a Hyperconnected Era*, Berlino, Springer

Floridi L. [2017], *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, trad. di M. Durante, Milano, Raffaello Cortina Editore

Floridi L. [2020], *What the Near Future of Artificial Intelligence Could Be*, in C. Burr, S. Milano (a cura di), *The 2019 Yearbook of the Digital Ethics Lab. Digital Ethics Lab Yearbook*, Cham, Springer

Foglia C. [2019], *Il dilemma (ancora aperto) dell'anonimizzazione e il ruolo della pseudonimizzazione nel GDPR*, in R. Panetta (a cura di) [2019], *Circolazione e protezione dei dati personali tra libertà e regole del mercato*, Milano, Giuffrè Francis Lefebvre, 309-332

Foglia M. [2020], *Patients and Privacy: GDPR Compliance for Healthcare Organizations*, in *European Journal of Privacy Law & Technologies*, Special issue 2020, 43-50

Foucault M. [1975], *Surveiller et punir: naissance de la prison*, Parigi, Gallimard

Frosini V. [1984], *Diritto alla riservatezza e calcolatori elettronici*, in G. Alpa, M. Bessone (a cura di) [1984], *Banche dati, telematica e diritti della persona*, Padova, Cedam, 29-43

Galgano F. (a cura di) [1988], *Commentario del Codice Civile Scialoja-Branca*, *Libro Primo - Della persona e della famiglia*, *Delle persone fisiche*, Bologna, Nicola Zanichelli Editore

Giampiccolo G. [1958], *La tutela della persona umana e il c.d. diritto alla riservatezza*, in *Riv. trim. dir. e proc. civ*., 458-475

Giannantonio E., Losano M. G., Zeno-Zencovich V. [1997], *La tutela dei dati personali. Commentario alla Legge 675/1996*, Padova, Cedam

Giovanella F. [2013], *Enforcement del diritto d'autore nell'ambito di Internet vs. protezione dei dati personali: bilanciamento tra diritti fondamentali e contesto culturale*, in *Riv. critica dir. privato*, n. 4, 637-664

Giovanella F. [2017], *Copyright and Information Privacy. Conflicting Rights in Balance*, Cheltenham, Edward Elgar

Giovanella F. [2019]*, Le persone e le cose: la tutela dei dati personali nell'ambito dell'*Internet of Things, in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di) [2019], *I dati personali nel diritto europeo*, Bologna, Giappichelli, 1213-1242

Giovanella F. [2022], *From the "right to delisting" to the "right to relisting"*, in *Media Laws*, n. 2, 1-22

Granieri M. [2017], *Il trattamento di categorie particolari di dati personali nel Reg. UE 2016/679*, in *Nuove leggi civ. comm.*, n. 1, 165-190

Graziadei M. [2021], *Commento art. 2 GDPR*, in R. D'Orazio, G. Finocchiaro, O. Pollicino, G. Resta (a cura di) [2021], *Codice della privacy e data protection*, Giuffré, Milano, 129-143

Groos D., van Veen E. [2020], *Anonymised Data and the Rule of Law*, in *European Data Protection Law Review*, Vol. 6, n. 4, 498-508

Guarda P. [2004], *Agenti software e sicurezza informatica*, in Pascuzzi G. (a cura di) [2004], *Diritto e tecnologie evolute del commercio elettronico*, Padova, Cedam, 315-342

Guarda P. [2011], *Fascicolo sanitario elettronico e protezione dei dati personali*, Trento, Quaderni del Dipartimento di Scienze Giuridiche, anche in http://eprints.biblio.unitn.it/archive/00002212/

Guarda P. [2019a], *'Ok Google, Am I Sick?': Artificial Intelligence, e-Health, and Data Protection Regulation*, in *Biolaw Journal – Rivista di Biodiritto*, n. 1, 359-375

Guarda P. [2019b], *I dati sanitari*, in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di) [2109], *I dati personali nel diritto europeo*, Giappichelli, Torino, 591-626

Guarda P. [2021], *Il regime giuridico dei dati della ricerca scientifica*, Napoli, Editoriale Scientifica

Guarda P., Ducato R. [2014], *Profili giuridici dei Personal Health Records: l'autogestione dei dati sanitari da parte del paziente tra privacy e tutela della salute*, in *Riv. crit. dir. priv.*, n. 3, 389-419

Guarda P., Petrucci L. [2020], *Quando l'intelligenza artificiale parla: assistenti vocali e sanità digitale alla luce del nuovo regolamento generale in materia di protezione dei dati*, in *Biolaw Journal – Rivista di Biodiritto*, n. 2, 425-446

Harari Y.N. [2014], *Sapiens. Da animali a dei. Breve storia dell'umanità*, Milano, Bompiani

Harari Y.N. [2017], *Homo deus. Breve storia del futuro*, Firenze-Milano, Giunti-Bompiani

Hartzog W. [2018], *Privacy blueprint: the battle to control the design of new technologies*, Harvard, Harvard University Press

Hintze M. [2019], *Science and Privacy: Data Privacy Laws and their Impact on Research*, in *Wash. J. L. Tech. & Arts*, Vol. 14, 103-137

Hoffman S., Podgurski A. [2013], *Big Bad Data: Law, Public Health, and Biomedical Databases*, in *J Law Med Ethics*, Vol. 41, Suppl. 1, 56-60

Hondius E., Santos Silva M., Nicolussi A., Coderch P. S., Wendehorst C., Zoll F. (a cura di) [2021], *Coronavirus and the Law in Europe*, Cambridge, Intersentia

Iakovidis I. [1998], *Towards personal health record: current situation, obstacles and trends in implementation of electronic healthcare record in Europe*, in *International journal of medical informatics*, Vol. 52, n. 3, 105-115

Iaselli M. [2019], *Sanzioni e responsabilità in ambito GDPR*, Milano, Giuffrè Francis Lefebvre

Ibánez L.D, O'Hara K., Simperl E. [2018], *On Blockchains and the General Data Protection Regulation*, https://eprints.soton.ac.uk/422879/1/BLockchains_GDPR_4.pdf

Irti N., Severino E. [2000], *Le domande del giurista e le risposte del filosofo (un dialogo su diritto e tecnica)*, in *Contratto e impr*., n. 2, 665-679

Izzo U. [2000], *Medicina e diritto nell'era digitale: i problemi giuridici della cibermedicina*, in *Danno e resp*., 807-818

Jasmontaite L., Kamara I., Zanfir-Fortuna G., Leucci S. [2018], *Data protection by design and by default: Framing guiding principles into legal obligations in the GDPR*, in *European Data Protection Law Review*, n. 4, 168-189

Karagianni A., Papakonstantinou V. [2022], *Surveillance in Schools Across Europe: A New Phenomenon in Light of the COVID-19 Pandemic? The Cases of Greece and France*, in *European Journal of Educational Research*, Vol. 11, n. 2, 1219-1229

Klitou D. [2014], *Privacy-invading technologies and privacy by design. Safeguarding Privacy, Liberty and Security in the 21st Century*, The Hague, Springer

Kotschy W. [2020], *Article 6. Lawfulness of processing*, in C. Kuner, L.A. Bygrave, C. Docksey, L. Drechsler (a cura di) [2020], *The EU General Data Protection Regulation: a Commentary*, Oxford, Oxford University Press, 321-344

Kranenborg H. [2020], *Article 17. Right to erasure ('right to be forgotten')*, in C. Kuner, L.A. Bygrave, C. Docksey, L. Drechsler (a cura di) [2020], *The EU General Data Protection Regulation: a Commentary*, Oxford, Oxford University Press, 475-484

Kulhari S. [2018], *Building-Blocks of a Data Protection Revolution: The Uneasy Case for Blockchain Technology to Secure Privacy and Identity*, https://www.jstor.org/stable/j.ctv941qz6

Kuner C. [2007], *European Data Protection Law*, Oxford, Oxford University Press

Kuner C., Bygrave L. A., Docksey C., Drechsler L. (a cura di) [2020], *The EU General Data Protection Regulation: a Commentary*, Oxford, Oxford University Press

Kuner C., Cate F. H., Svantesson D. J. B., Lynskey O., Millard C. [2017], *Machine learning with personal data: is data protection law smart enough to meet the challenge?*, in *International Data Privacy Law*, vol. 7, n. 1, 1-2

Lachaud E. [2016], *Could the CE Marking Be Relevant to Enforce Privacy by Design in the Internet of Things?*, in S. Gutwirth, S. Leenes, P. De Heert (a cura di) [2016], *Data Protection on the Move*, Berlino, Springer, 135-162

Legg S., Hutter M. [2007], *A Collection of Definitions of Intelligence (Technical report)*, IDSIA, *arXiv:0706.3639*

Leonelli S. [2018], *La ricerca scientifica nell'era dei big data*, Sesto San Giovanni, Meltemi

Lessig L. [1999], *Code and Other Laws of Cyberspace*, New York, Basic Books

Levy S. [1993], *Crypto Rebels*, in *Wired*, Issue 2, https://www.wired.com/1993/02/crypto-rebels/

Lynksey O. [2015a], *Article 84. Penalties*, in C. Kuner, L.A. Bygrave, C. Docksey, L. Drechsler (a cura di) [2020], *The EU General Data Protection Regulation: a Commentary*, Oxford, Oxford University Press, 1194-1201

Lynksey O. [2015b], *The Foundation of EU Data Protection Law*, Oxford, Oxford University Press

Malgieri G., Comandè G. [2017], *Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation*, in *International Data Privacy Law*, Vol. 7, n. 4, 243-265

Malgieri G., Pasquale F. A. [2022], *From Transparency to Justification: Toward Ex Ante Accountability for AI*, Brooklyn Law School, Legal Studies Paper No. 712, Brussels Privacy Hub Working Paper, n. 33, disponibile in https://ssrn.com/abstract=4099657

Manes V., Mazzacuva F. [2021], *Commento al Capo II Illeciti penali*, in R. D'Orazio, G. Finocchiaro, O. Pollicino, G. Resta (a cura di) [2021], *Codice della privacy e data protection*, Giuffré, Milano, 1667-1684

Manis M.L. [2017], *The processing of personal data in the context of scientific research. The new regime under the EU-GDPR*, in *BioLaw Journal – Rivista di BioDiritto*, 2017, n. 3, 325-354

Mantelero A. [2017], *Regulating Big Data. The guidelines of the Council of Europe in the Context of the European Data Protection Framework*, in *Computer Law & Sec. Rev*., Vol. 33, n. 5, 584-602.

Mantelero A. [2019], *La privacy all'epoca dei* Big Data, in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di) [2019], *I dati personali nel diritto europeo*, Bologna, Zanichelli, 1181-1212

Mantelero A. [2020], *The future of data protection: Gold standard vs. global standard*, in *Computer Law & Sec. Rep*., Vol. 40, 1-5

Maresca A. [2021], *Commento agli artt. 114 e 115 Codice privacy*, in R. D'Orazio, G. Finocchiaro, O. Pollicino, G. Resta (a cura di) [2021], *Codice della privacy e data protection*, Milano, Giuffrè Francis Lefebvre, 1393-1409

Martinelli S., Perri P., Ziccardi G. [2017], *Diritto all'oblio e motori di ricerca*, Milano, Giuffrè Editore

Martinico G. [2021], *Commento all'art. 7 Carta dei diritti fondamentali dell'Unione Europea*, in R. D'orazio, G. Finocchiaro, O. Pollicino, G. Resta (a cura di) [2021], *Codice della privacy e data protection*, Milano, Giuffrè Francis Lefebvre, 17-35

Mascia A. [2008], *Diritti della personalità*, in P. Cendon (a cura di) [2008], *Famiglia e Persone*, Milano, Utet Giuridica, 77-280

Mittelstadt B., Allo P., Taddeo M., Wachter S., Floridi L. [2016], *The Ethics of Algorithms: Mapping the Debate*, in *Big Data & Society*, Vol. 3, n. 2, https://journals.sagepub.com/doi/full/10.1177/2053951716679679)

Moerel L. [2018], *Blockchain and Data Protection ... and Why They Are Not on a Collision Course*, in *European Review of Private Law*, Vol. 26, n. 6, 840-842

Monateri P. G. [2014], *Methods of Comparative Law*, Cheltenham, Edward Elgar

Mulder T. [2019], *Health apps, their privacy policies and the GDPR*, in *European Journal of Law and Technology*, Vol. 10, n. 1, disponibile in https://ssrn.com/abstract=3506805

Nakamoto S. [2009], *Bitcoin: A Peer-to-Peer Electronic Cash System*, https://bitcoin.org/bitcoin.pdf

Nathan O., Pentland A., Zyskind G. [2015], *Enigma: Decentralized Computation Platform with Guaranteed Privacy*, https://enigma.co/enigma_full.pdf

Nicholson Price W. [2017], *Artificial Intelligence in Health Care: Applications and Legal Implications*, in *The SciTech Lawyer*, Vol. 14, n. 1, 10-13

Nicola F. G., Pollicino O. [2020], *The balkanization of data privacy regulation*, in *West Virginia Law Review*, Vol. 123, 61-115

Noto la Diega G. [2016], *Machine Rules. Of Drones, Robots, and the Info-Capitalist Society*, in *The Italian Law Journal*, Vol. 2, n. 2, 367-404

Noto La Diega G. [2018], *Against the Dehumanization of Decision-Making - Algorithmic Decisions at the Crossroads of Intellectual Property, Data Protection, and Freedom of Information*, in *JIPITEC*, Vol. 9, n. 3, https://www.jipitec.eu/issues/jipitec-9-1-2018/4677

Noto La Diega G. [2023], *Internet of Things and the Law. Legal Strategies for Comsumer-Centric Smart Technologies*, Londra, Routledge

Noto La Diega G., Sappa C. [2020], *The Internet of Things at the intersection of data protection and trade secrets. Non-conventional paths to counter data appropriation and empower consumers*, in *European Journal of Consumer Law*, Vol. 3, 419-458

Orwell, G. [2017], *1984 & Animal Farm*, Melbourne, Text Publishing

Pagallo U. [2008], *La tutela della privacy negli Stati Uniti d'America e in Europa: modelli giuridici a confronto*, Bologna, Giuffrè Editore

Palmieri A. [2022a], *Diritto all'oblio, deindicizzazione e conclusioni non consequenziali alle premesse (nota a Cass., ord. 31 maggio 2021, n. 15160)*, in *Foro it.*, I, 331-335

Palmieri A. [2022b], *nota a Corte di Cassazione, Sezione VI civile, ordinanza 30 agosto 2022, n. 25481*, in *Foro it.*, I, 2669-2674

Palmieri A., Pardolesi R. [2014], *Diritto all'oblio: il futuro dietro le spalle (Nota a corte giust. 13 maggio 2014, causa C-131/12)*, in *Foro it.*, IV, 317-322

Palmieri A., Pardolesi R. [2020], *Polarità estreme: oblio e archivio digitali,* in *Foro it.*, I, 1570-1576

Palmieri A., Pardolesi R. [2022], *Diritti costituzionali effimeri? L'overruling di Roe v. Wade (nota a Corte suprema Stati uniti d'America 24 giugno 2022, Dobbs)*, in *Foro it.*, IV, 432-441

Palmirani M. [2020], *Big Data e conoscenza*, in *Riv. di filosofia del diritto*, n. 1, 73-91

Palmirani M., Sapienza S. (a cura di) [2022], *La trasformazione digitale della giustizia nel dialogo tra discipline. Diritto e intelligenza artificiale*, Milano, Giuffrè Editore

Pardolesi R. [1984], *nota a Corte di Cassazione, Sezione I civile, sentenza 18 ottobre 1984, n. 5259*, in *Foro It.*, I, 2712-2721

Pardolesi R. [2003], *Dalla riservatezza alla protezione dei dati personali: una storia di evoluzione e discontinuità*, in R. Pardolesi (a cura di) [2003], *Diritto alla riservatezza e circolazione dei dati personali*, vol. 1, Milano, Giuffrè Editore, 1

Pardolesi R. [2005], *Diritti della personalità*, in *Annali it. dir. autore*, 3-8

Pardolesi R. [2017], *Oltre «Google Spain» e il diritto all'oblio*, in *Foro it.*, IV, 219-222

Pardolesi R., Davola A. [2019], *"Smart contract": lusinghe ed equivoci dell'innovazione purchessia*, in *Foro it*., V, 195-207

Pascault L., Jütte B.J., Noto La Diega G., Priora G. [2020], *Copyright and Remote Teaching in the Time of COVID-19: A Study of Contractual Terms and Conditions of Selected Online Services*, in *European Intellectual Property Review*, Vol. 42, n. 9, 548-555

Pascuzzi G. [2013], *La creatività del giurista*, Bologna, Zanichelli

Pascuzzi G. [2020], *Il diritto dell'era digitale*, V ed., Bologna, Il Mulino

Pasquale F., *Black Box Society. The Secret Algorithms That Control Money and Information* [2015], Cambridge – Massachusetts, Harvard University Press,

Pfenninger R. [2021], *The Right to be Forgotten has Not Found its Home in United States Law: A Comparison of Law between the European Union and the United States*, in *Willamette Journal of International Law & Dispute Resolution*, Vol. 28, 291-314

Pierucci A. [2019], *Elaborazione dei dati e profilazione delle persone*, in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di) [2019], *I dati personali nel diritto europeo*, Giappichelli, Torino, 413-451

Pievatolo M. C. [2022], *Sulle spalle dei mercanti? Teledidattica e civiltà tecnologica*, disponibile su Zenodo: https://doi.org/10.5281/zenodo.6439508

Piroddi P. [2021a], *Commento art. 44 GDPR*, R. D'Orazio, G. Finocchiaro, O. Pollicino, G. Resta (a cura di) [2021], *Codice della privacy e data protection*, Giuffré, Milano, 616-628

Piroddi P. [2021b], *Commento art. 45 GDPR*, R. D'Orazio, G. Finocchiaro, O. Pollicino, G. Resta (a cura di) [2021], *Codice della privacy e data protection*, Giuffré, Milano, 628-640

Piroddi P. [2021c], *Commento art. 46 GDPR*, R. D'Orazio, G. Finocchiaro, O. Pollicino, G. Resta (a cura di) [2021], *Codice della privacy e data protection*, Giuffré, Milano, 640-651

Pizzetti F. [2021], *Protezione dei dati personali in Italia tra GDPR e codice novellato*, Torino, Giappichelli

Podda E., Palmirani M. [2021], *Inferring the Meaning of Non-personal, Anonymized, and Anonymous Data*, in V. Rodríguez-Doncel, M. Palmirani, M. Araszkiewicz, P. Casanovas, U. Pagallo, G. Sartor (a cura di) [2021], *AI*

Approaches to the Complexity of Legal Systems XI-XII, Lecture Notes in Computer Science, Cham, Springer, 269-282

Podda E., Vigna F. [2021], *Anonymization Between Minimization and Erasure: The Perspectives of French and Italian Data Protection Authorities*, in A. Kö, E. Francesconi, G. Kotsis, A. M. Tjoa, I. Khalil (a cura di), *Electronic Government and the Information Systems Perspective*, EGOVIS 2021, Lecture Notes in Computer Science, Cham, Springer, 103-114

Poddighe E. [2021a], *Commento art. 121 Codice*, in R. D'Orazio, G. Finocchiaro, O. Pollicino, G. Resta (a cura di), *Codice della privacy e data protection*, Giuffré, Milano, 1420-1431

Poddighe E. [2021b], *Commento art. 122 Codice*, in R. D'Orazio, G. Finocchiaro, O. Pollicino, G. Resta (a cura di), *Codice della privacy e data protection*, Giuffré, Milano, 1432-1441

Poddighe E. [2021c], *Commento art. 129 e 130 Codice*, in R. D'Orazio, G. Finocchiaro, O. Pollicino, G. Resta (a cura di), *Codice della privacy e data protection*, Giuffré, Milano, 1474-1487

Poillot E., Lenzini G., Resta G., Zeno-Zencovich V. [2021], *Data protection in the context of Covid-19, A short (hi)story of tracing applications*, Roma, Consumatori e Mercato

Poletti D. [2020], *Il trattamento dei dati inerenti alla salute nell'epoca della pandemia: cronaca dell'emergenza*, In *Persona e Mercato*, n. 2, 66-76

Poletti D. [2021], *Contact tracing e app immuni: atto secondo*, in *Persona e mercato*, n. 1, 92-101

Prosser W. [1960], *Privacy*, in *Cal. L. Rev.*, Vol. 48, 383-423

Quarta A., Smorto G. [2020], *Diritto privato dei mercati digitali*, Milano, Mondadori-Le Monnier Università

Ratti M. [2021], *Commento art. 25*, in R. D'Orazio, G. Finocchiaro, O. Pollicino, G. Resta (a cura di) [2021], *Codice della privacy e data protection*, Giuffré, Milano, 410-422

Ravà A. [1937], *Istituzioni di diritto privato*, Padova, Cedam

Reidenberg J.R. [1998], *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, in *Tex. L. Rev.*, Vol. 76, 553-593

Resta F. [2021], *Commento art. 57 Codice*, in R. D'Orazio, G. Finocchiaro, O. Pollicino, G. Resta (a cura di) [2021], *Codice della privacy e data protection*, Giuffré, Milano, 1192-1204

Resta G. [2014], *Dignità, persone, mercati*, Torino, G. Giappichelli Editore

Resta, G. [2015], *La sorveglianza elettronica di massa e il conflitto regolatorio USA/UE*, in *Il Diritto dell'informazione e dell'informatica*, 697-718

Resta G. [2019], *La successione nei rapporti digitali e la tutela postmortale dei dati personali*, in *Contratto e impresa*, n. 1, 85-105.

Resta G. [2021], *Commento art. 2-terdecies del Codice*, in R. D'Orazio, G. Finocchiaro, O. Pollicino, G. Resta (a cura di) [2021], *Codice della privacy e data protection*, Milano, Giuffré, 1115-1125

Resta G., Somma A., Zeno Zencovich V. [2020], *Comparare. Una riflessione tra le discipline*, Sesto San Giovanni, Mimesis Edizioni

Ricci A. [2019], *I diritti dell'interessato*, in G. Finocchiaro (a cura di) [2019], *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna, Zanichelli, 392-472

Richards, N. M. [2013], *The Dangers of Surveillance*, in *Harvard Law Review*, Vol. 126, n. 7, 1934-1965

Rodotà S. [1973], *Elaboratori elettronici e controllo sociale*, Bologna, Il Mulino

Rodotà S. [1999], *Repertorio di fine secolo*, Roma – Bari, Laterza

Rodotà S. [2009], voce *Controllo e privacy della vita quotidiana*, in *Enciclopedia Treccani online*, https://www.treccani.it/enciclopedia/controllo-e-privacy-della-vita-quotidiana_%28XXI-Secolo%29/

Rodotà S. [2012], *Il diritto di avere diritti*, Roma, Laterza

Royston S. W. [2016], *The Right to Be Forgotten: Comparing U.S. and European Approaches*, in *St. Mary's Law Journal*, Vol. 48, 253-275

Rubinstein, I. S., Good N. [2019], *The trouble with Article 25 (and how to fix it): the future of data protection by design and default*, in *International Data Privacy Law*, 1-20

Sacco R., Rossi P. [2019], *Introduzione al diritto comparato*, settima ed., Milano, Utet giuridica

Sætnan A.R., Schneider I., Green S. (a cura di) [2018], *The Policy and Politics of Big Data*, Oxon, Routledge

Sajfert J., Quintel T. [2017], *Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities*, disponibile in https://ssrn.com/abstract=3285873

Sartori L. [2009], *La tutela della salute pubblica nell'Unione europea*, Cittadella, Biblos

Sater S. [2017], *Blockchain and the European Union's General Data Protection Regulation*, disponibile in https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3080987

Scassa T. [2020], *A Human Rights-Based Approach to Data Protection in Canada*, in E. Dubois, F. Martin-Bariteau (a cura di) [2020], *Citizenship in a Connected Canada: A Research and Policy Agenda*, Ottawa Faculty of Law Working Paper No. 2020-26, disponibile in https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3620450

Schwartz P.M. [2021], *The Data Privacy Law of Brexit: Theories of Preference Change*, in *Theoretical Inquiries in Law*, vol. 22.2:111, disponibile in https://ssrn.com/abstract=3895999

Schwartz P.M., Peifer K. [2017], *Transatlantic data privacy law*, in *Georgetown Law Journal*, Vol. 106, n. 1, 115-180

Schweikart S.J. [2021], *Who Will Be Liable for Medical Malpractice in the Future? How the Use of Artificial Intelligence in Medicine Will Shape Medical Tort Law*, in *MINN. J.L. SCI. & TECH.*, Vol. 22, anche disponibile in https://scholarship.law.umn.edu/mjlst/vol22/iss2/2

Shabo A. [2017], *Electronic Health Record*, in *Encyclopedia of Database Systems*, Verlag, Springer, 101-177

Sigulem D., Ramos M.P., de Holanda Albuquerque R. [2017], *The New Medicine: From the Paper Medical Record to the Digitized Human Being* [2017], in H. Marin, E. Massad, M.A. Gutierrez, R.J. Rodrigues, D. Sigulem (a cura di) [2017], *Global Health Informatics*, *How Information Technology Can Change Our Lives in a Globalized World*, Amsterdam, Elsevier, 152-167

Snowden E. [2019], *Errore di sistema*, Milano, Longanesi

Solove D. [2002], *Conceptualizing privacy*, in *Calif. L. Rev.*, Vol. 90, 1087-1156

Solove D. [2006], *A Taxonomy of Privacy*, in *U. Pa. L. Rev.*, Vol. 154, 477-560

Solove D. [2011], *Nothing to Hide*, *The False Tradeoff Between Privacy and Security*, Yale University Press

Solove D., Hartzog W. [2014], *The FTC and the new common law of privacy*, in *Colum. L. Rev*., Vol. 114, 583-676

Solove D., Schwartz P.M. [2014], *Reconciling Personal Information in the United States and European Union*, in *Cal. L. Rev.*, Vol. 102, 877-916

Solove D., Schwartz P.M. [2021], *Information Privacy Law*, New York, Wolters Kluwer Law & Business

Solove D., Schwartz P.M. [2022], *ALI Data Privacy: Overview and Black Letter Text*, in *UCLA Law Review*, Vol. 68, 1252-1300

Somma A. [2019], *Introduzione al diritto comparato*, Torino, Giappichelli

Spedicato G. [2009], *Law as Code? Divertissement sulla lex informatica*, in *Ciberspazio e diritto*, n. 2, 233-259

Stalla-Bourdillon S., Knight A. [2017], *Anonymous data v. personal data–a false debate: an EU perspective on anonymization, pseudonymization and personal data,* in *Wis. Int'l L. J.*, Vol. 34, 284-322, disponibile in https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2927945

Staunton C., Slokenberga S., Mascalzoni D. [2019], *The GDPR and the research exemption: considerations on the necessary safeguards for research biobanks*, in *European Journal of Human Genetics*, Vol. 27, 1159-1167

Tambou O. [2018], *France: the French approach to the GDPR implementation*, in *European Data Protection Law Review*, Vol. 4, n. 1, 88-94

Tapscott D., Tapscott A. [2016], *Blockchain revolution: How the technology behind Bitcoin is changing money, business and the world*, London, Portfolio

TIPIK Legal [2021], *Report on the implementation of specific provisions of the Regulation (EU) 2016/679*, https://www.dataguidance.com/sites/default/files/1609930170392.pdf

Tosi E. (a cura di) [2019a], *Privacy Digitale, Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, Giuffrè Francis Lefebvre

Tosi E. [2019b], *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale*, Milano, Giuffrè Francis Lefebvre

Tosi E. [2021], *Diritto privato delle nuove tecnologie digitali*. *Riservatezza, contratti, responsabilità tra persona e mercato*, Milano, Giuffrè Francis Lefebvre

Tosoni L. [2020], *Article 4(5). Pseudonymisation*, in C. Kuner, L. A. Bygrave, C. Docksey, L. Drechsler (a cura di) [2020], *The EU General Data Protection Regulation: a Commentary*, Oxford, Oxford University Press, 225-230

Turco V. [2019], *Il trattamento dei dati personali nell'ambito del rapporto di lavoro*, in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di) [2019], *I dati personali nel diritto europeo*, Torino, Giappichelli, 517-556

Uda G.M. [2019]*, Il trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici,* in V. Cuffaro, V. Ricciuto, R. D'Orazio (a cura di) [2019], I *dati personali nel diritto europeo*, Torino, Giappichelli, 557-578

Ukrow J. [2018], *Data protection without frontiers: On the relationship between EU GDPR and amended OoE Convention 108*, in *European Data Protection Law Review*, Vol. 4, n. 2, 239-247

Van Eecke P, Simkus A. [2020], *Article 88. Processing in the context of employment*, in C. Kuner, L.A. Bygrave, C. Docksey, L. Drechsler (a cura di) [2020], *The EU General Data Protection Regulation: a Commentary*, Oxford, Oxford University Press, 1229-1239

Wachter S., Mittelstadt B., Floridi L. [2017], *Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation*, in *International Data Privacy Law*, Vol. 7, n. 2, 76-99

Warren S. D., Brandeis L. D. [1890], *The right to privacy*, in *Harvard Law Review*, Vol. 5, n. 4, 193-220

Weitzenboeck E. M., Lison P., Cyndecka M., Langford M. [2022], *The GDPR and unstructured data: Is anonymization possible?*, in *International Data Privacy Law*, Vol. 12, n. 3, 184-206

Werbach K. [2018], *Trust, But Verify: Why the Blockchain Needs the Law*, in *Berk. Tech. L. J.*, Vol. 33, 489-553

Westin A. F. [1966], *Science, privacy, and freedom: issues and proposals for the 1970's: part II--balancing the conflicting demands of privacy, disclosure, and surveillance*, in *Columbia Law Review*, Vol. 66, n. 7, 1205-1253

Wiese Svanber C. [2020], *Article 89. Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes*, in C. Kuner, L.A. Bygrave, C. Docksey, L. Drechsler (a cura di) [2020], *The EU General Data Protection Regulation: a Commentary*, Oxford, Oxford University Press, 1240-1251

Zambrano V. [2019], *Il Comitato europeo per la protezione dei dati*, in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di) [2019], *I dati personali nel diritto europeo*, Torino, Giappichelli, 985-999

Zuboff S. [2019], *The age of surveillance capitalism: The fight for a human future at the new frontier of power*, New York, Profile Books

Indice delle abbreviazioni e degli acronimi

American Law Institute = ALI

Cassazione = Cass.

Codice civile = c.c.

Codice della proprietà industriale = c.p.i.

Codice di procedura civile = c.p.c.

Codice penale = c.p.

Comma = co.

Convenzione Europea dei Diritto dell'Uomo = Cedu

Corte di Giustizia dell'Unione Europea = CGUE

Corte Europea dei Diritto dell'Uomo = CEDU

Costituzione della Repubblica Italiana = Cost.

D.lgs. 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali = Codice Privacy

Data Protection by Default= DPbDf

Data Protection by Design= DPbD

Data Protection Impact Assessment = DPIA

Data Protection Officer = DPO

Decreto del Presidente del Consiglio dei Ministri = d.p.c.m.

Decreto del Presidente della Repubblica = d.p.r.

Decreto legge = d.l.

Decreto legislativo = d.lgs.

Decreto ministeriale = d.m.

European Data Protection Board = EDPB

European Data Protection Supervisor = EDPS

Garante per la protezione dei dati personali = Garante Privacy

Gruppo di lavoro art. 29 = Gruppo art. 29 o WP29

Internet of Things = IoT

Legge = l.

Ordinanza = ord.

Paragrafo = par.

Privacy by design = PbD

Regio decreto = r.d.

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) = GDPR

Unione europea = UE

Diritto aperto / 2

www.ledizioni.it

versione Open Access