MANUALE SULLA PROTEZIONE E CIRCOLAZIONE DEI DATI PERSONALI

a cura di
Chiara Angiolini, Antonello Iuliani

FIRENZE UNIVERSITY PRESS
USiena PRESS

STRUMENTI DEL DIPARTIMENTO DI GIURISPRUDENZA DI SIENA

ISSN 3035-5656 (PRINT) | ISSN 3035-5842 (ONLINE)

– 4 –

STRUMENTI DEL DIPARTIMENTO DI GIURISPRUDENZA DI SIENA

Manuale sulla protezione e circolazione dei dati personali

a cura di
Chiara Angiolini, Antonello Iuliani

FIRENZE UNIVERSITY PRESS | USIENA PRESS
2025

Manuale sulla protezione e circolazione dei dati personali / a cura di Chiara Angiolini, Antonello Iuliani. – Firenze : Firenze University Press ; Siena : USiena PRESS, 2025.
(Strumenti del Dipartimento di Giurisprudenza di Siena ; 4)

https://books.fupress.com/isbn/9791221507966

ISSN 3035-5656 (print)
ISSN 3035-5842 (online)
ISBN 979-12-215-0795-9 (Print)
ISBN 979-12-215-0796-6 (PDF)
ISBN 979-12-215-0797-3 (ePUB)
ISBN 979-12-215-0798-0 (XML)
DOI 10.36253/979-12-215-0796-6

Graphic design: Alberto Pizarro Fernández, Lettera Meccanica SRLs

La pubblicazione è stata possibile grazie al contributo specifico dell'Università di Siena per il supporto all'Open Access e a fondi del Dipartimento di Giurisprudenza.

Peer Review Policy
Peer-review is the cornerstone of the scientific evaluation of a book. All FUP - USiena PRESS's publications undergo a peer-review process by external experts under the responsibility of the Editorial Board and the Scientific Boards of each series (DOI 10.36253/fup_best_practice.3).

Referee List
In order to strengthen the network of researchers supporting FUP - USiena PRESS's evaluation process, and to recognise the valuable contribution of referees, a Referee List is published and constantly updated on FUP - USiena PRESS's website (DOI 10.36253/fup_referee_list).

Best Practice in Scholarly Publishing (DOI 10.36253/fup_best_practice)

The online digital edition is published in Open Access on www.fupress.com.

Published by Firenze University Press and USiena PRESS

Powered by Firenze University Press
Università degli Studi di Firenze
via Cittadella, 7, 50144 Firenze, Italy
www.fupress.com

This book is printed on acid-free paper
Printed in Italy

Sommario

FUP Best Practice in Scholarly Publishing (DOI 10.36253/fup_best_practice)

Introduzione

Chiara Angiolini, Antonello Iuliani

Un fitto dialogo scientifico e un costante confronto sulla didattica ci hanno portato all'idea, un paio di anni fa, del *Manuale sulla protezione e la circolazione dei dati personali*. Al progetto hanno entusiasticamente aderito come autori anche Gianluca Navone ed Elia Cremona, il cui contributo è stato fondamentale per la realizzazione dell'opera.

Siamo partiti dall'osservazione della moltiplicazione e della crescente importanza delle regole relative al trattamento dei dati personali, nel quadro di un *diritto dei dati* che va formandosi in seno all'ordinamento europeo e nazionale.

L'obiettivo è stato quello di costruire un volume volto a offrire agli studenti, ai professionisti del settore e, più in generale, a chiunque voglia accostarsi alla materia, uno *strumento* che permetta di acquisire una conoscenza sistematica delle nozioni e degli istituti relativi alla protezione e alla circolazione dei dati personali.

L'analisi del dettato normativo, non limitata al solo Regolamento Generale sulla Protezione dei Dati Personali (Reg. UE 2016/679) ed estesa anche ad alcuni profili dei più recenti atti normativi, come il *Data Act* (Reg. UE 2023/2854) e il *Data Governance Act* (Reg. UE 2022/868), è arricchita da una disamina della giurisprudenza europea e nazionale più rilevante, indispensabile per comprendere le *rationes* e l'effettiva portata delle regole che compongono il diritto attuale.

FUP Best Practice in Scholarly Publishing (DOI 10.36253/fup_best_practice)

Il trattamento dei dati personali in una pluralità di interessi

Chiara Angiolini, Antonello Iuliani

Abstract: This chapter introduces the book's subject through a brief history of data protection laws. The variety of interests protected by laws is highlighted. Indeed, it is shown how the legal changes are mainly due to the technological developments.

Keywords: History of data protection laws, variety of interests protected by laws, technological developments and regulation.

1. Le origini del diritto alla riservatezza delle informazioni personali

Fin dall'antichità le informazioni personali, che per il momento possiamo genericamente definire come quelle che riguardano un individuo, sono state oggetto, sotto qualche forma, di attività di raccolta e utilizzo da parte di altri individui, singolarmente considerati o all'interno di un'organizzazione. Tali attività, tuttavia, sono state a lungo pressoché ignorate dalle regole giuridiche.

In realtà, sebbene non vi siano state per secoli regole espressamente deputate a disciplinare, in via generale, la raccolta e/o l'utilizzo di informazioni personali, queste ultime potevano ritenersi comunque strumentali allo svolgimento di azioni rilevanti di carattere pubblico (ad esempio, i censimenti) o privato (ad esempio, la conclusione di contratti), a dimostrazione del fatto che il trattamento di informazioni personali ha sempre avuto un rilievo sociale e, seppur indirettamente, anche giuridico.

Il modo di considerare la *comunicazione* di informazioni riguardanti una persona cambia, a livello giuridico, per la prima volta intorno alla fine del XIX secolo, principalmente per due ordini di ragioni: il primo tecnologico, il secondo politico-sociale.

Innanzitutto, l'avvento dei mezzi di comunicazione di massa ha reso possibile un livello di diffusione delle informazioni prima del tutto inimmaginabile. Se si considera che hanno iniziato a ricevere una simile diffusione anche informazioni afferenti alla vita privata degli individui, tramite, ad esempio, i primi

Chiara Angiolini, University of Siena, Italy, chiara.angiolini@unisi.it
Antonello Iuliani, Università digitale Pegaso, Italy, antonello.iuliani@unipegaso.it, 0000-0001-9931-6934

Referee List (DOI 10.36253/fup_referee_list)
FUP Best Practice in Scholarly Publishing (DOI 10.36253/fup_best_practice)

giornali sensazionalistici corredati di inserzioni fotografiche, ben si spiega come l'innovazione tecnologica sia stata determinante per l'affermazione di un interesse giuridico nei confronti di *alcune* informazioni personali, cioè quelle che si vogliono tenere riservate e, dunque, protette dalle interferenze esterne. D'altra parte, nel contesto sociale di fine Ottocento, i rischi ricondotti alle nuove tecnologie hanno rappresentato più che altro l'occasione per far emergere nitidamente quel desiderio di intimità che già si era formato con la transizione da una società feudale a una di stampo industriale (Rodotà 1995).

L'affacciarsi di un interesse alla riservatezza può considerarsi strettamente connaturato a un ordine giuridico borghese che intende difendere la sfera privata alla stregua di un bene su cui si esercita un diritto di proprietà. Invero, anche quando si è cercato di costruire un nuovo concetto – il *right to privacy* – autonomo, secondo le intenzioni dei suoi padri fondatori americani (Warren, Brandeis 1890), dal diritto di proprietà esercitabile sui beni materiali o immateriali, la componente individualistica-escludente era comunque ben rappresentata dalla celebre formula del «diritto di essere lasciati soli» (*the right to be let alone*).

La vicenda che presumibilmente spinse i due giuristi sopra evocati a prendere posizione, a favore del riconoscimento del nuovo diritto, è emblematica del contesto appena descritto: Samuel Warren, facoltoso avvocato ed esponente dell'alta borghesia di Boston, era indispettito dall'attenzione che la stampa locale era solita rivolgere a circostanze private della sua famiglia e desiderava, quindi, porre un freno a intrusioni giornalistiche di tal genere (cfr. Solove, Schwartz 2024). Si avvalse così dell'aiuto e dell'ingegno di Louis Brandeis – che successivamente sarebbe divenuto giudice della Corte Suprema degli Stati Uniti – per dimostrare come si dovesse configurare il diritto alla privacy e si potesse fornire ad esso tutela.

Parallelamente all'elaborazione statunitense del concetto di privacy, nell'Europa continentale – in particolar modo, in Germania – si andava affermando la teoria giuridica secondo cui ciascun individuo avrebbe un vero e proprio diritto alla tutela della personalità, quest'ultima composta da vari attributi quali, ad esempio, la vita, l'integrità fisica, il nome civile e commerciale, l'immagine. Ed è proprio all'interno di tale teoria che, negli anni a venire, i giuristi europei avrebbero accolto, pur con alcune differenze, la necessità di tutelare la *riservatezza* delle vicende riguardanti la sfera privata di una persona.

In Italia, in assenza per lungo tempo di norme espressamente dedicate alla materia, è stata la giurisprudenza a ricondurre il diritto alla riservatezza nell'alveo dei diritti della personalità, riuscendo a superare l'obiezione secondo cui gli interessi che possono assurgere al rango di tali diritti necessiterebbero di una tipizzazione legislativa. Invero, tra gli anni '50 e '70 del secolo scorso, la Corte di Cassazione ha affrontato il tema in diverse occasioni: inizialmente, negando del tutto l'esistenza di un diritto alla riservatezza nel nostro ordinamento (Cass. 22 dicembre 1956, n. 4487); successivamente, affermando che, pur in mancanza di un esplicito diritto alla riservatezza, la divulgazione di notizie relative alla vita privata altrui possa costituire un illecito (Cass. 20 aprile 1963, n. 990); infine, riconoscendo nella riservatezza un diritto pienamente autonomo e meritevole di tutela dalle ingeren-

ze di altri soggetti (Cass. 27 maggio 1975, n. 2129). I casi che hanno dato origine alle sentenze appena richiamate riguardano tutti la diffusione di vicende relative alla sfera privata di alcuni personaggi noti dell'epoca (il tenore Enrico Caruso; l'amante di Benito Mussolini, Claretta Petacci; la regina iraniana Soraya Esfandiyari Bakhtiyari), attraverso mezzi di comunicazione di massa di diverso tipo (nel primo caso, un film; nel secondo e nel terzo caso, un periodico).

Le fattispecie prese come riferimento del potenziale *vulnus* rimangono, quindi, sostanzialmente le stesse di quelle che, decenni prima, sollecitavano l'iniziativa d'oltreoceano di Warren e Brandeis: fattispecie in cui la riservatezza – elevata al rango di diritto della personalità – si contrappone principalmente alla libertà di informazione ed espressione esercitata attraverso i *mass media*, con l'evidente esigenza di operare un delicato bilanciamento di interessi onde evitare di sacrificare indiscriminatamente una fondamentale area di libertà come quella appena menzionata, essenziale per una società democratica.

Ebbene, l'affermarsi del diritto alla riservatezza (sul quale, v. più approfonditamente *infra* cap. *Le fonti*, § 5.1) certamente incide sul fenomeno della raccolta e dell'utilizzo di informazioni personali; tuttavia, occorre osservare che tale diritto, per un verso, copre parzialmente il nostro campo d'indagine e, per un altro, potrebbe eccederlo. Infatti, traducendosi la riservatezza nel diritto di proteggere la propria sfera privata da forme di intromissione esterna non desiderata, essa riguarda – nel suo contenuto sostanzialmente escludente – le sole informazioni personali rispetto a cui un individuo vuole mantenere un riserbo. D'altronde, l'interesse giuridicamente protetto non vale solo contro l'ingerenza altrui che si manifesta nel trattamento di informazioni sul proprio conto, ma si attesta contro qualunque tipo di ingerenza che leda la propria sfera privata al di là di un effettivo trattamento di informazioni personali (ad esempio, la richiesta continua e importuna di rivelare informazioni che non si è disposti a concedere).

Sebbene quest'accezione di riservatezza abbia subito nel tempo un'evoluzione o, per meglio dire, sia stata affiancata da altri interessi cui l'ordinamento ha deciso di attribuire maggiore rilevanza, non può negarsi che essa continui a rappresentare uno degli interessi sottesi alla materia che si sta affrontando. In altri termini, pur non costituendo più il nucleo centrale della disciplina sul trattamento di informazioni personali, non può considerarsi un interesse del tutto recessivo, almeno là dove le informazioni trattate richiedano una protezione particolare.

2. Dalla riservatezza al controllo dei dati personali: l'evoluzione delle tecnologie e del diritto

Fino ad ora ci si è riferiti genericamente alle informazioni concernenti un individuo, che – come si è visto – costituiscono da sempre oggetto di varie forme di trattamento (per le definizioni normative di «dati personali», «persona interessata» e «trattamento», v. *infra* cap. *Le definizioni fondamentali*, §§ 1-3). I *mass media* hanno indubbiamente facilitato la loro diffusione, ampliando in modo esponenziale la platea di destinatari di un messaggio comunicativo con-

tenente informazioni personali, e di conseguenza hanno palesato i rischi insiti in una simile attività.

Tuttavia, il vero punto di svolta è rappresentato dall'avvento delle procedure automatizzate con cui i primi computer – per lo più in mano pubblica – hanno iniziato a elaborare informazioni, divenute ormai dati. Con le tecnologie informatiche, infatti, i dati personali si moltiplicano a tal punto che la questione da risolvere non attiene più soltanto alla diffusione di informazioni che ci riguardano presso soggetti che non vorremmo le possedessero, ma attiene – prima ancora – alla mancata conoscenza di chi tratta simili informazioni e di quali risultano nella sua disponibilità.

Il cambiamento qualitativo e quantitativo nel trattamento delle informazioni personali generato dall'automatizzazione dei processi di raccolta ed elaborazione di dati inevitabilmente si riflette sul concetto di privacy. Non a caso, uno studio pioneristico di fine anni '60 non la definisce più come il diritto di essere lasciati soli, bensì come il diritto di ciascuno di *controllare* l'uso che altri fanno delle informazioni che lo riguardano (Westin 1967).

Negli anni '70, alcuni Paesi europei introducono le prime discipline appositamente dedicate al trattamento dei dati personali. In realtà, le primissime norme sono contenute nelle leggi regionali di due Land tedeschi, l'Assia e la Baviera, e a seguire intervengono le leggi nazionali di Stati come la Svezia (1973), la Repubblica federale tedesca (1977), la Francia, la Norvegia, la Danimarca, l'Austria (1978) e il Lussemburgo (1979). Inoltre, il 28 giugno 1981 viene adottato a Strasburgo il primo trattato internazionale in materia: la Convenzione del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (Convenzione n. 108/1981).

Il principale tratto comune di queste novità normative è l'attribuzione al soggetto interessato, le cui informazioni vengono trattate da altri, di un diritto di accesso ai dati personali oggetto di trattamento. L'accesso, infatti, è considerato uno strumento essenziale per poter esercitare un controllo effettivo sull'uso che viene fatto dei dati che ci riguardano. Solo accedendo a essi, è possibile richiedere, ad esempio, una rettifica delle informazioni sul proprio conto che altri trattano. Inoltre, valorizzando il diritto di accesso ai dati personali, si riconosce implicitamente che il trattamento di tali dati non dev'essere necessariamente ostacolato, purché sia controllabile e rispettoso di alcuni principi che riducono i rischi a esso connessi, come, ad esempio, i principi circa la qualità e la sicurezza dei dati trattati, già previsti dalla Convenzione di Strasburgo (Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, 1981).

La raccolta e l'elaborazione di grandi moli di dati iniziano a essere viste come un'opportunità per rendere più efficienti i processi decisionali sia a livello imprenditoriale, che nell'ambito dei programmi di politica sociale portati avanti dalle autorità pubbliche. Se, dunque, il trattamento di dati personali tramite le tecnologie informatiche può assecondare efficacemente il legittimo perseguimento di interessi sociali ed economici, lo strumento di tutela dei soggetti interessati non può più risolversi nell'innalzamento di una stabile barriera a protezione della propria sfera di riservatezza individuale. Infatti, se la riserva-

tezza della sfera privata rimane un interesse tutelato dall'ordinamento, questo non sempre prevale di fronte ad altri interessi di vari soggetti al trattamento dei dati (es. trattamento dei dati personali per ragioni di interesse pubblico o sulla base di legittimi interessi).

Da un lato, il passaggio dallo Stato liberale allo Stato sociale ha, in parte, depotenziato la garanzia di uno spazio di intimità privata reclamato dalla classe borghese, vista l'esigenza di raccogliere notevoli informazioni sulla popolazione per una migliore erogazione dei servizi pubblici; dall'altro, la transizione a un capitalismo post-industriale ha reso l'informazione sulla clientela un fattore fondamentale per lo svolgimento di vari servizi, su tutti quelli di natura finanziaria (ad esempio, servizi bancari e assicurativi).

Cionondimeno, il trattamento di dati personali resta tutt'altro che privo di insidie, le quali, a ben vedere, non riguardano solo la sicurezza dei sistemi informatici, per la loro esposizione, ad esempio, a eventuali furti di dati. I principali rischi riguardano, infatti, i possibili abusi derivanti dall'esercizio del nuovo potere informatico profondamente pervasivo: disporre di molte informazioni personali consente, invero, di profilare gli individui, discriminandoli in base a diversi fattori e attribuisce a chi tratta i dati un potere conoscitivo spesse volte molto rilevante (Zuboff 2019). Di conseguenza, se tali fattori discriminanti finiscono per essere gli aspetti che maggiormente segnano l'identità degli individui, è evidente che gli esiti possano essere distopici e preoccupanti, limitando la stessa libertà di esprimersi e di scegliere. In questo quadro, può facilmente spiegarsi come mai la prima norma dell'ordinamento italiano a tutela dei dati personali si ritrovi nello Statuto dei lavoratori, il cui art. 8 – tuttora vigente – stabilisce che «è fatto divieto al datore di lavoro, ai fini dell'assunzione, come nel corso dello svolgimento del rapporto di lavoro, di effettuare indagini, anche a mezzo di terzi, sulle opinioni politiche, religiose o sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore».

Una chiave di lettura della materia di cui ci si sta occupando è costituita proprio dal *potere* che inevitabilmente si forma in capo a chi detiene grandi quantità di dati, vista la capacità di manipolazione che da essi può discendere. Al di là dell'imposizione di divieti, come quello appena citato, volti a delimitare delle zone impenetrabili per le attività di raccolta di dati, è lo strumento dell'accesso – sopra menzionato – a farsi carico, nella prima stagione normativa, del compito di assicurare un controllo di tale potere. Tuttavia, nonostante le speranze riposte nel diritto di accesso ai dati, ben presto ci si è accorti che si trattava di un dispositivo poco utilizzato e soprattutto incapace di affrontare, da solo, le nuove sfide poste dall'aumento considerevole dei soggetti che trattano dati personali con mezzi automatizzati, non più circoscritti – a partire dagli anni '90, per la diffusione dei personal computer – ai titolari di grandi banche dati.

Il controllo individuale dell'interessato sui dati che lo riguardano, che nel frattempo si è andato configurando come diritto all'autodeterminazione informativa (secondo la celebre formula utilizzata dalla Corte costituzionale tedesca, il *Bundesverfassungsgericht*, in una famosa pronuncia del 1983), richiedeva di essere corredato da un ben più articolato sistema di regole, passante per la

previsione di obblighi più definiti in capo al titolare del trattamento e rimedi più efficaci in capo al soggetto interessato (v. *infra* capp. *La disciplina dell'attività di trattamento* e *I diritti dell'interessato*).

A ciò si aggiunga che, negli stessi anni, la circolazione dei dati personali diveniva, in ambito europeo, sempre di più una componente fondamentale per garantire non solo – com'è evidente – la libera circolazione delle persone all'interno dello spazio comunitario, ma anche – seppur indirettamente – la libera circolazione di merci, servizi e capitali. Infatti, le relazioni commerciali spesso implicano un trattamento di dati personali; pertanto, le regole sul flusso di tali dati dovevano essere armonizzate per favorire la creazione di un mercato unico, al centro dell'agenda politica dell'allora Comunità europea (oggi Unione europea).

Le nuove istanze hanno sollecitato l'adozione del primo intervento organico a livello comunitario, la direttiva 95/46/Ce (c.d. «Direttiva madre»), la quale ha reso evidente come il trattamento dei dati personali costituisca un campo regolatorio in cui gravitano svariati interessi. La protezione dei dati personali rappresenta indubbiamente il principale obiettivo della disciplina, ma, oltre alla presenza di obiettivi concorrenti (la libera circolazione di tali dati nel mercato e, più in generale, in contesti sociali), è il combinarsi di situazioni giuridiche soggettive a esercizio individuale, da un lato, e di poteri pubblici esercitati da un'autorità indipendente con funzioni di controllo (v. *infra* cap. *La regolamentazione e la tutela amministrativa*), dall'altro, che dà l'idea della sempre maggiore distanza che separa la nuova privacy da quella degli albori, improntata esclusivamente sulla dimensione individualistica. La direttiva in questione, infatti, ha obbligato gli Stati membri della Comunità europea a istituire un'autorità nazionale che sorvegli sull'applicazione delle nuove regole. Molti Stati europei, in realtà, già contemplavano nel loro ordinamento simili autorità; non così l'Italia, che solo a partire dal 1997 ha visto operare il Garante per la protezione dei dati personali, istituito dalla prima legge contenente norme sulla tutela delle persone rispetto al trattamento dei dati (l. n. 675/1996).

Il recepimento nazionale della direttiva comunitaria ha costituito un passaggio di grande importanza non solo per i motivi appena citati, ma anche per l'opera di sistematizzazione degli interessi, che si stavano via via addensando attorno a un fenomeno – il trattamento dei dati personali – che finiva per ricomprendere fattispecie molto diverse. Invero, solo a titolo esemplificativo, un 'trattamento' può consistere tanto nell'archiviazione di informazioni personali in banche dati, quanto nell'utilizzo di dati semplici, non strutturati in archivi, ma riguardanti comunque persone fisiche, così come nella diffusione, tramite qualunque tipo di *mass media*, di fatti o rappresentazioni riferibili pur sempre a singoli individui. Con riguardo a quest'ultima fattispecie, ci si accorge, inoltre, che il trattamento di dati personali è il terreno d'elezione in cui può prendere forma quel diritto all'identità personale, riconosciuto a metà degli anni '80 dalla Suprema Corte (Cass. 22 giugno 1985, n. 3769), che tutela l'interesse di ciascuna persona di essere rappresentata, nella vita di relazione, in modo corrispondente alla propria personalità, ossia in un modo che raffiguri senza alterazioni il proprio patrimonio intellettuale, politico, sociale, religioso, ideologico, professionale, ecc.

Tale diritto, infatti, distinto da quello alla riservatezza, ma anche dai ben più risalenti diritti all'onore e alla reputazione, è stato tradizionalmente invocato rispetto a situazioni riconducibili all'ampia nozione di trattamento di dati personali, quali, ad esempio, l'impiego di sosia di persone note a fini pubblicitari o l'attribuzione a una persona di una posizione politica diversa da quella sostenuta. D'altronde, in una società in cui circolano sempre più informazioni e l'esposizione mediatica, almeno per alcuni soggetti, risulta frequente, diventa fondamentale tutelare la corretta rappresentazione dell'immagine sociale delle persone coinvolte. Non solo: l'affermazione del diritto all'identità personale (sul quale, v. per ulteriori dettagli *infra* cap. *Le fonti*, § 5.2) si spiega soprattutto all'interno di una società pluralistica in cui sia possibile per gli individui manifestare ciò che si è, senza subire interferenze esterne distorsive della propria personalità. In questo scenario, la riservatezza e l'identità personale possono considerarsi dei dispositivi complementari nel garantire il pieno esercizio dell'autonomia individuale, al netto di pressioni conformistiche provenienti da poteri pubblici o privati (Pino 2010).

Anche in questa nuova versione della privacy, strumentale alla costruzione della propria sfera esistenziale e, dunque, strettamente connessa all'attuazione dei valori personalistici sanciti nella Carta costituzionale (Marini 2006), continua a restare presente l'elemento del controllo individuale, declinato in un'ottica di autodeterminazione.

Occorre comunque chiarire che, sebbene la violazione del diritto all'identità personale spesso si riconduca a trattamenti illeciti di dati personali, il rispetto delle scelte esistenziali può travalicare l'ambito di cui ci si sta occupando. Ciò dimostra ancora una volta come le regole sul trattamento dei dati personali rappresentino un'area dell'ordinamento in cui si intersecano diverse posizioni giuridiche, la maggior parte delle quali, tuttavia, non attengono esclusivamente all'ambito in esame, pur caratterizzandolo in modo significativo.

Delle situazioni giuridiche che vengono in gioco, però, ve n'è una che nasce e si esercita necessariamente in relazione a un trattamento dei dati personali: è il diritto alla protezione degli stessi, assurto – come si vedrà (v. *infra* cap. *Le fonti*, § 4.1) – a diritto fondamentale nella Carta dei diritti fondamentali dell'Unione europea. Infatti, l'art. 8 CDFUE sancisce *tout court* il diritto alla protezione dei dati personali. L 'incidenza del trattamento – e dunque della raccolta, dell'uso e della circolazione – dei dati personali sulla persona è al cuore di tale norma, che stabilisce i principi e i limiti del trattamento, sancisce il diritto di accesso e rettifica dell'interessato e prevede come necessaria l'istituzione di un'autorità indipendente (v. infra, cap. *Le fonti*). Il diritto alla protezione dei dati personali di cui all'art. 8 CDFUE è stato letto da parte della dottrina come posto a tutela di interessi, fra cui la correttezza del trattamento, la non discriminazione e i principi di finalità e di qualità dei dati, diversi da quelli protetti attraverso il diritto alla riservatezza,(De Hert, Gutwirth, 2009). Dunque, il diritto alla protezione dei dati è da leggere in chiave relazionale ed è da interpretare come norma che impone di considerare lo squilibrio di potere, *in primis* conoscitivo, fra chi tratta i dati e chi è descritto attraverso tali dati. In ogni caso, al pari dei suoi an-

tecedenti, anche il diritto alla protezione dei dati personali viene ritenuto capace di individuare un'ulteriore dimensione della personalità, assunta a elemento unificante attraverso il prisma della tutela della dignità umana (Rodotà 2004).

L'elaborazione che si è venuta formando negli anni successivi al recepimento nazionale della direttiva 95/46, in merito agli interessi sottesi al trattamento dei dati personali, restituisce dunque un quadro fortemente incentrato sulla *tutela della persona* alla luce dei rischi ampiamente riconosciuti alle attività di trattamento (rischi per giunta amplificati dall'avvento di Internet, che ha frantumato ulteriormente le informazioni che riguardano individui, disperdendole e moltiplicandole nella rete). In altri termini, le regole sul trattamento dei dati personali sono state inquadrate in una dimensione essenzialmente non patrimoniale, in quanto di tale natura sono gli interessi – tutelati – ascrivibili agli interessati.

D'altronde, i principali casi giunti dinanzi agli organi giudicanti hanno sostanzialmente confermato l'incidenza della normativa in materia di dati personali sugli aspetti finora evocati: la violazione della disciplina è stata contestata in relazione, ad esempio, all'archiviazione sul *web* di notizie di cronaca non più attuali (Cass. 5 aprile 2012, n. 5525), allo 'spionaggio' privato tramite intercettazioni telefoniche (Cass. civ. 28 giugno 2018, n. 17036), alla prolungata conservazione dei dati concernenti indagini di polizia giudiziaria presso il Centro di elaborazione dei dati, c.d. C.E.D., del Dipartimento di pubblica sicurezza del Ministero dell'Interno (Cass. 29 agosto 2018, n. 21362), con quest'ultimo caso che fa riflettere anche sul rapporto notoriamente delicato tra esigenze di sicurezza pubblica e istanze di riservatezza dei dati.

Sebbene un tale inquadramento della materia al di fuori del diritto patrimoniale si giustifichi in ragione dell'attenzione rivolta alla tutela della persona, saldata dal richiamo alla categoria tradizionale dei diritti della personalità e a quella più recente dei diritti fondamentali di respiro costituzionale, non può passare inosservato che la rimozione del filtro nazionale nel recepimento della disciplina europea, avvenuta con l'adozione del Reg. UE 2016/679 (General Data Protection Regulation, d'ora in avanti: GDPR) (v. *infra* cap. *Le fonti*, § 4.2), abbia in parte ridimensionato l'assetto di interessi sopra descritto. Invero, nel GDPR, applicabile senza la necessità di una normativa nazionale di attuazione, (ri)emerge chiaramente – in termini ancora più netti rispetto alla direttiva 95/46 – l'obiettivo di disciplinare il trattamento dei dati personali non solo per proteggere i diritti e le libertà fondamentali delle persone fisiche, ma anche per non ostacolare la *libera circolazione* dei dati personali nell'Unione europea.

L'interesse sociale, compreso quello di carattere economico, che sospinge l'attività di trattamento dei dati personali riceve, quindi, espressa tutela, al punto che rischia di diventare parziale una lettura che attribuisca alle regole in questione una connotazione esclusivamente personalistica (Ricciuto 2018).

In fondo, l'aspetto da sottolineare è che i dispositivi di controllo, individuali o istituzionali – che possono essere attivati in relazione a un trattamento di dati personali, e che rappresentano una componente fondamentale per la tutela della persona nella sua proiezione difensiva (diritto alla riservatezza), costruttiva (diritto all'identità personale) e relazionale (diritto alla non discriminazione,

diritto alla protezione dei dati) – certamente caratterizzano in modo preminente la disciplina sul trattamento dei dati, ma, ciononostante, non ricoprono tutti gli interessi sottostanti.

3. Controllo e governance dei dati in un vortice di interessi

Per comprendere appieno quanto emerso nella parte conclusiva del precedente paragrafo, occorre soffermarsi ancora una volta sulle innovazioni tecnologiche e su come esse condizionano la prospettiva da cui si guarda a un fenomeno. Invero, se già le tecnologie informatiche avevano consentito di trasformare l'informazione in dati, permettendo alle imprese di utilizzare questi ultimi come risorsa economica per migliorare la propria attività (cfr. Camardi 1998), è nell'ambito dei servizi digitali – diffusisi, prima, con l'accesso in massa a Internet e, dopo, con l'utilizzo costante di *smartphones* e altri *smart devices* – che i dati personali vengono visti definitivamente come qualcos'altro da un insieme di segni che possono concorrere alla definizione della sfera individuale.

Il più delle volte, infatti, il rilascio di dati personali, per lo più di dati comportamentali, è il mezzo attraverso cui gli utenti godono dei servizi digitali offerti da imprese all'interno di infrastrutture che si è soliti definire «piattaforme» (cfr. Perlingieri 2014; Resta, Zeno-Zencovich 2018): basti pensare ai servizi di *social network*, ai servizi di condivisione e visualizzazione di contenuti multimediali o ai servizi di archiviazione di dati su *cloud*, la cui fruizione da parte degli utenti avviene frequentemente senza il pagamento di un corrispettivo pecuniario. Tali utenti si qualificano soprattutto come consumatori, con la conseguenza di dover tutelare – oltre ai loro dati – anche l'interesse di tali soggetti ad assumere scelte economiche consapevoli e a ottenere prestazioni contrattuali soddisfacenti (v. *infra* cap. *Le intersezioni fra disciplina in materia di dati personali e diritto dei consumatori*).

Non solo: gli algoritmi, spesso di intelligenza artificiale (v. la postfazione *La base giuridica dell'AI Act ex art. 114 Tfue: l'intelligenza artificiale tra mercato e persona*), utilizzati nell'ambito di molti servizi digitali funzionano grazie all'elaborazione di grandi quantità di dati, e più dati riescono a processare, migliori sono i risultati che forniscono; di conseguenza, i dati acquisiscono sempre di più un grande valore, anche per allenare i sistemi di intelligenza artificiale (v. ad esempio l'art. 10 del Reg. UE 2024/1689, AI ACT). Nell'era dei *Big Data*, il ruolo dei dati è spesso paragonato a quello svolto dal petrolio per l'economia industriale (da qui la nota espressione *data is the new oil*).

Si è giunti in una fase in cui tutto viene 'datificato': in particolare, moltissimi oggetti sono connessi a una rete telematica (c.d. *Internet of things*) e generano dati che riguardano elementi dell'ambiente circostante grazie a sensori incorporati negli oggetti stessi.

In un simile contesto, definire quali dati sono personali e quali non lo sono diventa sempre più ambiguo, ma soprattutto il processo di valorizzazione in atto riguarda tanto gli uni quanto gli altri (v. cap. *Le definizioni fondamentali*, par. 1). Il conflitto di interessi che si profila non è più soltanto tra l'interesse alla

circolazione e l'interesse alla protezione dei dati personali, potendo adesso riguardare la stessa appropriazione del *valore* generato dai dati, personali e non. Ciò non toglie che, anche rispetto a questo secondo conflitto di interessi, il carattere personale dei dati possa giustificare un sistema di regole almeno in parte diverso da quello applicabile ai dati che non presentano tale carattere.

In termini più generali, rimane centrale la questione del *potere* detenuto da chi possiede una grande mole di dati: non più solo come meccanismo in grado di intaccare la personalità degli individui (che comunque sono sottoposti a ulteriori rischi di discriminazione algoritmica), ma anche come mezzo che rischia, da un lato, di alterare il mercato accentrando a dismisura il valore generato dai dati nelle mani di pochi operatori e, dall'altro, di trasformare persino gli equilibri tra poteri pubblici e privati a causa della pervasità di questi ultimi nel mondo digitale (cfr. Pollicino 2023; Stanzione (a cura di) 2022). I tentativi per affrontare le nuove problematiche possono volgere in varie direzioni. Finora, una delle principali iniziative, sul piano giuseconomico, è stata condotta in Germania dall'autorità nazionale garante della concorrenza (il *Bundeskartellamt*), che ha contestato a Facebook, oggi Meta Platforms, un abuso di posizione dominante in riferimento a determinate pratiche di raccolta e utilizzo dei dati degli utenti iscritti al *social network* (cfr. Pardolesi, Van den Bergh, Weber 2020).

Non mancano, comunque, interventi sul piano regolatorio che provano a farsi carico del difficile contemperamento di interessi con riguardo alla condivisione dei dati, per garantire una più ampia distribuzione del valore che gli stessi possono generare. In particolare, come si vedrà più avanti (v. *infra* cap. *La disciplina dei diversi rapporti che riguardano i dati personali*, §§ 7 e 8), il legislatore europeo, attraverso l'introduzione di nuove discipline dirette a governare i flussi di dati, si prefigge l'obiettivo di favorire tale condivisione sia nei rapporti fra soggetti privati, sia nei rapporti fra privati ed enti pubblici. Invero, oltre a un problema di giustizia distributiva sullo sfruttamento economico dei dati, si pone anche la questione della loro maggiore valorizzazione per finalità di carattere sociale: si pensi all'utilizzo dei dati per fini di ricerca scientifica o nell'ambito dei servizi sanitari o delle politiche di *smart city*.

L'architettura regolatoria che concerne il trattamento dei dati personali si estende, in tal modo, su più articolazioni normative, proprio perché – come si è cercato fin qui di dimostrare – sono molteplici gli interessi che vengono coinvolti nelle diverse attività di trattamento. In ogni caso, non tutte le fonti che intervengono sulla materia sono da porre sullo stesso livello, come si dirà nel prossimo capitolo.

Riferimenti bibliografici

Camardi, Carmela. 1998. "Mercato delle informazioni e privacy: riflessioni generali sulla L. n. 675/1996." *Europa e diritto privato* 4: 1049-73.

De Hert, Paul, GutwIrth. 2009. "Serge Data protection in the case law of Strasbourg and Luxemburg: Constitutionalisation in Action." In GutwIrth, Serge, Poullet, Yves, De Hert, Paul, de Terwangne, Cécile, Nouwt Sjaak (a cura di). *Reinventing Data Protection?* Springer.

Finocchiaro, Giusella. 2012. *Privacy e protezione dei dati personali. Disciplina e strumenti operativi*. Bologna: Zanichelli.
Marini, Giovanni. 2006. "La giuridificazione della persona. Ideologie e tecniche nei diritti della personalità." *Rivista di diritto civile* 1: 359 ss.
Pardolesi, Roberto, Van den Bergh Roger e Franziska Weber. 2020. "Facebook e i peccati da «Konditionenmissbrauch»." in *Mercato Concorrenza Regole, Società* 3: 507-37.
Perlingieri, Carolina. 2014. *Profili civilistici dei social networks*. Napoli: Edizioni Scientifiche Italiane.
Pino, Giorgio. 2010. "L'identità personale." In Stefano Rodotà e Mariachiara Tallacchini (a cura di). *Ambito e fonti del biodiritto*, vol. I: *Trattato di biodiritto*, 297-321. Milano: Giuffrè.
Pollicino, Oreste. 2023. "Potere digitale." In Marta Cartabia e Marco Ruotolo. *Potere e Costituzione. Enciclopedia del diritto. I tematici*, 410-46. Milano: Giuffrè.
Resta, Giorgio, e Vincenzo Zeno-Zencovich. 2018. "Volontà e consenso nella fruizione dei servizi in rete." *Rivista trimestrale di diritto e procedura civile*: 411-40.
Ricciuto, Vincenzo. 2018. "La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno." *Il diritto dell'informazione e dell'informatica* 34: 689-726.
Rodotà, Stefano. 1995. *Tecnologie e diritti*. Bologna: Il Mulino.
Rodotà, Stefano. 2004. "Tra diritti fondamentali ed elasticità della normativa: il nuovo codice della privacy." *Europa e diritto privato* 1: 1-12.
Stanzione, Pasquale (a cura di). 2022. *I 'poteri privati' delle piattaforme e le nuove frontiere della privacy*. Torino: Giappichelli.
Solove, Daniel J. e Paul M. Schwartz. 2024. *Information Privacy Law*. Burlington: Aspen.
Warren, Samuel D., e Louis D. Brandeis. 1890. "The Right to Privacy." *Harvard Law Review* 4, 5: 193-200.
Westin, Alan D. 1967. *Privacy and Freedom*. New York: Atheneum.
Zuboff, Shoshana. 2019. *Il capitalismo della sorveglianza*. Luiss: Roma.

Le fonti

Elia Cremona

Abstract: This chapter examines data protection sources, focusing on both European and national ones. It also deals with private sources such as codes of conduct.

Keywords: Legal sources, fundamental rights, codes of conduct

1. Introduzione

Sin dalle origini, a fine Ottocento, la disciplina giuridica dei dati personali si è caratterizzata per un elevato grado di dinamicità: nel corso del tempo, infatti, sono cambiate le esigenze di protezione, i centri del potere legislativo e di quello economico, sono cambiati i costumi ed è cambiata la società, oggi sempre più immersa nella dimensione digitale.

Il risultato di questa evoluzione è un paesaggio normativo complesso, fatto di princìpi e regole che promanano da soggetti diversi, che rispondono a logiche diverse, anche se tra loro complementari. Prima, dunque, di passare in rassegna le *fonti* di questa disciplina, ripercorriamo brevemente questa linea evolutiva.

Quando, come è stato ricordato in precedenza, Samuel D. Warren e Louis Brandeis si inventarono il diritto alla privacy, inteso nel senso di *right to be let alone* (Warren, Brandeis 1890), avevano in mente le intrusioni nella vita privata da parte della neonata stampa scandalistica, accusata da parte loro di aver varcato i limiti della decenza e del rispetto del diritto di proprietà. Il diritto alla privacy veniva cioè coniato come 'espansione' del più sacro dei diritti dello stato liberale: la proprietà, appunto, non più considerata come dominio sulle cose connotate da materialità, ma estesa al diritto di impedire la divulgazione di informazioni, pensieri e sentimenti riferibili al soggetto interessato.

Oggi, se pure l'etichetta privacy sia sopravvissuta e ancora largamente impiegata anche nel comune dibattito pubblico, è rimasto ben poco del «diritto

Elia Cremona, University of Siena, Italy, elia.cremona@unisi.it, 0000-0001-9336-218X

Referee List (DOI 10.36253/fup_referee_list)
FUP Best Practice in Scholarly Publishing (DOI 10.36253/fup_best_practice)

ad essere lasciati soli». Anzi, il principale campo di applicazione della normativa privacy è quello delle relazioni sociali e dei rapporti economici nello spazio digitale, nel quale l'*animus* dell'utente medio è non già quello di escludere qualcuno dal proprio dominio (*excludendi*) bensì di condividere (*communicandi*) informazioni, pensieri e sentimenti che lo riguardano con una platea più ampia possibile di soggetti.

Ciò si verifica sia nell'ipotesi in cui la condivisione del dato personale è lo scopo diretto dell'utente sul *web*, come nel caso delle piattaforme social (Instagram, X o Facebook), sia quando la condivisione è invece strumentale all'accesso ad un servizio, come nel caso dei servizi 'gratuiti' di cui fruiamo quotidianamente attraverso internet dando in cambio in nostri dati (dalla galassia dei servizi Google ai software Microsoft, fino ai più recenti sistemi di intelligenza artificiale generativa come Chat-GPT o Gemini). Nonostante ciò, il grado di consapevolezza dell'effetto «sorveglianza» (Zuboff 2018) che questa fruizione gratuita produce rimane molto scarso e, oggi, la privacy, intesa tradizionalmente come «riservatezza», sembra essere divenuta un problema meno percepito di un tempo.

L'evoluzione dei costumi sociali è così 'ruotata' intorno al concetto di privacy, che sul piano giuridico è però rimasto per lungo tempo ancorato alla cultura proprietaria che lo aveva ispirato.

Volendo scandire le tappe essenziali di questo percorso, prima di affermazione e poi di affrancamento dal modello proprietario, possiamo – sul piano del diritto internazionale ed europeo – indicare questa prima sequenza di atti: la Convenzione Europea dei Diritti dell'Uomo (del 1950), la Convenzione sulla protezione delle persone rispetto al trattamento automatizzato dei dati di carattere personale (c.d. Convenzione n. 108 del 1981), la Direttiva 95/46/CE, la Carta dei Diritti Fondamentali dell'Unione Europea (c.d. Carta di Nizza, 2001), il Reg. UE 2016/679 (il Regolamento Generale sulla Protezione dei Dati Personali; d'ora in avanti: GDPR) e, da ultimo, il corposo pacchetto di atti con i quali l'Unione Europea ha disciplinato il fenomeno digitale (a partire dal febbraio 2020).

In via di sintesi: il citato modello proprietario ha prodotto sul piano normativo l'affermazione del diritto al rispetto della vita privata e familiare, postulato in ambito convenzionale dall'art. 8 della CEDU e ribadito all'art. 7 della Carta di Nizza. A questo si è affiancato, dapprima con la Direttiva 95/46/CE, poi con l'art. 8 della Carta di Nizza, l'art. 16 del TFUE e infine con il GDPR, il paradigma del 'controllo' e della 'protezione dei dati', non più inteso in senso assolutistico quale proiezione di un diritto di proprietà, ma quale punto di caduta del bilanciamento tra l'esigenza di tutelare un diritto fondamentale della personalità e l'opposta esigenza di garantire quanto più possibile la 'circolazione' dei dati, personali e non personali.

E così, il GDPR ha rappresentato un compromesso tra le esigenze del mercato dei dati e quello della tutela dei diritti, delineando uno statuto giuridico dei dati personali, da una parte, strumentale alla *garanzia* delle libertà fondamentali dell'Unione e, dall'altra, anche *funzionale* al consolidamento del mercato unico.

Dopodiché, il processo non si è arrestato e il concetto giuridico di 'dato' ha iniziato ad essere disciplinato in un'ottica sempre più funzionale all'integrazio-

ne del mercato unico. A partire dal 2017, l'Unione Europea ha avviato un ampio processo di riforma che si è incentrato sui temi della «apertura dei dati» e del «riutilizzo delle informazioni» del settore pubblico (favorendo flussi di dati *Government to Government*, c.d. G2G, e *Government to Business*, c.d. G2B), in particolare con l'approvazione della Direttiva *Open Data*. Dopodiché, le tappe sono state scandite dall'approvazione, nel 2018, del Regolamento sulla circolazione dei dati non personali e poi dalla pubblicazione della *Strategia europea per i dati* del febbraio 2020, che ha gettato le basi, tra gli altri, per il *Data Governance Act* (che per primo definisce il 'dato' in quanto tale) e il *Data Act*. In particolare, l'Unione ha annunciato la creazione di spazi comuni europei di dati in alcuni settori strategici, non rinunciando ad incoraggiare lo sblocco di flussi di dati dal settore privato a quello pubblico (*Business to Government*, c.d. B2G) e tra privati (*Business to Business*, c.d. B2B, e *Business to Consumer,* c.d. B2C).

In definitiva, la linea tracciata descrive un processo di allontanamento dal paradigma proprietario che ha caratterizzato la prima (*right to be let alone*) e, in parte, la seconda stagione (*protezione e controllo*) della normativa privacy, per un approdo ad una terza fase regolatoria caratterizzata da un accento sul tema della 'condivisione', che mira a 'liberare' enormi quantità di dati a beneficio del mercato unico e della collettività.

2. L'ordinamento multilivello delle fonti in materia di dati personali

Come ormai avviene in molti settori dell'ordinamento, la disciplina in materia di protezione dei dati personali è distribuita su più livelli normativi: vi sono le fonti di diritto internazionale (la CEDU, la Convenzione 108 e le sentenze della Corte EDU); le fonti di diritto europeo (i Trattati, il GDPR, le sentenze della Corte di Giustizia, le Linee guida e i provvedimenti del Comitato europeo per la protezione dei dati); le fonti di diritto interno (la Costituzione, il codice privacy, alcuni atti del Garante per la protezione dei dati personali); le fonti di diritto privato (i codici di condotta, i contratti).

Tutte queste fonti – che analizzeremo separatamente nei paragrafi seguenti – concorrono tra loro, pur avendo un diverso grado gerarchico, diversi ambiti di competenza ed essendo state adottate in tempi diversi.

Per comporre a sistema, dunque, questa pluralità di fonti, occorre anzitutto saper bene governare i criteri di risoluzione delle possibili antinomie, ovvero: il criterio gerarchico, il criterio della competenza e il criterio cronologico.

Il criterio gerarchico prevede che le fonti di grado superiore prevalgano su quelle di grado inferiore. Queste ultime – se in contrasto con la fonte di grado superiore – sono affette da un vizio di validità e debbono essere disapplicate o annullate. Ad esempio, una norma del codice privacy (dunque di diritto italiano) che fosse in contrasto con il GDPR (dunque un regolamento europeo direttamente applicabile) sarebbe invalida. Il che significa che il giudice italiano dovrebbe non applicarla nel caso concreto o che la Corte costituzionale italiana, se investita della questione, dovrebbe annullarla attraverso una dichiarazione di incostituzionalità per violazione degli articoli 11 e 117 della Costituzione,

che impegnano l'Italia al rispetto del diritto europeo (secondo il principio del 'primato' del diritto europeo, affermato a partire dalla sentenza della Corte di Giustizia nel caso 15 luglio 1964, C-6/64, e poi ancora nella sentenza, 9 marzo 1978, C-106/77).

Il criterio della competenza prevede invece che l'eventuale contrasto tra fonti – di eguale grado gerarchico – sia risolto in favore della fonte cui è attribuita la competenza per materia, mentre il criterio cronologico prevede che, in caso di contrasto tra fonti di eguale grado gerarchico ed entrambi competenti, la norma successiva abroghi la precedente, e cioè la sostituisca dal momento in cui entra in vigore.

Nelle pagine che seguiranno, dunque, tutte le fonti che saranno passate in rassegna dovranno ritenersi 'contemporaneamente' applicabili, ogniqualvolta non si ravvisi un'ipotesi di antinomia, che quindi dovrà essere risolta alla luce dei criteri appena indicati.

3. Il diritto internazionale: la Convenzione Europea dei Diritti dell'Uomo e la Convenzione 108

L'articolo 8 della Convenzione Europea dei Diritti dell'Uomo (CEDU) e la Convenzione 108 del Consiglio d'Europa sono due pilastri fondamentali nella tutela di diritto internazionale del diritto alla privacy e alla protezione dei dati personali. La CEDU e la Convenzione 108 sono state approvate nell'ambito del Consiglio d'Europa, una organizzazione internazionale fondata nel 1949 – che conta oggi 46 stati membri – con l'obiettivo di promuovere i diritti umani, la democrazia e lo stato di diritto. In particolare, dal punto di vista giuridico, la CEDU, adottata nel 1950, è un trattato internazionale che garantisce una serie di diritti e libertà fondamentali agli individui e che ha istituito un giudice appositamente dedicato: la Corte Europea dei Diritti dell'Uomo.

La Convenzione 108, adottata nel 1981, è stata invece il primo trattato internazionale vincolante dedicato esclusivamente alla protezione dei dati personali e alla privacy. Con il protocollo di modifica adottato nel 2018, noto come Convenzione 108 *plus*, sono state ampliate e rafforzate le misure di protezione al fine di raccogliere le nuove sfide poste dalla digitalizzazione e dalla globalizzazione.

In Italia, entrambe queste convenzioni hanno un valore normativo rilevante. La CEDU, ratificata dall'Italia con la legge n. 848 del 1955, è applicabile e vincolante per il nostro ordinamento (Corte cost. 24 ottobre 2007, nn. 348 e 349). La Convenzione 108 è stata ratificata dall'Italia nel 1985, nella sua versione originaria, e nel 2021, nella sua versione aggiornata.

Entrando nel merito dei due testi normativi, vediamo che l'articolo 8 della CEDU stabilisce il diritto al rispetto della vita privata e familiare, del domicilio e della corrispondenza, tutelando la sfera privata delle persone da ingerenze arbitrarie da parte dello Stato (le uniche giustificazioni ammesse di tali 'interferenze' sono relative alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà

altrui). La Corte Europea dei Diritti dell'Uomo ha sviluppato nel corso degli anni un'ampia giurisprudenza sull'applicazione dell'articolo 8, chiarendo che qualsiasi interferenza nella vita privata e familiare deve essere giustificata, proporzionata e basata su una norma chiara e anteriormente conoscibile.

La Convenzione 108 integra la disciplina di principio contenuta nella CEDU, dettagliando maggiormente quali debbono essere gli obblighi degli stati aderenti in tema di protezione delle persone rispetto al trattamento automatizzato dei dati personali. In particolare, si prevede: i) che sia assicurata la trasparenza nelle modalità di trattamento dei dati e la qualità del dato e siano garantiti i diritti degli individui, come il diritto di rettifica; ii) che siano previste rigorose misure di sicurezza per proteggere i dati personali da accessi abusivi non autorizzati; iii) che sia assicurata la collaborazione tra le autorità di protezione dei dati dei vari paesi per affrontare le violazioni transfrontaliere.

4. Il diritto europeo

4.1. La Carta di Nizza e il TFUE

Nel sistema delle fonti relative alla protezione dei dati personali, il ruolo centrale è assunto senz'altro dal diritto dell'Unione Europea. Le fonti rilevanti sono tre: gli artt. 7 e 8 della Carta dei diritti fondamentali dell'Unione Europea (Carta di Nizza), l'art. 16 del Trattato sul funzionamento dell'Unione Europea (TFUE) e, soprattutto, il Regolamento Generale sulla Protezione dei Dati (GDPR), che ne dà compiuta disciplina. Tutte queste fonti sono immediatamente applicabili all'interno dell'ordinamento italiano (in attuazione del principio dell'*effetto diretto* affermato dalla Corte di Giustizia a partire dalla sentenza *Van Gend en Loos* del 1963). Come detto, inoltre, esse prevalgono sul diritto interno in caso di antinomia, in ossequio al principio del *primato* del diritto europeo sugli ordinamenti nazionali, incluso il diritto costituzionale, salvi i principi fondamentali (c.d. controlimiti).

Muovendo dalla Carta di Nizza, proclamata nel 2000 e divenuta giuridicamente vincolante con il Trattato di Lisbona nel 2009, possiamo ancora rilevare le due diverse anime di questa materia: quella della privacy intesa come 'riservatezza', come diritto di escludere altri dalla propria sfera personale, e quella della privacy intesa come diritto ad avere il 'controllo' sui propri dati personali, senza necessariamente accedere ad una logica esclusiva ed escludente.

In particolare, l'articolo 7 della Carta di Nizza riprende il contenuto dell'articolo 8 della CEDU che abbiamo toccato nel paragrafo precedente, stabilendo che «ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni». Ancora una volta, il diritto alla privacy viene garantito *contro* ingerenze arbitrarie da parte dello Stato e di terzi. La Corte di Giustizia ha interpretato questo diritto in modo ampio, includendovi ogni forma di comunicazione e interazione di carattere privato.

L'articolo 8 è invece specificamente dedicato ai dati personali, prevedendo che ogni persona abbia diritto alla protezione dei dati di carattere personale

che la riguardano. La norma individua già alcuni princìpi fondamentali legati al trattamento dei dati, che ritroveremo anche nel GDPR, ovvero che i dati debbano essere trattati secondo il principio di lealtà, per scopi specifici e sulla base del consenso dell'interessato o su altra legittima base prevista dalla legge. Ogni persona ha altresì il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica. Pure si prescrive che il rispetto di tali regole sia soggetto al controllo di un'autorità indipendente.

L'articolo 16 del Trattato sul funzionamento dell'Unione Europea (TFUE) stabilisce il quadro giuridico per la protezione dei dati personali, fissando la competenza delle istituzioni europee (Parlamento e Consiglio) alla adozione della normativa in materia e prevedendo altresì che tale disciplina sia, da una parte, funzionale alla protezione dei diritti fondamentali e, dall'altra, che sia funzionale a garantire comunque la circolazione dei dati all'interno dell'Unione.

4.2. Il Regolamento Generale sulla Protezione dei Dati n. 679/2016 (GDPR)

In questa logica di compromesso, tra esigenze di tutela dei diritti fondamentali ed esigenze di circolazione dei dati in funzione di promozione del mercato, l'Unione Europea ha varato il Regolamento Generale sulla Protezione dei Dati (GDPR) n. 679/2016, entrato in vigore il 25 maggio 2018, che rappresenta l'evoluzione e il rafforzamento della precedente Direttiva 95/46/CE sulla protezione dei dati personali. Tale direttiva infatti, adottata nel 1995, aveva già stabilito i primi standard a livello europeo per la protezione dei dati personali e introdotto alcuni concetti fondamentali come il consenso dell'interessato, il diritto di accesso e rettifica dei dati personali; tuttavia, proprio perché si trattava di una direttiva, richiedeva il recepimento da parte degli stati membri tramite leggi nazionali, determinando così una frammentazione del sistema della protezione dei dati personali all'interno dell'UE.

Il GDPR, essendo un regolamento, è invece direttamente applicabile in tutti gli Stati membri senza bisogno di recepimento (salvo che per alcune parti che espressamente prevedono l'adozione di normative da parte degli ordinamenti nazionali), garantendo così finalmente un livello uniforme di protezione dei dati personali.

L'articolo 2 del GDPR stabilisce l'ambito di applicazione materiale, individuando cioè le situazioni in cui il Regolamento si applica. In linea generale, il GDPR si applica al trattamento di dati personali di un soggetto «interessato» effettuato da un «titolare del trattamento» o da un «responsabile del trattamento» nell'Unione Europea (tali definizioni saranno affrontate nel dettaglio nei capitoli seguenti), con alcune eccezioni relative ad esempio ad attività non rientranti nell'ambito di applicazione del diritto dell'Unione (come la sicurezza nazionale), ad attività svolte da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico (come la gestione delle proprie rubriche di contatti o la corrispondenza privata) o ad attività di prevenzione, in-

dagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali (che sono disciplinate dalla Direttiva UE 2016/680).

Tale regolamento ha, poi, un ambito di applicazione territoriale particolarmente ampio. Ai sensi dell'art. 3, esso si applica su tutto il territorio dell'Unione, non solo ai trattamenti di dati di cittadini europei da parte di soggetti europei, ma anche ai trattamenti di dati effettuati da società con sede extra-europea che svolgano una attività effettiva e stabile sul territorio europeo (*establishment criterion*) e ai trattamenti che riguardano soggetti interessati che si trovino all'interno dell'Unione (*targeting criterion*).

Con riferimento al primo criterio di applicazione, è opportuno precisare che non rileva la forma giuridica assunta (sia essa, ad esempio, una succursale o una filiale di una società con sede all'estero) quanto piuttosto l'effettivo legame tra l'attività svolta sul territorio europeo in maniera stabile e il trattamento dei dati personali, indipendentemente dal fatto che quest'ultimo avvenga o meno sul territorio dell'Unione.

Il secondo criterio, quello dell'indirizzamento (*targeting*) del trattamento, è invece preordinato ad assicurare la piena applicabilità del GDPR a prescindere dalla cittadinanza, dalla residenza o da altri elementi propri della condizione giuridica del soggetto interessato, in applicazione di quanto previsto dall'art. 8 della Carta di Nizza, in forza del quale ogni 'persona' ha diritto alla protezione dei dati personali che lo riguardano. Sul punto, l'*European Data Protection Board* ha raccomandato di applicare tale criterio secondo un approccio 'bifasico' volto a determinare, *in primis*, se il trattamento si riferisce a dati personali di interessati che si trovano nell'UE e, in secondo luogo, se riguarda l'offerta di beni o la prestazione di servizi o il monitoraggio del comportamento di soggetti interessati all'interno dell'Unione Europea.

Non solo. Vale la pena evidenziare che il GDPR ha avuto una significativa influenza anche a livello globale. Infatti, dopo la sua adozione, sono molti gli stati che hanno adottato normative simili (dal Brasile, alla California, al Cile, al Giappone) secondo quello che è stato definito come *Brussels Effect* (Bradford 2020), ovvero la capacità dell'Unione di fissare standard normativi globali.

Il GDPR rappresenta il principale testo normativo che sarà esaminato nei capitoli che seguiranno. In linea generale, può sin qui osservarsi che le principali novità introdotte dal GDPR riguardano:

1. il rafforzamento dei diritti dei soggetti interessati, introducendo – tra gli altri – il diritto alla portabilità dei dati, e novellando, ad esempio, il diritto alla cancellazione (c.d. diritto all'oblio) e il diritto di opposizione al trattamento;
2. la previsione di un principio generale di responsabilizzazione (*accountability*), in virtù del quale i titolari del trattamento devono adottare misure tecniche e organizzative adeguate a garantire e dimostrare la conformità al regolamento. Il che implica che i titolari del trattamento non solo devono rispettare le norme del regolamento, ma devono anche essere sempre in grado di dimostrare di aver adottato idonee misure tecniche e organizzative;
3. l'introduzione di un obbligo per alcune organizzazioni di nominare un responsabile della protezione dei dati (*Data Protection Officer*), che svolge un

ruolo cruciale nel garantire la conformità al GDPR all'interno dell'organizzazione e funge da punto di contatto per le autorità di controllo e gli interessati;
4. la previsione di sanzioni elevate per le violazioni, fino a 20 milioni di euro o il 4% del fatturato globale annuo, allo scopo di assicurare l'efficacia delle sue disposizioni;
5. la regolamentazione rigorosa dei trasferimenti di dati personali verso paesi terzi, richiedendo adeguate garanzie come decisioni di «adeguatezza» da parte della Commissione Europea, clausole contrattuali standard, o norme vincolanti d'impresa (*Binding Corporate Rules*).

4.3. Le sentenze della Corte di Giustizia dell'Unione Europea

Anche se non si tratta di vere e proprie fonti normative, le sentenze della Corte di Giustizia dell'Unione Europea (CGUE) sono altrettanto importanti nel sistema di disciplina della protezione dei dati personali. Infatti, le sentenze della CGUE forniscono l'interpretazione autentica del diritto europeo e vincolano i giudici nazionali al rispetto di quella interpretazione. La CGUE ha emesso numerose sentenze che hanno avuto un impatto significativo sull'applicazione delle norme sulla protezione dei dati personali.

Ad esempio, con la sentenza resa nel caso *Google Spain* (CGUE, Grande Sezione, 13 maggio 2014, C-131/12), la Corte ha per la prima volta riconosciuto il c.d. diritto all'oblio, che è stato poi inserito due anni dopo all'art. 17 del GDPR. In quella vicenda, un cittadino spagnolo aveva presentato un reclamo all'Agencia Española de Protección de Datos (AEPD) contro Google Spain e Google Inc., chiedendo che Google rimuovesse dai risultati di ricerca i *link* ad un articolo di un giornale spagnolo del 1998, che riguardava un'asta immobiliare per il recupero di alcuni crediti insoluti, in cui veniva menzionato il suo nome. Il reclamo sosteneva che l'articolo fosse ormai irrilevante e che il continuo collegamento a esso attraverso il motore di ricerca fosse lesivo del diritto alla privacy. L'Autorità spagnola accolse la richiesta e Google impugnò la decisione, sostenendo che – essendo un 'mero' motore di ricerca – non aveva responsabilità sui contenuti pubblicati da terze parti e che l'articolo in questione fosse stato pubblicato legittimamente. La Corte, investita della questione, riconobbe invece la prevalenza del diritto all'oblio, stabilendo che i motori di ricerca sono «titolari del trattamento» dei dati personali che appaiono nelle pagine *web* che indicizzano e che, pertanto, gli individui hanno sempre il diritto di chiedere la rimozione dei *link* che contengono informazioni personali quando sono obsolete o non più rilevanti.

Altre importanti decisioni sono state quelle note come *Schrems I* (CGUE, 6 ottobre 2015, C-362/14) e *Schrems II* (CGUE, 16 luglio 2020, C-311/18), dal nome del cittadino austriaco, attivista della privacy, che aveva intentato i due giudizi. In entrambi i casi, la CGUE ha annullato gli accordi – denominati *Safe Harbor* e *Privacy Shield* – per il trasferimento dei dati personali dall'UE agli USA, così imponendo l'adozione di più elevati standard di tutela a tutte le imprese (ad esempio le grandi piattaforme digitali stabilite negli Stati Uniti) che

'importavano' i dati relativi ai cittadini europei (in tema v. cap. *La regolamentazione di diversi rapporti che riguardano i dati personali*).

O ancora, si ricordi la sentenza resa nel caso *Meta Platforms Ireland Limited* (già *Facebook Ireland Limited*) contro *Bundeskartellamt* (l'Autorità antitrust tedesca) nel 2023, in cui si discuteva della condotta di Facebook consistente nella raccolta e nella combinazione di dati personali raccolti su diverse piattaforme in assenza di uno specifico consenso (CGUE, C-252/21, 4 luglio 2023). In quel caso, la Corte di Giustizia ha affermato che il mancato rispetto delle norme in materia di protezione dei dati personali può essere valutato per capire se una pratica commerciale costituisce o meno un abuso di posizione dominante. In altre parole, se una piattaforma che detiene una posizione dominante sul mercato, come Facebook, impone condizioni che violano le norme sulla protezione dei dati, ciò può essere rilevante anche per l'irrogazione di una sanzione antitrust.

Questa decisione riconosce che le pratiche di trattamento dei dati possono avere un impatto significativo anche sul grado di concorrenza nel mercato, specialmente nel contesto di piattaforme digitali che basano il proprio *business model* sulla raccolta di enormi quantità di dati degli utenti.

4.4. Le Linee Guida dell'European Data Protection Board

Nel quadro generale delle fonti, particolare importanza è rivestita dalle linee guida fornite dall'European Data Protection Board (EDPB), un organismo indipendente dell'Unione Europea responsabile di garantire l'applicazione coerente del GDPR in tutta l'UE. Queste linee guida offrono chiarimenti e orientamenti su vari aspetti della materia della protezione dei dati personali, aiutando sia i titolari del trattamento che gli interessati a comprendere meglio gli adempimenti necessari al rispetto del regolamento (*compliance*), le responsabilità e i diritti. Questi documenti sono il risultato di un processo di consultazione pubblica e della collaborazione tra le autorità nazionali di protezione dei dati.

Ad esempio, tra le principali Linee Guida dell'EDPB, si rammentano quelle sul diritto di accesso dell'interessato (1/2022), sulle notificazioni di *data breach* (9/2022), sul *targeting* degli utenti dei social media (8/2020), sull'esercizio del diritto all'oblio (5/2019), sui requisiti per la prestazione del consenso al trattamento (5/2020).

5. Il diritto costituzionale italiano

5.1. Il diritto alla riservatezza

Anche se il diritto alla privacy non ricorre espressamente nel testo della Costituzione italiana, la sua disciplina ha una sua dimensione propriamente 'costituzionale', per due ordini di ragioni. La prima è rappresentata, come abbiamo visto, dal livello delle fonti che regolano la materia. Le fonti internazionali e le fonti del diritto europeo si collocano su di un piano gerarchico superiore alle

fonti primarie (leggi e atti aventi forza di legge) ed entrano nell'ordinamento italiano proprio grazie agli artt. 11 e 117 della Costituzione.

Tale dimensione costituzionale, però, deriva anche dalla natura di diritto fondamentale che nel tempo – attraverso una interpretazione evolutiva di alcune disposizioni del testo costituzionale – è stata riconosciuta al diritto alla privacy.

Sebbene infatti inizialmente la giurisprudenza della Corte di Cassazione avesse escluso l'ammissibilità di una protezione autonoma del diritto al rispetto della vita privata (Cass. 22 dicembre 1956, n. 4487), a partire dal 1975 l'orientamento mutò, individuando in particolare nell'art. 2 della Costituzione la principale norma di copertura costituzionale della materia.

L'art. 2 Cost., infatti, afferma il principio «personalista», riconoscendo e garantendo i diritti inviolabili dell'uomo, ed è considerato una norma a fattispecie aperta, suscettibile – a certe condizioni – di incrementare il catalogo dei diritti costituzionalmente tutelati, ancorché non espressamente nominati.

Anche grazie all'intervento della dottrina (in particolare, Rodotà 1973), la giurisprudenza di legittimità e costituzionale iniziò ad individuare via via gli ulteriori interessi costituzionalmente rilevanti coinvolti nella tutela del diritto alla privacy.

Oltre alla funzione di promozione del pieno sviluppo della persona umana promossa dall'articolo 3, comma 2, Cost., le norme costituzionali rilevanti sono state individuate nell'articolo 13, che garantisce l'inviolabilità della libertà personale proteggendo il singolo da ingerenze indebite nella sfera fisica e psichica, nell'articolo 14, che sancisce l'inviolabilità del domicilio proteggendo la casa come luogo privilegiato della vita privata, nell'articolo 15, che tutela la libertà e la segretezza della corrispondenza e delle comunicazioni da intrusioni non giustificate e, infine, nell'articolo 21, che, regolando la libertà di manifestazione del pensiero e di informazione, tutela anche il diritto di non vedere divulgate informazioni di carattere personale. A completare il sistema di tutela della vita privata, vanno richiamati anche gli articoli 19 (diritto di professare la propria fede religiosa), 16 (libertà di circolazione), 17 (diritto di riunirsi pacificamente) e 18 (libertà di associazione), tutti rilevanti per la protezione della 'personalità' dell'individuo.

Come è dunque evidente, la giurisprudenza della Corte costituzionale non ha ricondotto il diritto alla vita privata a un unico parametro costituzionale. Ad esempio, nella sentenza 12 aprile 1974, n. 38, la Corte ha collegato i diritti inviolabili dell'uomo, come decoro, onore, rispettabilità, riservatezza, intimità e reputazione, all'articolo 2 della Costituzione, in combinato con gli articoli 3, comma 2, e 13, comma 1.

La Corte ha inoltre evidenziato che il diritto alla tutela della vita privata è un corollario della dignità della persona. Nella sentenza 19 dicembre 1991, n. 467, la Corte ha affermato che la sfera intima e personale deve essere considerata il riflesso giuridico più profondo della dignità della persona umana e merita una tutela proporzionata al suo livello di priorità e al suo carattere fondante nella scala dei valori espressa dalla Costituzione italiana.

5.2. Il diritto all'identità personale

A fianco del diritto al rispetto della vita privata, ma parimenti ricompreso nella dimensione costituzionale del diritto alla privacy in virtù della stretta correlazione con il diritto alla riservatezza (come accennato *supra* nel cap. I, § 1), vi è il c.d. diritto all'identità personale, ovvero l'interesse del soggetto ad «essere se stesso» e a esprimere una «verità» attinente alla propria persona nella vita di relazione.

Il diritto all'identità personale si è differenziato dagli altri diritti della personalità, avendo per oggetto la proiezione sociale della personalità complessiva dell'individuo, garantendo la rappresentazione della sua vera identità nella vita di relazione, senza alterazioni del patrimonio intellettuale, ideologico, politico, etico, religioso o professionale (Cass. 7 febbraio 1966, n. 978). Il travisamento dell'identità può consistere sia nell'attribuzione di qualità inesistenti che nell'omissione di elementi esistenti, siano essi migliorativi o peggiorativi. Anche un'alterazione migliorativa può essere illegittima se incide sulla personalità, indipendentemente dalla lesione di altri diritti.

La Corte costituzionale, con la sentenza 3 febbraio 1994, n. 13, ha riconosciuto che il diritto all'identità personale rientra nella tutela prevista dall'art. 2 della Costituzione, contribuendo a formare il patrimonio inviolabile della persona umana. I fondamenti normativi della tutela dell'identità personale si trovano nelle disposizioni relative al nome, all'immagine e, ancora una volta, nell'art. 2 della Costituzione.

Naturalmente, il diritto all'identità personale – come tutti i diritti di rango costituzionale – può entrare in bilanciamento con altri diritti. Ad esempio, il diritto all'identità personale incontra un limite necessario nei diritti di cronaca, critica, satira e creazione artistica, riconducibili all'art. 21 della Costituzione. Il diritto di cronaca prevale infatti se sorretto dall'utilità sociale della notizia, dalla verità dei fatti divulgati e dalla continenza dell'esposizione.

6. Il Codice in materia di protezione dei dati personali

Il codice in materia di protezione dei dati personali, noto come codice privacy (d.lgs. n. 196/2003 che ha abrogato la precedente disciplina rappresentata dalla l. 675/1996), ha rappresentato per anni il principale riferimento per la protezione dei dati personali in Italia.

Con l'entrata in vigore del GDPR nel 2018, il Codice Privacy è stato significativamente novellato ad opera del d.lgs. n. 101/2018 che ne ha abrogato molte disposizioni, in virtù della attrazione della disciplina al livello regolamentare europeo, apportando altresì molte modifiche e integrazioni alle disposizioni residue.

Il Codice Privacy italiano è dunque una fonte gerarchicamente inferiore al GDPR e contiene solamente una disciplina di carattere attuativo (per le materie nelle quali il legislatore europeo non può intervenire, come le sanzioni penali)

e integrativo (per previsioni di dettaglio che lo stesso GDPR ha rimesso alla legislazione degli stati membri).

Essenzialmente, oggi il Codice Privacy fornisce: 1) i principi relativi al trattamento dei dati in situazioni specifiche (come quelli relativi al perseguimento di un compito di interesse pubblico o quelli relativi ai minori, alla sanità e alla giustizia); 2) la disciplina dei trattamenti in ambito pubblico, con particolare riferimento alle strutture socio-sanitarie, all'istruzione, alla ricerca, al lavoro e ai servizi di comunicazione elettronica; 3) la disciplina della composizione, del funzionamento e dei poteri del Garante per la protezione dei dati personali e degli strumenti di tutela amministrativa e giurisdizionale a disposizione dei soggetti interessati; 4) la disciplina del sistema sanzionatorio, amministrativo e penale.

7. La co-regolazione pubblico-privata: codici di condotta, certificazioni e Binding Corporate Rules

Uno degli aspetti più significativi del GDPR, di particolare interesse per quanto attiene al sistema delle fonti analizzato in questo capitolo, è l'approccio di forte incoraggiamento verso forme di co-regolazione pubblico-privata, nelle quali gli attori privati contribuiscono alla individuazione di regole e prassi conformi alle norme di protezione dei dati. Tale approccio si manifesta attraverso diversi strumenti, tra cui codici di condotta, certificazioni, *Binding Corporate Rules* (BCR), tutti orientati a fornire pratiche settoriali specifiche, aumentare la trasparenza e facilitare la *compliance* al Regolamento.

Analizziamoli singolarmente. I codici di condotta, ai sensi dell'art. 40 del GDPR, sono strumenti di autoregolamentazione che le associazioni e altri organismi rappresentativi possono sviluppare per facilitare l'applicazione del GDPR in contesti specifici. Il processo di adozione di un codice di condotta prevede che il testo sia sottoposto all'autorità di controllo nazionale competente per la revisione e l'approvazione. Una volta approvato, il codice viene pubblicato e ulteriori organizzazioni di settore possono aderirvi volontariamente. I soggetti promotori del codice di condotta devono altresì istituire organismi di monitoraggio, che debbono essere accreditati dall'autorità di controllo, per verificare il livello di adesione al codice e per gestire eventuali violazioni.

Le certificazioni sono invece strumenti che attestano la conformità di un'organizzazione alle norme del GDPR. L'art. 42 del GDPR incoraggia la creazione di meccanismi di certificazione, sigilli e marchi per dimostrare che i trattamenti di dati personali da parte di titolari e responsabili del trattamento sono conformi al regolamento. Tali certificazioni sono rilasciate da organismi accreditati deputati alla redazione di norme tecniche (*standard*). Ad esempio, una delle principali certificazioni è la ISO 27001 (rilasciata dalla International Organization for Standardization), che rappresenta lo standard internazionale che descrive le *best practices* per un sistema di gestione della sicurezza delle informazioni (SGSI).

Le *Binding Corporate Rules* (BCR) sono uno strumento volto a consentire il trasferimento di dati personali dal territorio dello Stato verso Paesi terzi (extra-

UE) tra società facenti parti dello stesso gruppo d'impresa. Ai sensi dell'art. 47 del GDPR, le BCR si concretizzano in una serie di regole, di natura contrattuale, che fissano i principi vincolanti al cui rispetto sono tenute tutte le società appartenenti ad uno stesso gruppo, allo scopo di semplificare gli oneri amministrativi a carico delle società multinazionali con riferimento ai flussi infra-gruppo di dati personali (art. 47 GDPR).

Sempre al fine di agevolare la *compliance* al GDPR, le BCR sono sottoposte alla revisione dell'autorità di controllo nazionale competente, che può coinvolgere anche altre autorità di controllo europee. Una volta approvate, le BCR sono applicate in tutte le entità del gruppo e il loro rispetto deve essere costantemente monitorato attraverso meccanismi di sorveglianza. Molte grandi aziende tecnologiche, come Google e Microsoft, hanno adottato BCR per gestire i trasferimenti di dati personali tra le loro filiali globali.

Riferimenti bibliografici

Bradford, Anu. 2020. *The Brussels Effect: How the European Union Rules the World*. Oxford: Oxford University Press.

Colapietro, Carlo, e Antonio Iannuzzi. 2017. "I principi generali del trattamento dei dati personali e i diritti dell'interessato." In C.C. Licia Califano (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, 85-136. Napoli: Editoriale scientifica.

Rodotà, Stefano. 1973. *Elaboratori elettronici e controllo*. Bologna: Il Mulino.

Ryngaert, Cedric, e Mistale Taylor. 2020. "The GDPR as Global Data Protection Regulation?." *AJIL Unbound* 114: 5-9.

Warren, Samuel D., e Louis D. Brandeis. 1890. "The Right to Privacy." *Harvard Law Review* 4, 5: 193-200.

Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: Public Affairs.

Le definizioni fondamentali

Chiara Angiolini

Abstract: The chapter analyses the main data protection definitions provided for by Reg. UE 2016/679, such as that of personal data, data subjects, data controllers and data processors. Furthermore, the intersections between EU Reg. 2016/679, Reg. 2022/868 and EU Reg. 2023/2854 are analysed with regard to basic definitions of Data Law.

Keywords: Data protection definitions, data subject, data processor, data controller, data protection officer, personal data

1. I dati personali

I dati personali sono definiti dall'art. 4, par. 1, n. 1 del Reg. UE 2016/679 (d'ora in avanti: GDPR) come «informazion[i] riguardant[i] una persona fisica identificata o identificabile "interessato"».

L'analisi della definizione si può scomporre in due parti, la prima, oggettiva, relativa alla nozione di 'informazione' e la seconda relativa al versante soggettivo e dunque al legame fra i dati e la persona che è descritta da tali dati.

Con riguardo alla nozione di informazione, in linea generale questa può indicare un processo, così come il suo risultato. Nel linguaggio normativo del GDPR la nozione di dati personali si basa prevalentemente sulla seconda accezione. Infatti, gli artt. 15 e 20 GDPR fanno riferimento al formato dei dati e il GDPR ne regola la conservazione, la cancellazione (art. 17), la richiesta di copia (art 15).

Questa impostazione, che guarda ai dati come risultati, rende possibile scinderli dall'interessato e da chi li ha raccolti e dunque dare loro un connotato di oggettività.

Considerare i dati come oggetti permette anche di dar conto di quelle ipotesi, sempre più frequenti, in cui i dati personali descrivono dei comportamenti che non riguardano un solo soggetto e delle relazioni, ma una collettività. Si pensi ad esempio alle informazioni circa l'età e il nome delle persone che hanno visualizzato un post di un utente di *Instagram,* ai dati relativi all'esistenza di un contratto fra due parti, o alle annotazioni di un esaminatore relative a una pro-

Chiara Angiolini, University of Siena, Italy, chiara.angiolini@unisi.it

Referee List (DOI 10.36253/fup_referee_list)
FUP Best Practice in Scholarly Publishing (DOI 10.36253/fup_best_practice)

va d'esame, personali sia rispetto al valutatore che al candidato (quest'ultima ipotesi è tratta da: CGUE, 20 dicembre 2017, C-434/16).

Sul piano normativo la definizione di dati personali crea un legame persistente fra tali dati e l'interessato. I profili più rilevanti sono due.

In primo luogo, la posizione dell'interessato non è tutelata soltanto perché i dati lo riguardano, per così dire, originariamente, ma anche in quanto sono utilizzati riferendoli a questi. A tal proposito il Gruppo di Lavoro Art. 29 ha affermato che se un impiego dei dati può avere un impatto sui diritti e gli interessi dell'interessato, questi sono da ritenere personali (Gruppo di Lavoro Art. 29, *Parere 4/2007 sul concetto di dati personali*).

A contrario, i dati c.d. «fittizi», utilizzati ad esempio come strumento per test informatici o a fini di ricerca, non sono dati personali, in quanto non descrivono una persona fisica identificata o identificabile ma una persona che non esiste (così CGUE, 5 dicembre 2023, C-683/21, § 55).

In secondo luogo, la connessione fra persona interessata e dati personali creata a livello normativo è resa particolarmente forte grazie al riferimento nella definizione giuridica di dati personali, non soltanto a una persona identificata, ma anche identificabile. La nozione di identificabilità assume sicura importanza nei contesti di trattamento massivo dei dati. Sul punto, il considerando 26 GDPR recita:

> Per stabilire l'identificabilità di una persona è opportuno considerare tutti i mezzi, come l'individuazione, di cui il titolare del trattamento o un terzo può ragionevolmente avvalersi per identificare detta persona fisica direttamente o indirettamente. 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.

È di particolare interesse qui il caso *Breyer,* nel quale la Corte di Giustizia dell'Unione Europea ha affermato che ai fini della qualificazione di un dato come personale non è necessario che tutte le informazioni che consentono di identificare la persona interessata «debbano essere in possesso di una sola persona» (CGUE, 19 ottobre 2016, C-582/14, §§ 43 ss.; si veda anche: CGUE, 9 novembre 2023, C-319/2022). Di recente la Corte di Giustizia dell'UE è ritornata sulla questione, affermando che la circostanza per cui un soggetto non acceda alle informazioni Y che, associate a quelle X, che tratta, permettono di identificare una persona fisica non esclude la qualificazione delle informazioni X trattate come dati personali (CGUE, 7 marzo 2024, C-604/22, §§ 38 ss.).

A fronte di tale orientamento, la sentenza della Corte di Giustizia dell'UE del 4 settembre 2025, C-413/23 P è di particolare rilevanza. In questa pronuncia la Corte assume una prospettiva soggettiva con riguardo alla definizione di dati personali, applicata in ragione delle informazioni disponibili per il titolare del trattamento. In particolare, con riguardo ai dati pseudonimizzati la Corte distingue, non sempre con un'argomentazione chiara, fra i soggetti che hanno accesso o possono aver accesso ai codici di identificazione o altre informazioni aggiuntive che permettano l'identificazione o l'identificabilità degli interessati, per cui i dati sono

personali, e i soggetti che hanno accesso ai soli dati pseudonimizzati, senza avere la possibilità di accesso ai codici di identificazione o ad altre informazioni aggiuntive che permettano l'identificazione o l'identificabilità degli interessati. Rispetto a tali ultimi soggetti, la Corte afferma che i dati non sono da considerare personali. L'impatto e l'interpretazione di tale pronuncia sono in discussione in dottrina.

La nozione di identificabilità è molto ampia e non definibile una volta per tutte, in quanto assume importanza il contesto di riferimento e lo sviluppo tecnologico, come emerge anche dalla lettura del considerando 26 GDPR già richiamato. È ben possibile quindi che un dato inizialmente anonimo divenga personale, in ragione del tipo di trattamento o dell'evoluzione della tecnologia (Purtova 2018).

Il procedimento inverso, l'anonimizzazione, è ritenuto sempre più difficile da ottenere in pratica: l'attuale tecnologia ha portato la comunità scientifica e poi anche il Gruppo di Lavoro Art. 29, a sottolineare la difficoltà di un'anonimizzazione sicura e dunque di avere certezza circa una definitiva trasformazione dei dati da personali ad anonimi, con il conseguente venir meno del legame, giuridicamente sancito, fra dati personali e interessato (Gruppo di Lavoro Art. 29, *Parere 5/2014 sulle tecniche di anonimizzazione,* 10 aprile 2014).

2. La persona interessata

La nozione di persona interessata è strettamente legata a quella di dato personale come risulta evidente dalla lettura dell'art. 4, par. 1, n. 1 GDPR, già citato in apertura del precedente paragrafo.

Infatti, i dati sono «personali» in quanto descrivono una persona fisica ed è proprio il legame, anche giuridico, fra dati e persona la ragione principale per la definizione di un regime *ad hoc*. In proposito, è stato da tempo mostrato che il trattamento dei dati personali permette di acquisire una conoscenza anche molto approfondita dell'interessato, modulata in base al punto di vista di chi raccoglie e tratta i dati. Tale conoscenza risulta utile a vari fini e la letteratura ha a più riprese sottolineato come questa fondi un potere capace di incidere sulle relazioni di cui l'interessato è parte (Rodotà 1995; Zuboff 2019). In una prospettiva giuridica, i trattamenti possono incidere sulla sfera della personalità e delle relazioni dell'interessato, ed è questa una delle ragioni per cui i dati personali sono utili a vari fini, anche profittevoli.

Una questione giuridica si pone rispetto ai diritti delle persone decedute su cui si rinvia al relativo box nel capitolo *I diritti dell'interessato*.

3. Il trattamento

Il trattamento dei dati personali, secondo quanto previsto dall'art. 4, par. 1, n. 2 GDPR, è:

> 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'a-

> dattamento 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.

L'ampiezza di questa definizione, che include un elenco non tassativo di operazioni (così CGUE, 7 marzo 2024, C-740/20) contribuisce a garantire un'applicazione estesa della disciplina in materia di trattamento dei dati personali, funzionale alla tutela del diritto fondamentale alla protezione dei dati personali di cui all'art. 8 CDFUE (così CGUE, 5 ottobre 2023, C-659/22, §§ 27-28; v. anche CGUE, 5 ottobre 2023, C-659/22; sull'art. 8 CDFUE v. cap. *Le fonti della disciplina in materia di dati personali*).

A titolo di esempio, far comparire su una pagina Internet dati personali è da considerare come un'operazione di trattamento (CGUE, 6 novembre 2003, C-101/01, § 25), anche quando riguardano informazioni già pubblicate nei media tali e quali (CGUE, 13 maggio 2014, C-131/12, § 30). Ancora, la CGUE qualifica come trattamento la comunicazione orale di dati personali (CGUE, 7 marzo 2024, C-740/20)

Alcune operazioni di trattamento, come la raccolta e la conservazione, hanno regole peculiari, dovute alla loro specificità rispetto all'uso dei dati personali. Infatti, la raccolta è l'operazione che permette di creare i dati personali come un oggetto, anche giuridico, distinto dall'interessato, e la conservazione rende possibili ulteriori usi dei dati personali (Angiolini 2020).

Altri tipi di trattamenti si distinguono in ragione delle modalità, anche tecniche. Un esempio è quello della profilazione, che è definita dall'art. 4, par. 1, n. 4 GDPR come:

> qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica.

La profilazione porta con sé alcuni rischi, legati alla mancata trasparenza delle tecniche usate per attuarla e alle conseguenze per gli interessati e può avere effetti discriminatori (Gruppo di Lavoro Art. 29, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del Reg. UE 2016/679,* 6 febbraio 2018). E per questo ad essa si applicano anche particolari norme, come l'art. 22 GDPR, rubricato «processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione» (v. cap. *I diritti dell'interessato*).

4. Le categorie particolari di dati personali

L'art. 9 GDPR detta un regime specifico per le «categorie particolari di dati personali» (v. cap. *La disciplina dell'attività di trattamento*). Questi dati sono denominati anche 'sensibili' in quanto il loro trattamento può avere conseguenze significative rispetto alle libertà e ai diritti fondamentali dell'interessato (si vedano in proposito: il considerando 51 GDPR e le seguenti pronunce della Corte

di Giustizia dell'UE CGUE, 4 luglio 2023, C-252/21, spec. §§ 66 ss.; CGUE, 21 dicembre 2023, C-667/21, spec. §§ 37 ss.).

Le categorie particolari di dati personali sono descritte dal par. 1 dell'art. 9 GDPR, come quelle relative a quei dati che:

> rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché [...] 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.

Tale elenco va letto congiuntamente all'art. 4, par. 1 nn. 13, 14 e 15 GDPR, che definisce i dati relativi alla salute, i dati genetici e i dati biometrici.

I dati relativi alla salute sono definiti come «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».

Rispetto alla definizione di tale categoria di dati, la Corte di Giustizia dell'UE ha affermato che l'espressione «dati relativi alla salute» deve essere interpretata in modo ampio, «in modo da includere informazioni relative a tutti gli aspetti, sia fisici che mentali, della salute di un individuo» (CGUE 6 novembre 2003, C-101/01; cfr., altresì, CGUE, 4 ottobre 2024, C-21/23, secondo la quale nel caso in cui il gestore di una farmacia commercializzi, tramite una piattaforma online, medicinali la cui vendita è riservata alle farmacie, le informazioni che i clienti di tale gestore inseriscono al momento dell'ordine online dei medicinali, quali il loro nome, l'indirizzo di consegna e gli elementi necessari all'individualizzazione dei medicinali, costituiscono dati relativi alla salute anche qualora la vendita di tali medicinali non sia soggetta a prescrizione medica).

Nella stessa ottica, il Comitato Europeo per la Protezione dei Dati (d'ora in avanti: EDPB) ha ritenuto che i dati relativi alla salute possono essere ricavati da fonti diverse; ad esempio, possono essere raccolti da un operatore sanitario nel corso di una visita di controllo o in una cartella clinica o ancora vi possono essere dati che, mediante riferimenti incrociati con altri dati, divengono «relativi alla salute» in quanto rivelano lo stato di salute o i rischi per la salute (EDPB, *Linee guida 03/2020 sul trattamento dei dati relativi alla salute a fini di ricerca scientifica nel contesto dell'emergenza legata al COVID-19*, 21 aprile 2020).

Poi, sono considerati dati genetici *ex* art. 4, par. 1, n. 13:

> 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 [si veda anche il considerando 34 del Reg. Ue 2016/679].

La peculiarità di tali dati è che possono riguardare più persone, come riconosciuto dalla Corte Europea dei Diritti dell'Uomo nella causa *Marper c. Regno Unito*, del 4 dicembre 2008, ric. n. 30562/04 e 30566/04.

A questo proposito, il Gruppo di lavoro art. 29 (ora sostituito dall'EDPB v. cap. *La regolamentazione e la tutela amministrativa*) nel suo documento di lavoro sui dati genetici, adottato il 17 marzo 2004, ha affermato che:

> se da un lato le informazioni genetiche sono uniche e distinguono un individuo da altri individui, dall'altro possono anche rivelare informazioni e avere implicazioni per i parenti di sangue di quell'individuo (famiglia biologica), compresi quelli delle generazioni successive e precedenti. Inoltre, i dati genetici possono caratterizzare un gruppo di persone (ad esempio, comunità etniche).

I dati genetici sono una categoria di dati che mostra la complessità della dimensione individuale e collettiva dei dati e della protezione della salute: questi dati possono riguardare più persone e il loro trattamento può essere necessario per proteggere la salute di una o di molte di esse.

I dati biometrici sono definiti dall'art. 4, par. 1, n. 14 GDPR come

> i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.

Dunque, ai sensi dell'art. 4, par. 1, n. 14 GDPR i dati biometrici sono generati attraverso l'uso di tecnologie specifiche che elaborano le caratteristiche degli individui per identificare (identificazione biometrica) o confermare (verifica biometrica) l'identità della persona interessata.

Nel leggere congiuntamente l'art. 4, par. 1, n. 14 e l'art. 9 GDPR emerge una questione interpretativa, discussa in dottrina; il regime, più rigoroso, definito dall'art. 9 GDPR relativo alle categorie particolari di dati personali (su cui v. cap. *Le definizioni fondamentali*) si applica anche a quei dati biometrici che non sono utilizzati per identificare in modo univoco una persona?

Dal punto di vista degli indici normativi, il nodo interpretativo sorge in quanto l'art. 9 GDPR fa riferimento ai «dati biometrici intesi a identificare in modo univoco una persona fisica», mentre l'art. 4 GDPR si riferisce ai dati che «ne consentono o confermano l'identificazione univoca».

L'interrogativo a cui rispondere è dunque se vi siano dati biometrici ai sensi dell'art. 4 GDPR che non siano però sottoposti al regime di cui all'art. 9 GDPR in quanto non sono, in concreto, trattati al fine di identificare in modo univoco una persona fisica.

La soluzione di tale questione interpretativa è in discussione. Infatti, se gli indici normativi non escludono *a priori* la possibilità di individuare dati biometrici *ex* art. 4 GDPR che non rientrino nelle categorie particolari di dati personali, d'altro canto da più parti si è notato che a prescindere dallo scopo per cui un dato biometrico viene utilizzato, le caratteristiche che possono essere estratte da esso mantengono un notevole potenziale per consentire l'identificazione delle persone o per influenzarle negativamente (European Union Agency for Fundamental Rights 2020, 8). Tali ultime considerazioni mostrano i rischi di una lettura restrittiva dell'art. 9 GDPR, e la necessità di interpretare le norme in materia di protezione dei dati personali alla luce della Carta dei Diritti Fondamentali dell'UE.

A fronte di una pluralità di interpretazioni dottrinali, nel contesto italiano è esemplificativa la pronuncia della Corte di Cassazione del 13 maggio 2024, n.

12967, dove la Corte, naturalmente anche in ragione del caso concreto che le era sottoposto, ha enunciato il seguente principio di diritto:

> In tema di trattamento dei dati personali, ai sensi dell'art. 9 del Reg (UE) 2016/679, ricorre un trattamento di dati biometrici, come definiti dall'art. 4, n. 14 del Regolamento 2016/679, quando i dati personali sono ottenuti mediante un trattamento tecnico automatizzato specifico, realizzato con un software che, sulla base di riprese e analisi delle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica, le elabora, evidenziando comportamenti o elementi anomali, e che perviene a un esito conclusivo, costituito da una elaborato video/foto che consente (o che conferma) l'identificazione univoca della persona fisica, restando irrilevante la circostanza che l'esito finale del trattamento sia successivamente sottoposto alla verifica finale di una persona fisica.

5. Il titolare del trattamento e la contitolarità

Il titolare del trattamento, secondo quanto prevede l'art. 4, par. 1, n. 7 GDPR è:

> la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.

Dunque, sono principalmente due gli elementi che definiscono la figura del titolare: la determinazione dei mezzi e delle finalità del trattamento.

Occorre sottolineare che la qualifica di titolare del trattamento non dipende dalla volontà di chi tratta i dati ma dal ruolo che questi assume rispetto alla pianificazione del trattamento; con un esempio, sarà possibile scegliere se determinare finalità e mezzi del trattamento, ma una volta che si sia scelto questo assetto, non ci si potrà sottrarre alla qualificazione di titolare del trattamento.

La *ratio* di tale scelta legislativa è chiara: al soggetto che ha un ruolo molto significativo nell'organizzazione del trattamento sono anche attribuiti specifici obblighi (v. anche il considerando 74 GDPR), come quello relativo all'informativa di cui agli artt. 13 e 14 GDPR, e responsabilità, regolate anche dall'art. 82 GDPR (su cui v. il cap. *Il risarcimento del danno da illecito trattamento dei dati personali*).

Guardando alla giurisprudenza, la nozione di titolare del trattamento è stata interpretata in senso estensivo dalla Corte di Giustizia dell'UE, secondo cui

> qualsiasi persona fisica o giuridica che influisca, per fini che le sono propri, sul trattamento di tali dati e partecipi pertanto alla determinazione delle finalità e dei mezzi di tale trattamento può essere considerata titolare di detto trattamento. A tal riguardo, non è necessario che le finalità e i mezzi del trattamento siano determinati mediante orientamenti scritti o istruzioni da parte del titolare del trattamento […], né che quest'ultimo sia stato formalmente designato come tale. (CGUE, C-683/21, 5 dicembre 2023, *Nacionalinis Visuomenės Sveikatos Centras*, § 30)

Con riguardo alle ipotesi in cui la determinazione delle finalità e dei mezzi del trattamento sia fatta dal diritto nazionale, la Corte di Giustizia dell'UE ha affermato che la designazione del titolare da parte del diritto nazionale può essere anche implicita, purché «derivi in maniera sufficientemente certa dal ruolo, dalla funzione e dalle attribuzioni devoluti alla persona o all'entità» (CGUE, 11 gennaio 2024, C-231/22, § 30).

Quando più soggetti determinano congiuntamente i mezzi e le finalità del trattamento, questi sono contitolari. Una questione interpretativa significativa riguarda la definizione dei confini entro cui i mezzi o le finalità del trattamento sono determinati congiuntamente.

In proposito, la Corte di Giustizia dell'UE ha affermato che vi può essere una contitolarità anche se i ruoli dei contitolari sono diversi, tanto che non è necessario che tutti i contitolari abbiano accesso ai dati (CGUE, 10 luglio 2018, C-25/17, § 69; così anche CGUE, 7 marzo 2024, C-604/22). Si legge nella pronuncia CGUE, 5 dicembre 2023, C-683/21, che

> la partecipazione alla determinazione delle finalità e dei mezzi del trattamento può assumere forme diverse, potendo tale partecipazione risultare sia da una decisione comune adottata da due o più soggetti sia da decisioni convergenti di tali soggetti. Orbene, in quest'ultimo caso, dette decisioni devono integrarsi, di modo che ciascuna di esse abbia un effetto concreto sulla determinazione delle finalità e dei mezzi del trattamento. (CGUE, 5 dicembre 2023, C-683/21, *Nacionalinis Visuomenės Sveikatos Centras*, § 43; si vedano anche: 5 giugno 2018, C-210/16, *Wirtschaftsakademie Schleswig-Holstein*; 29 luglio 2019, *Fashion ID*, C-40/17, 10 luglio 2018, *Jehovan todistajat*, C-25/17; CEPD, *Linee guida 7/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR*).

Ancora, a più riprese la Corte di Giustizia ha affermato che i contitolari possono non avere una responsabilità equivalente quando sono coinvolti in fasi diverse del trattamento e con differenti modalità (CGUE, 5 dicembre 2023, C-683/21, § 43; CGUE 5 giugno 2018, C-210/16).

L'art. 26 GDPR prevede alcuni obblighi in capo ai contitolari del trattamento. In particolare, i contitolari devono stabilire

> in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14, [...].
> 2. L'accordo di cui al paragrafo 1 riflette adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati. Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato.

L'art. 26, par. 3 GDPR prevede inoltre che l'interessato possa comunque esercitare i diritti previsti dall'GDPR verso ciascun titolare del trattamento.

Qualora i contitolari violino l'accordo di contitolarità secondo la più recente giurisprudenza della Corte di Giustizia dell'UE, vi sarà una violazione del GDPR che non comporta un trattamento illecito di dati personali, in quanto l'art. 26

GDPR non è parte del gruppo di norme, riunite attorno all'art. 6 GDPR rubricato «liceità del trattamento» che concorrono a determinare la liceità di un trattamento (CGUE, 4 maggio 2023, C-60/22).

Dunque, i rimedi per reagire a tale violazione andranno individuati nei poteri correttivi delle autorità di controllo (*ex* art. 58 par. 2, GDPR), nella proposizione di un reclamo all'autorità di controllo (art. 77, par. 1, GDPR) e nel risarcimento del danno eventualmente cagionato dal titolare del trattamento *ex* art. 82 GDPR (così CGUE, 4 maggio 2023, C-60/22).

6. Il responsabile del trattamento

Il responsabile del trattamento è definito dall'art. 4, par. 1, n. 8 GDPR come: «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento».

Dal punto di vista soggettivo, il responsabile è soggetto distinto dal titolare e non sono posti limiti particolari alla natura del soggetto che può essere nominato come responsabile, e può dunque essere una persona fisica, una persona giuridica, un'autorità pubblica, o un ente.

L'elemento che connota la figura del responsabile è che questi tratta i dati *per conto* del titolare da parte del responsabile, come risulta evidente anche dalla lettura dell'art. 28 GDPR, rubricato 'Responsabile del trattamento', su cui si tornerà (v. cap. 7 *La regolamentazione di diversi rapporti che riguardano i dati personali*), e il cui par. 2, lett. a) prevede che il responsabile tratti i dati personali «soltanto su istruzione documentata del titolare del trattamento», salve alcune eccezioni.

Proprio perché il responsabile del trattamento tratta i dati personali per conto del titolare, fra i suoi obblighi vi sono l'adozione delle misure che garantiscano la sicurezza del trattamento *ex* art. 32 GDPR e quello di assistere il titolare nel garantire la sicurezza del trattamento e nel dare seguito alle richieste per l'esercizio dei diritti dell'interessato (su cui v. cap. *I diritti dell'interessato*).

7. Il responsabile della protezione dei dati

Il responsabile per la protezione dei dati è una figura disciplinata dagli articoli da 37 a 39 del GDPR, che deve avere, ex art. 37, par. 5 GDPR, una conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati.

Secondo quanto previsto dall'art. 39 RGDP, il responsabile della protezione dei dati deve:

a) informare e fornire consulenza al titolare o al responsabile del trattamento rispetto agli obblighi derivanti dalla legislazione in materia di protezione dei dati;
b) sorvegliare l'osservanza della legislazione sulla protezione dei dati;
c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35 GDPR;
d) cooperare con l'autorità di controllo e fungere da punto di contatto per tale autorità per questioni connesse al trattamento.

L'art. 38 GDPR prevede alcune regole specifiche che concernono il rapporto fra il responsabile per la protezione dei dati e il titolare o il responsabile che lo designa.

In primo luogo, il responsabile per la protezione dei dati deve essere «tempestivamente e adeguatamente» coinvolto in tutte le questioni riguardanti la protezione dei dati personali e deve essere messo in condizioni di assolvere i propri compiti e dunque anche di accedere ai dati personali e ai trattamenti.

In secondo luogo, il titolare e il responsabile del trattamento si devono assicurare che il responsabile della protezione dei dati non riceva alcuna istruzione per quanto riguarda l'esecuzione dei suoi compiti, e non possono rimuoverlo o penalizzarlo per l'esecuzione dei suoi compiti.

Inoltre, il responsabile della protezione dei dati riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento, ed è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti.

Infine, gli interessati possono contattare il responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal presente regolamento.

Non sempre il titolare e il responsabile del trattamento sono obbligati a nominare un responsabile per la protezione dei dati.

Secondo quanto dispone l'art. 37 GDPR il titolare del trattamento e il responsabile del trattamento devono designare il responsabile per la protezione dei dati nei seguenti casi:

> 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 o di dati relativi a condanne penali e a reati di cui all'articolo 10.

Nelle altre ipotesi – e ove non sia previsto l'obbligo di nomina da altri atti normativi – i titolari del trattamento e i responsabili del trattamento *possono* designare tale figura.

Rispetto alla figura del Responsabile della Protezione dei Dati si possono menzionare il *Documento di indirizzo su designazione, posizione e compiti del Responsabile della protezione dei dati (RPD) in ambito pubblico*, adottato dal Garante per la Protezione dei Dati nel 2021 e *le Linee guida sui responsabili della protezione dei dati, nella versione adottata in data 5 aprile 2017 dal Gruppo di Lavoro Art. 29*, oggetto dell'*Endorsement 1/2018* del Comitato Europeo per la Protezione dei Dati (EDPB), documenti utili anche rispetto all'attività che in concreto svolgono i Responsabili della Protezione dei Dati.

8. Le definizioni nel Regolamento 2022/868 sulla governance dei dati e nel Regolamento 2023/2854 sui dati e il coordinamento con il GDPR

Oltre alle definizioni previste dal GDPR di cui ci si è occupati nei paragrafi precedenti, occorre considerare anche le nozioni introdotte con il Regolamento sulla governance dei dati n. 2022/868 del 30 maggio 2022 (d'ora in avanti: *Data Governance Act*) e il Regolamento sui dati n. 2023/2854, del 13 dicembre 2023 (d'ora in avanti *Data Act*).

Entrambi i regolamenti prevedono delle definizioni e una norma relativa al rapporto con il GDPR.

In particolare, l'art. 1 del *Data Governance Act* prevede che:

> 3. Il diritto dell'Unione e nazionale in materia di protezione dei dati personali si applica a qualsiasi dato personale trattato in relazione al presente regolamento. In particolare, il presente regolamento non pregiudica i regolamenti (UE) 2016/679 e (UE) 2018/1725 e le direttive 2002/58/CE e (UE) 2016/680, anche per quando riguarda i poteri e le competenze delle autorità di controllo. In caso di conflitto tra il presente regolamento e il diritto dell'Unione in materia di protezione dei dati personali o il diritto nazionale adottato conformemente a tale diritto dell'Unione, prevale il pertinente diritto dell'Unione o nazionale in materia di protezione dei dati personali. Il presente regolamento non crea una base giuridica per il trattamento dei dati personali e non influisce sui diritti e sugli obblighi di cui ai regolamenti (UE) 2016/679 e (UE) 2018/1725 o alle direttive 2002/58/CE o (UE) 2016/680.

L'art. 1 par. 5 del *Data Act* prevede che:

> 5. Il presente regolamento fa salvo il diritto dell'Unione e nazionale in materia di protezione dei dati personali, della vita privata e della riservatezza delle comunicazioni e dell'integrità delle apparecchiature terminali, che si applica ai dati personali trattati in relazione ai diritti e agli obblighi, in particolare i regolamenti (UE) 2016/679 e (UE) 2018/1725 e la direttiva 2002/58/CE, nonché i poteri e le competenze delle autorità di controllo e i diritti degli interessati. Nella misura in cui gli utenti sono gli interessati, i diritti di cui al capo II del presente regolamento integrano i diritti di accesso da parte degli interessati e i diritti alla portabilità dei dati di cui agli articoli 15 e 20 del regolamento (UE) 2016/679. In caso di conflitto tra il presente regolamento e il diritto dell'Unione in materia di protezione dei dati personali o della vita privata o la legislazione nazionale adottata conformemente a tale diritto dell'Unione, prevale il pertinente diritto dell'Unione o nazionale in materia di protezione dei dati personali o della vita privata.

Dunque, qualora vi sia un conflitto fra una norma dei due regolamenti appena citati e il GDPR, prevarrà quest'ultimo. Questa regola è di particolare importanza in quanto diviene un criterio ermeneutico per l'interprete che deve coordinare i testi normativi ai fini della loro applicazione.

Tale criterio risulta utile anche in relazione alle definizioni previste dall'art. 2 del *Data Act* e dall'art. 2 del *Data Governance Act*, in quanto alcune di queste devono essere coordinate con quelle previste dal GDPR.

In particolare, sia il *Data Governance Act* che il *Data Act* all'art. 2, par. 1 prevedono la seguente definizione di «dati»: «qualsiasi rappresentazione digitale di atti, fatti o informazioni e qualsiasi raccolta di tali atti, fatti o informazioni, anche sotto forma di registrazione sonora, visiva o audiovisiva».

A tale definizione segue quella di dati personali (art. 2, par. 1, n. 3, sia del *Data Governance Act*, sia del *Data Act*), che rinvia a quella data dall'art. 4, par. 1, n. 1, GDPR (v. in questo capitolo il § 3), e la definizione di dati non personali, che vengono descritti come «i dati diversi dai dati personali».

Alcune altre nozioni, come quella di consenso nell'art. 2, par. 1, n. 5 del *Data Governance Act* e quella di interessato (art 2, par. 1, n. 11 *Data Act*; art 2, par. 1, n. 7 *Data Governance Act*) rinviano espressamente alle relative definizioni previste dal GDPR.

Rispetto invece alle qualificazioni di chi tratta i dati, non vi è corrispondenza fra il GDPR e i nuovi regolamenti. Di seguito è tracciato un quadro delle principali definizioni rilevanti nel contesto di questo manuale.

8.1. La definizione dei soggetti

Gli elementi di differenza fra le definizioni date dai due regolamenti ben si colgono attraverso il loro raffronto nella tabella che segue.

	Art. 2 del *Data Governance Act*	Art. 2 del *Data Act*
Titolare dei dati	Una persona giuridica, compresi gli enti pubblici e le organizzazioni internazionali, o una persona fisica che non è l'interessato rispetto agli specifici dati in questione e che, conformemente al diritto dell'Unione o nazionale applicabile, ha il diritto di concedere l'accesso a determinati dati personali o dati non personali o di condividerli (n. 8)	Una persona fisica o giuridica che ha il diritto o l'obbligo, conformemente al presente regolamento, al diritto applicabile dell'Unione o alla legislazione nazionale adottata conformemente al diritto dell'Unione, di utilizzare e mettere a disposizione dati, compresi, se concordato contrattualmente, dati del prodotto o di un servizio correlato che ha reperito o generato nel corso della fornitura di un servizio correlato (n. 13)
Utente dei dati	Una persona fisica o giuridica che ha accesso legittimo a determinati dati personali o non personali e che *ha diritto*, anche a norma del GDPR in caso di dati personali, *a utilizzare tali dati a fini commerciali o non commerciali* (n. 9)	La definizione non è presente nel *Data Act*.
Utente	La definizione non è presente nel *Data Governance Act*.	Una persona fisica o giuridica che possiede un prodotto connesso o a cui sono stati trasferiti contrattualmente diritti temporanei di utilizzo di tale prodotto connesso o che riceve un servizio correlato (12)

	Art. 2 del *Data Governance Act*	Art. 2 del *Data Act*
Destinatario dei dati	La definizione non è presente nel *Data Governance Act*.	Una persona fisica o giuridica, che agisce per fini connessi alla sua attività commerciale, imprenditoriale, artigianale o professionale, diversa dall'utente di un prodotto connesso o di un servizio correlato, a disposizione della quale il titolare dei dati mette i dati, e che può essere un terzo in seguito a una richiesta da parte dell'utente al titolare dei dati o conformemente a un obbligo giuridico ai sensi del diritto dell'Unione o della legislazione nazionale adottata conformemente al diritto dell'Unione (14)

La tabella mostra infatti che alcune nozioni presenti nel *Data Act* non trovano una corrispondenza nel *Data Governance Act*. Seppur tale circostanza si può in linea generale spiegare in ragione della diversità delle funzioni e dell'oggetto della disciplina dettata dai due regolamenti, di certo non facilita lo sviluppo di un quadro sistematico chiaro e comune all'ambito del «diritto dei dati».

Un particolare elemento di criticità è la previsione di due definizioni diverse per la medesima nozione di «titolare dei dati» (in senso critico si veda anche EDPB-GEPD, *Parere congiunto EDPB-GEPD 2/2022 sulla proposta del Parlamento europeo e del Consiglio riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo*, 4 maggio 2022). Infatti, la coesistenza di due diverse definizioni della stessa nozione, all'interno della stessa materia e nella medesima area legislativa rende ancora più evidente la difficoltà nella costruzione di un sistema coerente all'interno del «diritto dei dati» e suggerisce una modifica legislativa che permetta un uso il più possibile univoco delle nozioni.

Inoltre, dal punto di vista del coordinamento fra il GDPR da una parte e *il Data Act* e il *Data Governance Act* dall'altra, si deve sottolineare che, come già ricordato in apertura di questo paragrafo, i recenti regolamenti non pregiudicano l'applicazione del GDPR.

Di conseguenza, quando i dati sono personali, è il GDPR che ne definisce lo statuto di base, e cioè i limiti del loro lecito trattamento, e dunque che in sostanza delinea anche i diritti di utilizzo e di circolazione alla base delle definizioni di «titolare dei dati» e «utente dei dati».

Rimane comunque un profilo critico, che corrisponde ad una discussione aperta in dottrina, legato alla qualificazione della situazione giuridica soggettiva di chi tratta i dati come «diritto» sia nel *Data Act* che nel *Data Governance Act*, qualificazione che non è per nulla scontata rispetto alla situazione giuridica soggettiva del titolare del trattamento che, se ricorrono le condizioni previste dalla disciplina in materia di protezione dei dati personali, può lecitamente trattare i dati personali su cui ha accesso, ma che, qualora non abbia accesso a dati personali non ha diritto – salvo che sia espressamente previsto da una norma di legge (v. cap. 6, *Le intersezioni fra disciplina in materia di dati personali e diritto dei consumatori*) – di ottenere tale accesso ai dati (Angiolini 2025).

Riferimenti bibliografici

Angiolini, Chiara. 2025. "Titolari dei dati, utenti, destinatari dei dati: ambito soggettivo di applicazione." In Bachelet, Vittorio, Gianluigi Marino e Antonio Racano (a cura di). *Accesso equo ai dati e loro utilizzo: profili sistematici e applicativi nell'orizzonte del diritto privato*. Wolters Kluwer.

Cerrina Feroni, Ginevra. 2025. "Data Act, accesso e riuso dei dati: quali sfide per la protezione dei dati personali?." In Morace Pinelli, Arnaldo (a cura di), *Data Act. Introduzione interdisciplinare e commentario al Regolamento (UE) 2023/2854*. Pisa: Pacini.

Kuner, Christopher, Bygrave Lee A, Docksey, Christopher, Drechsler, Laura. (a cura di). 2020. *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford: Oxford University Press.

Martial-Braz, Nathalie, Rochfeld, Judith (a cura di). 2019. *Droit des données personnelles. Les spécificités du droit français au regard du RGPD*. Paris: Dalloz.

European Union Agency for Fundamental Rights. 2020. *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law (ultima consultazione: aprile 2025).

Purtova, Nadezhda. 2018. "The law of everything. Broad concept of personal data and future of EU data protection law." *International Review of Law, Computers & Technology* 28, 2: 40-81.

Rodotà, Stefano. 1995. *Tecnologie e diritti*. Bologna: Il Mulino.

Zuboff, Shoshana. 2019. *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*. Roma: Luiss University Press.

La disciplina dell'attività di trattamento

Chiara Angiolini, Antonello Iuliani[1]

Abstract: The first section of the chapter illustrates the legal bases for processing personal data and exceptions to the prohibition of processing special categories of personal data. In the second section, the principles governing data processing are analyzed through a systematic and structured legal framework. In the last section, rules on data breach are analysed showing the relevance of EDPB guidelines on this subject.

Keywords: Principles relating to processing of personal data, rules on data breach

Sez. I. Le basi giuridiche del trattamento

1. Le basi giuridiche del trattamento dei dati personali

Il trattamento dei dati personali può essere svolto lecitamente se si fonda su una base giuridica del trattamento. Tali basi giuridiche sono previste dal Reg. UE 2016/679 (d'ora in avanti: GDPR) all'art. 6 che, nell'interpretazione della Corte di Giustizia dell'UE "prevede un elenco esaustivo e tassativo dei casi nei quali un trattamento di dati personali può essere considerato lecito" (CGUE, 9 gennaio 2025, C-394/23, § 25; così anche CGUE, 4 ottobre 2024, C-621/22, § 29, CGUE, 4 luglio 2023, C-252/21 § 90, CGUE, 22 giugno 2021, C-439/19, § 99). In particolare, l'art. 6 GDPR prevede le seguenti basi giuridiche:

[1] Chiara Angiolini ha scritto la prima sezione del presente capitolo, Antonello Iuliani la seconda e la terza.

Chiara Angiolini, University of Siena, Italy, chiara.angiolini@unisi.it
Antonello Iuliani, Università digitale Pegaso, Italy, antonello.iuliani@unipegaso.it, 0000-0001-9931-6934

Referee List (DOI 10.36253/fup_referee_list)
FUP Best Practice in Scholarly Publishing (DOI 10.36253/fup_best_practice)

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.

Con riguardo all'interpretazione dell'art. 6, par. 1, GDPR è di particolare interesse l'orientamento della Corte di Giustizia dell'UE secondo cui le basi giuridiche previste dalla lett. b) alla lett. f) sono da interpretare restrittivamente "nella misura in cui consentono di rendere lecito un trattamento di dati personali effettuato in assenza del consenso dell'interessato" (CGUE, 9 gennaio 2025, C-394/23, § 27; così anche CGUE, 4 ottobre 2024, C-621/22; CGUE, 4 luglio 2023, C-252/21, § 93)

Inoltre, la CGUE ha affermato che il requisito della necessità previsto nelle basi giuridiche da b) ad f) dell'art. 6, par. 1, GDPR

> non è soddisfatto quando l'obiettivo perseguito da tale trattamento di dati potrebbe ragionevolmente essere raggiunto in modo altrettanto efficace mediante altri mezzi meno pregiudizievoli per i diritti fondamentali degli interessati, in particolare per i diritti al rispetto della vita privata e alla protezione dei dati personali garantiti agli articoli 7 e 8 della Carta, atteso che le deroghe e le restrizioni al principio della protezione di tali dati devono avere luogo nei limiti dello stretto necessario.

2. *Segue*. Il consenso dell'interessato

La disciplina della base giuridica del consenso al trattamento è frutto della lettura sistematica di varie norme, e *in primis* dell'art. 6, par. 1, lett. a), dell'art. 4 e dell'art. 7 GDPR.

L'art. 6, par. 1, lett. a) GDPR prevede che il consenso al trattamento dei dati personali per una o più specifiche finalità sia una base giuridica del trattamento. L'art. 7 GDPR chiarisce che se il trattamento è fondato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato l'ha validamente prestato.

Il consenso al trattamento è strumento che attribuisce all'interessato un ruolo nella determinazione della possibilità e delle finalità del trattamento, e può essere letto come esercizio del diritto alla riservatezza e tecnica di tutela e partecipazione dell'interessato rispetto alla costruzione del regime dei dati personali, e dunque espressione dell'art. 8 CDFUE che sancisce il diritto alla protezione dei dati personali, e che infatti ne fa menzione (sull'art. 8 CDFUE, v. cap. *Le fonti della disciplina in materia di dati personali*).

La riflessione sul ruolo e sulla qualificazione del consenso al trattamento è stata per lungo tempo la chiave di volta del sistema della disciplina dei dati personali (Caggia 2019). È qui sufficiente dire che il consenso è un atto di autonomia privata, attraverso cui l'interessato esercita il diritto alla vita privata e alla protezione dei dati personali (Resta 2000, 307).

Una definizione generale di consenso al trattamento è data dall'art. 4, par. 1, n. 11 GDPR, ed è la seguente:

> «consenso dell'interessato»: 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;

Dunque, il consenso al trattamento per fondare validamente il trattamento deve essere: i) libero; ii) informato; iii) specifico, in particolare con riguardo alle finalità; iv) prestato attraverso una dichiarazione o un'azione positiva inequivocabile.

Con riguardo alle forme di prestazione del consenso, occorre aggiungere che l'art. 7 GDPR dispone che se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso deve essere presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Inoltre, l'articolo appena richiamato prevede che nessuna parte di una tale dichiarazione che costituisce una violazione del GDPR può essere ritenuta vincolante.

Di sicura importanza sono poi le norme che attengono alla libertà del consenso, che conferiscono rilevanza alle circostanze in cui questo è prestato. In proposito, secondo l'art. 7 GDPR, nel valutare se il consenso sia stato liberamente prestato, si deve tenere 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.

Ancora, l'articolo appena richiamato disciplina la revoca del consenso, che può essere letta come lo specchio della sua libertà. Infatti, l'art. 7 GDPR sancisce il diritto dell'interessato a revocare il proprio consenso in qualsiasi momento, con la stessa facilità con cui l'ha prestato. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca e prima di esprimere il proprio consenso, e l'interessato deve essere informato di tale aspetto.

Ancora in tema di libertà del consenso, i considerando 42 e 43 GDPR recitano:

> (42) [...] Il consenso non dovrebbe essere considerato liberamente espresso se l'interessato non è in grado di operare una scelta autenticamente libera o è nell'impossibilità di rifiutare o revocare il consenso senza subire pregiudizio.
> (43) Per assicurare la libertà di espressione del consenso, è opportuno che il consenso non costituisca un valido presupposto per il trattamento dei dati personali in un caso specifico, qualora esista un evidente squilibrio tra l'interessato e il titolare del trattamento, specie quando il titolare del trattamento è un'autorità pubblica e ciò rende pertanto improbabile che il consenso sia stato espresso liberamente in tutte

> le circostanze di tale situazione specifica. Si presume che il consenso non sia stato liberamente espresso se non è possibile esprimere un consenso separato a distinti trattamenti di dati personali, nonostante sia appropriato nel singolo caso, o se l'esecuzione di un contratto, compresa la prestazione di un servizio, è subordinata al consenso sebbene esso non sia necessario per tale esecuzione.

Anche alla luce di quanto si legge nel considerando 43 GDPR, si può affermare l'esistenza di una presunzione di non libera espressione del consenso quando non sia possibile prestarlo separatamente per distinti trattamenti di dati personali, nonostante sia appropriato nel singolo caso, o qualora l'esecuzione di un contratto, compresa la prestazione di un servizio, sia subordinata al consenso sebbene esso non sia necessario per tale esecuzione. L'onere della prova è in capo al titolare del trattamento, come confermato dalla Corte di Giustizia (CGUE, 11 novembre 2020, C-61/19) e ritenuto dal Comitato Europeo per la Protezione dei Dati (d'ora in avanti: EDPB) nelle linee guida in materia di consenso (EDPB, *Linee guida 5/2020 sul consenso ai sensi del regolamento (UE) 2016/679*, 4 maggio 2020, p. 11).

L'interpretazione del requisito della libertà del consenso è dibattuta in dottrina e in giurisprudenza, in particolare con riguardo alle ipotesi in cui il consenso e l'ottenimento di una prestazione da parte dell'interessato sono correlate.

In proposito, il Comitato Europeo per la Protezione dei Dati ritiene eccezionali i casi in cui il consenso è da considerare libero anche se l'esecuzione del contratto è subordinata alla sua prestazione (EDPB, *Linee guida 5/2020 sul consenso ai sensi del regolamento (UE) 2016/679,* 4 maggio 2020). Inoltre, secondo tali linee guida, la prova della libertà del consenso potrà essere data dimostrando che il titolare del trattamento offre, oltre a un servizio subordinato alla prestazione del consenso, anche un altro servizio effettivamente equivalente e non «condizionato».

In questo senso si è espressa anche la Corte di Giustizia (CGUE, 4 luglio 2023, C-252/21), secondo cui gli interessati devono disporre della libertà di rifiutare di prestare il loro consenso a operazioni particolari di trattamento di dati non necessarie all'esecuzione del contratto d'uso del social network (com'è la profilazione per finalità di personalizzazione dei contenuti, anche pubblicitari), senza essere per questo tenuti a rinunciare integralmente alla fruizione del servizio offerto dal social network online, il che implica che a detti utenti venga proposta, se del caso a fronte di un adeguato corrispettivo, un'*alternativa equivalente* non accompagnata da simili operazioni di trattamento di dati (dunque, un'alternativa che non comporti la profilazione per finalità di personalizzazione dei contenuti).

Con riguardo alla nozione di «alternativa equivalente» è di interesse anche il *Parere dell'EDPB 8/2024 sul consenso valido nel contesto dei modelli «consenso o pagamento» attuati dalle piattaforme online di grandi dimensioni*. Per comprendere la portata di tale documento occorre innanzi tutto chiarire la definizione di «piattaforma online di grandi dimensioni». È l'EDPB stesso a dare una definizione della nozione nell'ambito del parere, chiarendo che la nozione di «piattaforme online» comprende quella prevista dall'art. 3 del Regolamento 2022/2065 sui servizi digitali, ma non è a questa limitata e individuando i seguenti criteri, non cumulativi né esaustivi, utili per qualificare un soggetto come piattaforma online di grandi dimen-

sioni: i) il grande numero di interessati in qualità di utenti; ii) la posizione della società sul mercato; iii) l'esistenza di un trattamento su larga scala di dati personali; iv) la qualificazione del titolare del trattamento come «piattaforma online di dimensioni molto grandi» ai sensi del Regolamento 2022/2065 sui servizi digitali, o come *gatekeeper* ai sensi del Regolamento 2022/1925 sui mercati digitali. A tal riguardo l'EDPB afferma innanzi tutto che:

> se la versione alternativa si differenzia dalla versione con pubblicità comportamentale soltanto nella misura necessaria in considerazione dell'incapacità del titolare del trattamento di trattare dati personali per finalità di pubblicità comportamentale, tale versione alternativa può essere considerata equivalente.

Con riguardo agli altri possibili casi, l'EDPB ritiene che l'interessato debba poter comparare le due versioni e che tali versioni non debbano essere necessariamente identiche, ma che nel caso in cui la qualità sia inferiore e vi siano funzionalità soppresse, la versione non dovrebbe essere ritenuta equivalente. Un profilo di particolare rilevanza attiene al pagamento di un corrispettivo nella versione alternativa offerta dal titolare del trattamento. In proposito, nel parere appena citato l'EDPB, rispetto alla valutazione del requisito della libertà del consenso al trattamento per finalità di pubblicità comportamentale, ritiene che «quando sviluppano l'alternativa alla versione del servizio con pubblicità comportamentale, i titolari del trattamento dovrebbero prendere in considerazione la possibilità di fornire agli interessati una "alternativa equivalente" che non comporti il pagamento di un corrispettivo, come l'alternativa gratuita priva di pubblicità comportamentale». In proposito, l'EDPB afferma anche che, pur non essendoci alcun obbligo per le piattaforme online di grandi dimensioni di offrire sempre servizi gratuiti, la messa a disposizione degli interessati di tale ulteriore alternativa rafforza la loro libertà di scelta e questo rende più facile per i titolari del trattamento dimostrare che il consenso è liberamente prestato. Più in dettaglio, l'EPDB, con riguardo al possibile pregiudizio subito dagli interessati in assenza di un'alternativa gratuita in caso di mancato consenso al trattamento per pubblicità comportamentale, pregiudizio che può inficiare la libertà del consenso al trattamento ai sensi del GDPR, considera la possibile importanza del ruolo delle piattaforme nell'accesso alle informazioni e ai servizi, così come in ambito professionale e nella vita quotidiana e sociale e tiene conto della loro possibile difficile fungibilità che può derivare anche dai c.d. «effetti di rete» ed «effetti di dipendenza» (si pensi ad esempio alla fruizione di un noto social network su cui l'interessato ha un nutrito seguito di *followers*; cfr. le citate Linee guida, pp. 26 ss.).

Dunque, secondo l'EDPB la fornitura di un'alternativa gratuita priva di pubblicità comportamentale costituisce un fattore particolarmente importante da considerare nel valutare se gli interessati possano esercitare una scelta effettiva e quindi se il consenso sia valido. Rispetto alla previsione di un corrispettivo, l'EDPB nel *Parere 8/2024* già citato ritiene che:

> i titolari del trattamento dovrebbero valutare, caso per caso, tanto se un corrispettivo sia in effetti adeguato e quale sia l'importo adeguato in determinate circostanze, tenendo presenti i requisiti per un consenso valido ai sensi del GDPR, nonché la

> necessità di evitare che il diritto fondamentale alla protezione dei dati sia trasformato in una caratteristica il cui godimento è soggetto a pagamento da parte degli interessati oppure in una caratteristica premium riservata ai benestanti o agli abbienti.

Il Comitato prende in esame anche il profilo dello squilibrio di potere fra interessato e titolare del trattamento in relazione alla valutazione della libertà del consenso. In particolare, l'EDPB individua, nel caso in cui il titolare del trattamento sia una «piattaforma online di grandi dimensioni», alcuni elementi non esaustivi e non cumulativi, che possono essere tenuti in conto per valutare la sussistenza di una situazione di evidente squilibrio di potere capace di minare la libertà del consenso. Tali fattori sono: i) la posizione della società sul mercato, anche rispetto all'esistenza di una eventuale sua posizione dominante nel mercato o di un suo rilevante potere di mercato, e della presenza di effetti di rete o di dipendenza; ii) la misura in cui l'interessato fa affidamento sul servizio fornito, in relazione ad esempio alla ricerca di lavoro, all'accesso a informazioni essenziali per la vita quotidiana degli interessati o alla partecipazione al dibattito pubblico; iii) il pubblico destinatario o predominante della piattaforma, ad esempio in relazione alla presenza di minori. L'EDPB ritiene anche che una valutazione caso per caso di tali fattori dovrebbe essere sempre necessaria.

Guardando all'ambito nazionale, il Garante per la Protezione dei Dati Personali (GPDP) da tempo afferma che il consenso non può essere qualificato come libero quando la fornitura di un servizio sia a esso subordinato (ad esempio: GPDP, 10 gennaio 2019, n. 9080914; GPDP, 20 giugno 2019, n. 9124420).

Vi è poi una parte della dottrina e della giurisprudenza secondo cui il consenso può talvolta essere ritenuto libero pur se a questo è subordinata la fornitura di un servizio, e che quanto più il servizio è infungibile e irrinunciabile, quanto più il condizionamento che incide sulla libertà del consenso deve ritenersi sussistente (Cass., 2 luglio 2018, n. 17278).

Infine, la valutazione della libertà del consenso al trattamento può anche essere letta adottando una prospettiva che consideri il carattere massivo dei trattamenti, e che sia volta a garantire, in ossequio anche al principio di uguaglianza sostanziale sancito dall'art. 3 Cost., la necessità di una pari opportunità di soddisfacimento e di esercizio, in concreto, dei diritti fondamentali, e in particolare del diritto alla protezione dei dati personali e alla riservatezza, rispetto ai quali il consenso al trattamento costituisce una modalità di esercizio. Secondo tale punto di vista, la presunzione di cui al considerando 43 GDPR può essere vinta quando il titolare del trattamento dimostri di offrire un servizio non subordinato al consenso al trattamento, alle stesse condizioni economiche di quello condizionato al consenso (Angiolini 2020).

3. *Segue*. L'esecuzione di un contratto di cui l'interessato è parte

L'art. 6, par. 1, lett. b) GDPR prevede la base giuridica della necessità del trattamento per l'esecuzione di un contratto di cui l'interessato è parte o di misure precontrattuali adottate su richiesta dello stesso.

Il contratto diventa qui un elemento da valutare ai fini dell'operatività della base giuridica del trattamento. Il trattamento dei dati è in quest'ipotesi strumentale alla

messa in opera fisiologica del contratto: i dati possono essere trattati solo in virtù della necessità del loro trattamento rispetto a quanto previsto nel regolamento negoziale.

La definizione dei trattamenti necessari all'esecuzione del contratto non sempre è agevole. In alcuni casi il criterio della necessità risulta chiaro; si immagini il caso del trattamento dei dati consistenti nell'indirizzo del cliente-interessato volti all'adempimento dell'obbligazione di consegna di una merce in capo all'altra parte contrattuale. Più complesse sono le ipotesi in cui il trattamento è menzionato nel contratto, e in cui quindi sono le parti a includere il trattamento dei dati all'interno del testo contrattuale. Qui emerge il rischio, sottolineato anche dal EDPB, di aggirare le regole relative alla base giuridica del consenso al trattamento, includendo il trattamento nell'oggetto del contratto. A tal proposito, è utile richiamare l'indirizzo dell'EDPB, che ha escluso che tramite il contratto si possa espandere «artificiosamente» il novero dei trattamenti resi leciti dall'art. 6, par. 1, lett. b) GDPR, e ha elaborato delle linee guida in materia (EDPB, *Linee guida 2/2019 sul trattamento di dati personali ai sensi dell'articolo 6*, paragrafo 1, lettera b), del regolamento generale sulla protezione dei dati nel contesto della fornitura di servizi online agli interessati, versione 2.0, 8 ottobre 2019, p. 6). L'EDPB interpreta il requisito della necessità come oggettivo, e afferma che per utilizzare la base giuridica di cui all'art. 6, par. 1, lett b) GDPR, il titolare del trattamento deve dimostrare che il contratto non può essere eseguito, con riguardo al suo oggetto principale, senza che i dati personali siano trattati. Inoltre, se vi sono alternative meno intrusive, il trattamento non può avere come base giuridica quella dell'esecuzione del contratto. Poi, quando il contratto termina la liceità del trattamento viene meno e il titolare del trattamento non potrà trattare i dati facendo riferimento a una diversa base giuridica per il trattamento, a meno che non vi fossero distinte basi giuridiche comunicate ab initio all'interessato.

La Corte di Giustizia dell'UE è intervenuta sul tema, statuendo che

> affinché un trattamento di dati personali sia considerato necessario all'esecuzione di un contratto […] esso deve essere oggettivamente indispensabile per realizzare una finalità che è parte integrante della prestazione contrattuale destinata all'interessato. Il [titolare] del trattamento deve, quindi, essere in grado di dimostrare in che modo l'oggetto principale del contratto non potrebbe essere conseguito in assenza del trattamento di cui è causa. (CGUE, 4 luglio 2023, C- 252/21; così anche CGUE, 9 gennaio 2025, C-394/23, § 33)

Inoltre, la Corte di Giustizia dell'UE ha affermato che l'elemento determinante ai fini dell'applicazione dell'art. 6, paragrafo 1, lettera b), del RGPD è che il trattamento sia essenziale per consentire la corretta esecuzione del contratto stipulato tra il titolare e l'interessato e, pertanto, che non esistano altre soluzioni percorribili e meno invasive (CGUE, 9 gennaio 2025, C-394/23, § 34; v. anche: CGUE, 12 settembre 2024, C-17/22 e C-18/22; CGUE, 4 luglio 2023, C-252/21, § 99) e che se il contratto consiste in più servizi o in più elementi distinti di uno stesso servizio che possono essere prestati indipendentemente gli uni dagli altri, l'applicabilità dell'articolo 6, par. 1, lett. b), GDPR deve essere valutata separatamente nel contesto di ciascuno di tali servizi (CGUE, 9 gennaio 2025, C-394/23, § 35 e CGUE, 4 luglio 2023, C-252/21, § 100).

Rispetto all'applicazione di tali principi in un caso concreto, si può citare l'indirizzo della CGUE secondo cui

> il trattamento di dati personali relativi all'appellativo dei clienti di un'impresa di trasporto, avente la finalità di personalizzare la comunicazione commerciale fondata sulla loro identità di genere, non sembra essere né oggettivamente indispensabile né essenziale al fine di consentire la corretta esecuzione di un contratto e, pertanto, non può essere considerato necessario all'esecuzione di tale contratto. (CGUE, 9 gennaio 2025, C-394/23, § 43).

4. L'adempimento di un obbligo legale al quale è soggetto il titolare del trattamento

L'art. 6, par. 1, lett. c) GDPR prevede che il trattamento possa avvenire quando è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento.

Rispetto al requisito della necessità, la Corte di Giustizia dell'UE ha affermato che questo non è soddisfatto quando l'obiettivo di interesse generale sotteso all'obbligo di legge

> può ragionevolmente essere raggiunto in modo altrettanto efficace mediante altri mezzi meno pregiudizievoli per i diritti fondamentali degli interessati, in particolare per i diritti al rispetto della vita privata e alla protezione dei diritti personali garantiti agli articoli 7 e 8 della Carta, atteso che le deroghe e le restrizioni al principio della protezione di simili dati devono avere luogo nei limiti dello stretto necessario. (CGUE, 22 giugno 2021, *B*, C-439/19, § 110)

In virtù dell'art. 6, par. 3, GDPR, perché tale base giuridica possa fondare il trattamento, ci deve essere una norma di diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento che determini tale base giuridica.

Inoltre, in ogni caso, la norma che stabilisce tale base giuridica deve perseguire un obiettivo di interesse pubblico e il trattamento deve essere proporzionato a tale obiettivo. Con riguardo alla proporzionalità, la Corte di Giustizia ha affermato che:

> al fine di valutare la proporzionalità del trattamento […] occorre misurare la gravità dell'ingerenza nei diritti fondamentali al rispetto della vita privata e alla protezione dei dati personali che tale trattamento comporta e verificare se l'importanza dell'obiettivo di interesse generale da quest'ultimo perseguito sia in relazione con tale gravità. Al fine di valutare la gravità di tale ingerenza, si deve segnatamente tener conto della natura dei dati personali in questione, e in particolare della loro natura eventualmente sensibile, nonché della natura e delle modalità concrete del trattamento dei dati di cui trattasi, in particolare del numero di persone che hanno accesso a tali dati e delle modalità di accesso a questi ultimi. (CGUE, 1° agosto 2022, C-184/20).

Poi, l'art. 6, GDPR prevede che gli Stati membri possono mantenere o introdurre disposizioni più specifiche per adeguare l'applicazione del GDPR con riguardo al trattamento, determinando con maggiore precisione requisiti specifici per il trattamento e altre misure atte a garantire un trattamento lecito e corretto fra cui: i) le condizioni generali relative alla liceità del trattamento da parte del titolare del trattamento; ii)

le tipologie di dati oggetto del trattamento; iii) gli interessati; iv) i soggetti cui possono essere comunicati i dati personali e le finalità per cui sono comunicati; v) le limitazioni della finalità, vi) i periodi di conservazione; vii) le operazioni e procedure di trattamento, comprese le misure atte a garantire un trattamento lecito e corretto.

Sul piano nazionale, l'art. 2 *ter* d.lgs. 196/2003 (d'ora in avanti: cod. privacy) prevede che il trattamento, quando si applicano le basi giuridiche dell'art. 6, comma 1, lett. c) ed e) GDPR deve essere previsto da una norma di legge, di regolamento, o da atti amministrativi generali (sulla base giuridica di cui alla lett. e) dell'art. 6 GDPR si veda, in questo capitolo, il § 6.).

Inoltre, secondo quanto dispone l'art. 2 *quater* cod. privacy il Garante per la Protezione dei Dati personali può adottare delle regole deontologiche relative ai trattamenti fondati sulla base giuridica qui oggetto di commento.

5. La salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica

L'art. 6, comma 1, lett. d) GDPR prevede come base giuridica quella del trattamento necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica. Tale ipotesi è senz'altro residuale e potrà essere applicata in ipotesi residuali, come conferma anche la lettura del 46 GDPR, secondo cui:

> Il trattamento di dati personali dovrebbe essere altresì considerato lecito quando è necessario per proteggere un interesse essenziale per la vita dell'interessato o di un'altra persona fisica. Il trattamento di dati personali fondato sull'interesse vitale di un'altra persona fisica dovrebbe avere luogo in principio unicamente quando il trattamento non può essere manifestamente fondato su un'altra base giuridica. Alcuni tipi di trattamento dei dati personali possono rispondere sia a rilevanti motivi di interesse pubblico sia agli interessi vitali dell'interessato, per esempio se il trattamento è necessario a fini umanitari, tra l'altro per tenere sotto controllo l'evoluzione di epidemie e la loro diffusione o in casi di emergenze umanitarie, in particolare in casi di catastrofi di origine naturale e umana.

6. L'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento

L'art. 6, par. 1, lett. e) GDPR prevede come base giuridica del trattamento quella della sua necessità per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.

Rispetto alla definizione delle specifiche ipotesi da parte del diritto dell'UE o nazionale, si applica quanto illustrato in relazione all'art. 6, par. 3 GDPR e all'art. 2 *ter* cod. privacy in relazione alla base giuridica relativa all'esistenza di un obbligo legale (v. *supra*, § 4).

Inoltre, l'art. 2 *ter* cod. privacy, prevede alcune regole specifiche. In particolare:

a) Secondo quanto dispone il comma 1 *bis* di tale norma il trattamento dei dati personali è consentito se necessario per l'adempimento di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri attribuiti a una autorità pubblica che tratti tali dati e che sia: i) un'amministrazione pubblica di cui all'articolo 1, com-

ma 2, del d.lgs. 165/2001, ivi comprese le autorità indipendenti e le amministrazioni inserite nell'elenco di cui all'articolo 1, comma 3, della l. n. 196/2009; ii) una società a controllo pubblico statale; iii) limitatamente ai gestori di servizi pubblici, locale, di cui all'articolo 16 del testo unico in materia di società a partecipazione pubblica (d.lgs. n. 175/2016), con esclusione, per le società a controllo pubblico, dei trattamenti correlati ad attività svolte in regime di libero mercato;

b) la comunicazione fra titolari che effettuano trattamenti di dati personali, diversi da quelli che rientrano nelle categorie particolari di dati (v. cap. *Le definizioni fondamentali*) e da quelli relativi a condanne penali e reati di cui all'articolo 10 GDPR, per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri è ammessa se prevista da una norma di legge, di regolamento, o da atti amministrativi generali, o se necessaria ai sensi del comma 1-*bis* dell'art. 2 *ter* cod. privacy (su cui si veda la lettera precedente di questo elenco);

c) La diffusione e la comunicazione di dati personali, trattati per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, a soggetti che intendono trattarli per altre finalità sono ammesse unicamente se previste ai sensi del comma 1 o se necessarie ai sensi del comma 1-*bis*. In tale ultimo caso, ne viene data notizia al Garante almeno dieci giorni prima dell'inizio della comunicazione o diffusione.

Inoltre, secondo quanto dispone l'art. 2 *quater* cod. privacy il Garante per la Protezione dei Dati personali può adottare delle regole deontologiche relative ai trattamenti fondati sulla base giuridica qui oggetto di commento.

7. Il perseguimento del legittimo interesse del titolare del trattamento o di terzi

L'art. 6, par. 1, lett. f) GDPR prevede che i dati possano essere trattati se sono necessari 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.

Un punto chiave nell'applicazione della norma è la valutazione sul giudizio di prevalenza degli interessi o dei diritti e delle libertà fondamentali dell'interessato.

Per quanto riguarda la base giuridica del legittimo interesse la CGUE (CGUE, 9 gennaio 2025, C-394/23; CGUE, 4 ottobre 2024, C-621/22; CGUE, 4 luglio 2023, C-252/21, § 106; In precedenza, con riguardo all'art. 7, lett. f), della direttiva 95/46, si vedano: CGUE, 11 dicembre 2019, C-708/18; 4 maggio 2017, C-13/16, §28; 17 giugno 2021, C-597/19, § 106; CGUE, 29 luglio 2019, C-40/17) ha affermato che tale disposizione prevede tre condizioni cumulative affinché il trattamento dei dati personali sia legittimo:

1) il perseguimento di un legittimo interesse da parte del titolare del trattamento o del terzo o dei terzi ai quali i dati sono comunicati. In proposito, la CGUE ha affermato che l'interesse deve essere considerato attuale ed effettivo (CGUE, 11 dicembre 2019, C-708/18). A titolo di esempio, la Corte di Giustizia ha considerato un legittimo interesse quello del titolare del trattamento o di terzi a ottenere un dato personale di una persona che ha asseritamente danneggiato la sua proprietà, al fine

di agire nei confronti di quest'ultima per ottenere il risarcimento dei danni (CGUE, 17 giugno 2021, C-597/19);

2) la necessità di trattare i dati personali ai fini degli interessi legittimi perseguiti. A questo proposito, la CGUE (CGUE, 9 gennaio 2025, C-394/23, § 48; CGUE, 4 maggio 2017, C-13/16, §30; CGUE, 11 dicembre 2019, C-708/18) ha affermato che le deroghe e le limitazioni in materia di protezione dei dati personali devono essere applicate solo nella misura strettamente necessaria. In particolare, ai fini dell'applicazione della base giuridica del legittimo interesse, occorre valutare che tale interesse non possa ragionevolmente essere raggiunto in modo altrettanto efficace con altri mezzi meno restrittivi dei diritti e delle libertà fondamentali degli interessati, in particolare i diritti al rispetto della vita privata e alla protezione dei dati personali garantiti dagli articoli 7 e 8 della Carta (CGUE, 9 gennaio 2025, C-394/23; GUE, 4 ottobre 2024, C-621/22; CGUE, 4 luglio 2023, C-252/21,). Inoltre, la CGUE ha interpretato il criterio della necessità alla luce del principio di minimizzazione (CGUE, 9 gennaio 2025, C-394/23, § 49; GUE, 4 ottobre 2024, C-621/22; CGUE, 4 luglio 2023, C-252/21; sul principio di minimizzazione v. la sezione successiva di questo capitolo).

3) i diritti e le libertà fondamentali della persona interessata dalla protezione dei dati non prevalgono sull'interesse legittimo perseguito. Secondo l'indirizzo della CGUE (CGUE, 11 Dicembre 2019, C-708/18) la valutazione relativa all'esistenza di diritti e libertà fondamentali della persona interessata che prevalgono sugli interessi legittimi perseguiti dal responsabile del trattamento o dal terzo o dai terzi a cui vengono comunicati i dati, richiede un bilanciamento dei diritti e degli interessi contrapposti, che dipende dalle circostanze specifiche del caso concreto, in cui si deve tenere conto dell'importanza dei diritti dell'interessato derivanti dagli articoli 7 e 8 della Carta.

Inoltre, la CGUE ha affermato che il criterio della gravità della violazione dei diritti e delle libertà dell'interessato è una componente essenziale dell'esercizio di ponderazione o di bilanciamento caso per caso. A questo proposito, la Corte (CGUE, 11 dicembre 2019, C-708/18; CGUE, 24 novembre 2011, cause riunite C-468/10 e 469/10) ha affermato che nella valutazione della gravità della violazione dei diritti fondamentali dell'interessato derivante da tale trattamento devono essere considerati i seguenti elementi:

a) la disponibilità dei dati personali in questione in fonti pubbliche. A tal proposito, la Corte ha osservato che la violazione dei diritti dell'interessato sanciti dagli articoli 7 e 8 della Carta è più grave in caso di trattamento di dati provenienti da fonti non pubbliche, in quanto le informazioni relative alla vita privata dell'interessato saranno successivamente conosciute dal responsabile del trattamento e, a seconda dei casi, dal terzo o dai terzi a cui i dati sono comunicati;

b) la natura dei dati personali in questione, in particolare la loro natura potenzialmente sensibile;

c) la natura e le modalità specifiche del trattamento;

d) il numero di persone che hanno accesso ai dati e le modalità di accesso;

e) alla luce del considerando 47 del GDPR, la ragionevole aspettativa dell'interessato che i suoi dati personali non saranno trattati quando, nelle circostanze del

caso, non può ragionevolmente aspettarsi un ulteriore trattamento di tali dati (così anche: CGUE, 9 gennaio 2025, C-394/23; CGUE, 4 ottobre 2024, C-621/22; CGUE, 4 luglio 2023, C-252/21).

Inoltre, nella sentenza CGUE, 4 luglio 2023, C-252/21 la Corte ha rilevato che occorre considerare se l'interessato è un minore.

La CGUE ha ritenuto che tali fattori debbano essere bilanciati rispetto all'importanza degli interessi legittimi perseguiti nel caso di specie.

In tale valutazione, la specificità del contesto di raccolta potrebbe, almeno in alcune ipotesi, essere considerato rilevante nell'interpretazione delle basi giuridiche del trattamento. In particolare, l'ambiente entro cui i dati sono raccolti potrebbe influire sulla valutazione della posizione dell'interessato nel test comparativo che deve precedere l'uso di questa base giuridica. Ad esempio, rispetto alla raccolta dei dati presso l'abitazione dell'interessato, crescente in ragione dell'espansione del cosiddetto «Internet delle cose», può assumere importanza la tutela costituzionale del domicilio di cui all'art. 14 Cost., anche ai fini dell'esito della valutazione della prevalenza degli interessi, dei diritti e delle libertà dell'interessato.

8. Il trattamento delle categorie particolari di dati personali e le eccezioni di cui all'art. 9 GDPR

Nel capitolo 3 si è trattato della definizione di «categorie particolari di dati personali», che sono definiti dall'art. 9 GDPR come quei dati che rivelano «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» (v. cap. *Le definizioni fondamentali*).

L'art. 9 GDPR prevede anche alcune regole specifiche che si applicano a questa categoria di dati.

In primo luogo, il primo paragrafo dell'art. 9 GDPR prevede un divieto generale di trattamento di queste categorie di dati, mentre il secondo paragrafo della medesima norma sancisce alcune eccezioni a tale divieto. Da questa formulazione normativa si deduce *in primis* che le eccezioni ai divieti, in quanto tali, sono norme di stretta interpretazione (così CGUE, 4 luglio 2023, C-252/21, § 76; CGUE, 21 dicembre 2023, C-667/21, § 50).

Le eccezioni previste sono le seguenti:

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 trattamento delle categorie particolari di dati personali previsto dall'art. 9, par. 1 GDPR.

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. In questa ipotesi i dati sono trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti o da altra persona anch'essa soggetta all'obbligo di segretezza conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti.

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.

l) 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 GDPR, 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.

Inoltre, ai sensi dell'art. 9, comma 4, GDPR, a livello nazionale possono essere mantenute o introdotte ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute.

Come ben si evince dalla lettura della norma, il diritto dell'Unione e quello nazionale hanno un ruolo significativo nel definire, entro i limiti posti dall'art. 9 GDPR, i trattamenti possibili di categorie particolari di dati personali.

Sul piano nazionale, a titolo di esempio, l'art. 2 *sexies* cod. privacy prevede che i trattamenti delle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, del Regolamento, necessari per motivi di interesse pubblico rilevante ai sensi del paragrafo 2, lettera g), del medesimo articolo, sono ammessi qualora siano previsti dal diritto dell'Unione europea ovvero, nell'ordinamento interno, da disposizioni di legge o di regolamento o da atti amministrativi generali che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

Da ultimo, occorre affrontare il tema del rapporto fra le basi giuridiche di cui all'art. 6 GDPR (su cui v. *supra*, §§ 1-7) e quanto disposto dall'art. 9 GDPR. Sul punto, è da ritenere che per trattare lecitamente categorie particolari di dati, è necessario che sia applicabile sia un'eccezione al divieto di cui all'art. 9 che una base giuridica per il trattamento, tra quelle previste dall'art. 6 del GDPR (così CGUE 21 dicembre 2023, C-667/21, §§ 71 ss.). In altre parole, il trattamento di categorie particolari di dati personali che rientrano nell'art. 9 GDPR può essere effettuato solo se i) è applicabile un'eccezione al divieto di trattamento previsto dall'Art. 9 GDPR e ii) si applica una base giuridica prevista dall'art. 6 GDPR.

9. La disciplina sui c.d. cookies

Una disciplina specifica è prevista in relazione ai c.d. *cookies* e più tecnicamente all'archiviazione delle informazioni nell'apparecchio terminale di un contraente o di un utente e all'accesso a informazioni già archiviate.

Per comprendere cosa siano i cookie si può far riferimento alle linee guida in proposito adottate dal Garante per la Protezione dei Dati personali del 10 giugno 2021; nella scheda di sintesi allegata a dette linee guida si legge che:

> I *cookie* sono di regola stringhe di testo che i siti web (cd. publisher o «prima parte») visitati dall'utente ovvero siti o web server diversi (cd. «terze parti») posizionano e archiviano all'interno di un dispositivo terminale nella disponibilità dell'utente (cd. identificatori «attivi»). Analoghe funzioni possono essere svolte da altri strumenti che, pur utilizzando una tecnologia diversa (c.d. identificatori «passivi»), consentono di effettuare trattamenti analoghi a quelli svolti per il tramite dei *cookie*.

La disciplina di tali strumenti è data *in primis* dalla dir. 2002/58 (d'ora in avanti: direttiva e-privacy), recepita nell'ordinamento italiano all'art. 122 cod. privacy.

Con riguardo ai rapporti fra il GDPR e la direttiva e-privacy – e la relativa disciplina di recepimento –, l'art. 1, par. 2, direttiva e-privacy prevede che le disposizioni della direttiva precisino e integrino quanto previsto dalla dir. 95/46/CE; l'art. 94 GDPR prevede l'abrogazione di tale direttiva, e che i riferimenti fatti alla direttiva si devono intendere come riferiti al regolamento stesso.

Guardando alla disciplina nazionale di recepimento, l'art. 122 cod. privacy:

a) ammette testualmente 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;

b) salvo quanto detto nella lettera a), prevede che sia necessario il consenso del contraente o dell'utente, reso dopo che questi è stato informato con modalità semplificate, per l'archiviazione delle informazioni nell'apparecchio terminale di un contraente o di un utente o per l'accesso a informazioni già archiviate.

c) in tutti gli altri casi che non rientrano nelle ipotesi di cui alle lett. a) e b), 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.

Con riguardo ai caratteri del consenso da parte dell'interessato, è la stessa direttiva e-privacy a far riferimento alla disciplina generale in materia di dati personali dettata dal GDPR (v. *supra*, § 2). Infatti, l'art. 2 direttiva e-privacy dispone che il «"consenso" dell'utente o dell'abbonato corrisponde al consenso della persona interessata di cui alla direttiva 95/46/CE» e in virtù dell'art. 94 GDPR, il riferimento alla dir. 95/46 deve intendersi fatto al GDPR.

Con riguardo alla possibilità di adottare basi giuridiche diverse dal consenso nell'ipotesi *sub* b) il Garante per la Protezione dei Dati Personali, sulla base del principio di specialità, ha affermato che:

> la disciplina di carattere speciale applicabile [...] non contempla ulteriori basi giuridiche che rendano legittimo il trattamento se non in presenza del consenso dell'interessato ovvero al ricorrere di una delle ipotesi di deroga rispetto all'obbligo della sua raccolta previste proprio da tale disciplina speciale. (GPDP, *Linee guida* cookie *e altri strumenti di tracciamento,* 10 giugno 2021, punto 5)

Rispetto alle modalità di prestazione del consenso, il comma 2 dell'art. 122 prevede che possono essere utilizzate specifiche configurazioni di programmi informatici o di dispositivi che siano di facile e chiara utilizzabilità per il contraente o l'utente. In proposito, la Corte di Giustizia dell'Unione Europea ha affermato che il consenso

> non è validamente espresso quando l'archiviazione di informazioni o l'accesso a informazioni già archiviate nell'apparecchiatura terminale dell'utente di un sito Internet sono autorizzati mediante una casella preselezionata che l'utente deve deselezionare al fine di negare il proprio consenso (CGUE, 1° ottobre 2019, C-673/17).

La Corte di Giustizia arriva a tale soluzione anche richiamando il considerando 32 GDPR, secondo cui «non dovrebbe [...] configurare consenso il silenzio, l'inattività o la preselezione di caselle». Alcuni altri esempi e alcune considerazioni in proposito si trovano nelle *Linee guida* cookie *e altri strumenti di tracciamento,* del 10 giugno 2021 del Garante per la Protezione dei Dati Personali.

Con riguardo alle modalità semplificate dell'informazione, il Garante per la Protezione dei Dati personali nelle *Linee guida* cookie *e altri strumenti di tracciamento,* del 10 giugno 2021, ha dato alcune indicazioni, fra cui quella relativa alla necessità che questa sia fruibile, senza discriminazioni, anche da parte di coloro che a causa di disabilità necessitano di tecnologie assistive o configurazioni particolari.

Sez. II. I principi del trattamento

10. I principi di liceità, correttezza e trasparenza

L'art. 5 GDPR, accedendo ad una prospettiva della disciplina dei dati personali di tipo relazionale e dinamico, che riflette la trasformazione dell'interferenza nell'altrui sfera informativa, da occasionale a fisiologica, fissa presupposti, criteri organizzativi e limiti dell'attività di trattamento, obblighi di condotta, per lo più aventi natura procedimentale, che attribuiscono all'interessato il *potere* di compartecipare nell'utilizzazione dei propri dati personali seguendo, controllando, rettificando il dato personale – così da plasmare la propria identità personale – fino all'estremo della riappropriazione (mediante la revoca del consenso o l'esercizio del diritto di opposizione) delle informazioni che lo riguardano.

Si può dire, in maniera sintetica, che i c.d. principi del trattamento – così designati per la loro indeterminatezza e il carattere di direttive fondamentali della disciplina – dettano le condizioni di liceità del trattamento: la liceità, infatti, cui fa menzione l'art. 5, co. 1, lett. a) GDPR, non si esaurisce nell'esistenza di una delle basi giuridiche previste dall'art. 6 (rubricato, per l'appunto, condizioni di liceità) che consentono, in conformità agli artt. 52 della Carta di Nizza e 8, par. 2 della Convenzione Edu, l'ingerenza nella sfera giuridica dell'interessato – *i.e.*: consenso dell'interessato/necessarietà del trattamento rispetto a determinate finalità – né nella non contrarietà della finalità del trattamento all'ordine pubblico, al buon costume o ad una norma imperativa (secondo un controllo che ricalca quello affidato alla causa del contratto; si pensi all'ipotesi in cui il titolare intenda trattare dati personali dei propri clienti per la gestione di una casa di prostituzione: la raccolta del consenso presso l'interessato e, dunque, la ricorrenza di una delle basi giuridiche previste all'art. 6 GDPR, non scolora la illiceità del trattamento).

La liceità, invero, esprime più in generale la conformità del trattamento a tutte le prescrizioni contenute nel regolamento, o, perlomeno, a quelle contenute negli artt. da 5 a 11 [così, infatti, CGUE, 4 maggio 2023, C-60/22, che ha escluso dal novero dei «trattamenti illeciti», capace di fondare la cancellazione o la limitazione dei dati, «la violazione, da parte del titolare del trattamento, degli obblighi previsti agli articoli 26 e 30 di tale regolamento, relativi, rispettivamente, alla conclusione di un accordo che determina la contitolarità del trattamento e alla tenuta del registro delle attività di trattamento»].

In posizione dialettica con la liceità si pone la clausola generale di correttezza – anch'essa richiamata dall'art. 5, co. 1, lett. a) – la quale si inserisce negli spazi non compiutamente definiti dal regolamento, sanzionando, *ex post*, le modalità concrete con le quali il trattamento è stato eseguito. Prendendo in prestito le parole delle *Linee guida EDPB 4/2019 sull'art. 25 Protezione dei dati fin dalla progettazione e per*

impostazione predefinita, «La correttezza è un principio di natura trasversale secondo cui i dati personali non devono essere trattati in modo ingiustificatamente dannoso, illegittimamente discriminatorio, imprevisto o fuorviante per l'interessato». E così, a esempio, è stato giudicato contrario al canone della correttezza lo svolgimento di un'attività di *marketing* diretto, attuata per il tramite di chiamate mute (cioè a dire senza che ad essa faccia seguito una risposta dall'operatore) tale da ribaltare sull'interessato l'inefficienza del *call center* (Cass. 04 febbraio 2016, n. 2196). E alla stessa stregua deve essere giudicato il comportamento del titolare, che, al momento della raccolta del consenso, presenti le diverse opzioni del trattamento in modo da indurre l'interessato a consentirgli di raccogliere più dati personali di quanto avverrebbe se le opzioni fossero presentate in modo corretto e neutrale (cfr., a riguardo, anche EDPB *Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them*), o che ometta di fornire all'interessato informazioni, ulteriori rispetto a quelle elencate agli artt. 13 e 14 GDPR, ma necessarie nel caso concreto (così il considerando 60 GDPR, a mente del quale «il titolare del trattamento dovrebbe fornire all'interessato eventuali ulteriori informazioni necessarie ad assicurare un trattamento corretto e trasparente, prendendo in considerazione le circostanze e il contesto specifici in cui i dati personali sono trattati»). La regola della correttezza svolge dunque le consuete funzioni, valutativa (che consiste nella paralisi, in quanto abusiva, della pretesa avanzata dall'interessato) e integrativa (che si risolve nel riconoscimento della sussistenza di un obbligo ulteriore in capo al titolare), senza però esaurirsi in una soltanto delle due.

La prima terna di principi è completata dal dovere di trasparenza, il quale riveste preminente importanza nel contesto del regolamento giacché innerva di contenuto quel diritto alla protezione dei dati personali che si manifesta anzitutto nel potere di controllo sulle proprie informazioni. Al dovere di trasparenza sono infatti primariamente riconducibili le norme che prescrivono il contenuto dell'obbligo informativo che grava sul titolare al più tardi al momento della raccolta presso l'interessato o un terzo (artt. 13 e 14 GDPR), le modalità di trasmissione delle informazioni (art. 12 GDPR), il diritto di accesso alle proprie informazioni e, quello conseguente, di ottenere una copia dei dati personali (art. 15 GDPR) nonché l'obbligo di comunicare all'interessato una violazione dei dati personali (art. 34 GDPR).

11. Il principio di finalità

La liceità del trattamento, nel senso minimale di ricorrenza di una base giuridica, non si apprezza isolatamente, ma rispetto alla finalità che il titolare intende perseguire: quest'ultima, infatti, costituisce una limitazione interna al trattamento che, una volta determinata, si impone allo stesso titolare per tutta la durata del trattamento. Per consentire all'interessato di controllare la permanenza del nesso di strumentalità si prevede che la finalità debba essere *determinata*, *esplicita* e *legittima*. La *legittimità* assume diverse coloriture: rispetto al trattamento basato sul consenso o sull'esecuzione di un contratto, essa si risolve nella liceità dell'interesse che il titolare intende perseguire riguardata alla luce dei consueti parametri offerti dalle norme imperative, dal buon costume e dall'ordine pubblico. Nel caso di trattamento necessario per l'e-

secuzione di un contratto, l'adempimento di un obbligo legale, la salvaguardia di un interesse vitale dell'interessato, l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare, la delimitazione dell'ambito degli interessi e, dunque, delle finalità legittimamente perseguibili dal titolare è sostanzialmente data dalla tipizzazione in chiave funzionale delle condizioni di liceità del trattamento. Nel caso, invece, di trattamento fondato sul legittimo interesse del titolare la legittimità della finalità si risolve nella meritevolezza comparativa tra l'interesse perseguito dal titolare e l'istanza protezionistica dell'interessato.

I requisiti della *determinatezza* – la finalità deve essere definita con sufficiente precisione, di talché «a purpose that is vague or general, such as for instance 'improving users' experience', 'marketing purposes', 'IT-security purposes' or 'future research' will – without more detail – usually not meet the criteria of being 'specific'» (così WP29 *Opinion 03/2013 on purpose limitation*) – e del *carattere esplicito* – la finalità non può essere affidata ad una ricostruzione ermeneutica implicita o a fatti concludenti – testimoniano lo stretto rapporto che corre tra il dovere di trasparenza e la liceità del trattamento: un trattamento che si dovesse, ad esempio, basare su un consenso raccolto per una finalità non esplicitata o non determinata sarebbe evidentemente un trattamento illecito.

L'art. 5, co. 1, lett. b) GDPR prosegue disponendo che i dati personali (originariamente raccolti per finalità determinate, esplicite e legittime) possono essere trattati ulteriormente – si intende, per un trattamento diverso da quello iniziale, sia esso successivo o contestuale ad esso – purché la diversa finalità (che sorregge l'ulteriore trattamento) sia compatibile con quella iniziale. La regola è ulteriormente specificata all'art. 6, par. 4 GDPR, là dove è stabilito che qualora il trattamento per una finalità diversa da quella per la quale i dati personali sono stati (inizialmente) raccolti non sia basato (*i*) sul consenso dell'interessato (naturalmente prestato in relazione alla nuova finalità, non potendosi basare il trattamento effettuato per la diversa finalità sul consenso prestato in relazione alla originaria finalità, né essendo ammissibile, per carenza del requisito della specificità, prestare un consenso anche per una finalità diversa, non ancora determinata) o (*ii*) su un atto legislativo che preveda il trattamento dei dati personali, quale misura necessaria e proporzionata per la salvaguardia degli obiettivi di cui all'articolo 23, par. 1 – ipotesi, queste, nelle quali è possibile trattare ulteriormente i dati personali anche se le finalità sono tra loro incompatibili [cfr. CGUE, 2 marzo 2023, C-268/21 per la possibilità, da parte di una società committente, di utilizzare il registro del personale tenuto dall'appaltatore e contenente i dati dei lavoratori per finalità di controllo fiscale, per (il diverso fine) di dimostrare in giudizio l'infondatezza della domanda dell'appaltatore volta ad ottenere il pagamento del corrispettivo ancora dovuto] –; fuori da queste ipotesi è necessario accertare se la (diversa e ulteriore) finalità sia compatibile con quella originaria.

Di là dalle ipotesi del trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità a quanto previsto dall'art. 89 GDPR, trattamento considerato di per sé non incompatibile, al fine di verificare la compatibilità della ulteriore finalità (c.d. *test di compatibilità*) l'art. 6, par. 4 GDPR, unitamente al considerando 30 GDPR, invitano a tenere in considerazione: a) ogni nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulte-

riore trattamento previsto; b) il contesto in cui i dati personali sono stati raccolti, in particolare relativamente alla relazione tra l'interessato e il titolare del trattamento; c) la natura dei dati personali (categorie particolari di dati personali, dati relativi a condanne penali e a reati); d) le possibili conseguenze dell'ulteriore trattamento previsto per gli interessati; e) l'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione dei dati. Si tratta di criteri che, come ha precisato la Corte di Giustizia «riflettono la necessità di un nesso concreto, logico e sufficientemente stretto, tra le finalità della raccolta iniziale dei dati personali e l'ulteriore trattamento di tali dati, e consentono di assicurarsi che tale ulteriore trattamento non si discosti dalle legittime aspettative degli interessati quanto all'ulteriore utilizzo dei loro dati» [così CGUE, 20 ottobre 2022, C-77/21, secondo cui «il principio della "limitazione della finalità" non osta alla registrazione e alla conservazione da parte del titolare del trattamento, in una banca dati creata al fine di effettuare test e di correggere errori, di dati personali precedentemente raccolti per la diversa (ma compatibile) finalità consistente nella conclusione e nell'esecuzione di contratti di abbonamento»]. Laddove vi sia un trattamento ulteriore dei dati personali compatibile con le finalità originarie troveranno applicazione gli artt. 13, par. 3 e 14, par. 4 GDPR a mente dei quali il titolare «prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente». In particolare, secondo le *Linee guida WP29 sulla trasparenza ai sensi del regolamento 2016/679* i titolari del trattamento dovrebbero fornire «informazioni sull'analisi di compatibilità svolta ai sensi dell'articolo 6, paragrafo 4, qualora la nuova finalità del trattamento si fondi su una base giuridica diversa dal consenso o da un atto legislativo dell'Unione o degli Stati membri (in altre parole, una spiegazione del modo in cui il trattamento per una finalità diversa sia compatibile con la finalità iniziale)», in modo da consentire agli interessati «di valutare la compatibilità dell'ulteriore trattamento e delle garanzie fornite e di decidere se esercitare o no i loro diritti, ad esempio, tra gli altri, il diritto di limitazione di trattamento o il diritto di opporsi al trattamento».

12. Il principio di minimizzazione

Una volta fissata la finalità, il titolare deve trattare i dati personali nel rispetto del principio di necessità (o di minimizzazione) tra mezzi e fini: i dati personali devono essere pertanto adeguati e pertinenti (profilo qualitativo) e limitati (profilo quantitativo) a quanto necessario per il perseguimento della finalità per le quali sono trattati. I primi requisiti obbligano a verificare se la finalità perseguita (e es. la prova di un fatto in un giudizio instaurato per far valere un diritto o l'esecuzione di un servizio di trasporto ferroviario) «non possa essere realizzata ricorrendo a mezzi di prova meno invasivi» (CGUE, 2 marzo 2023, C-268/21) che non implichino i il trattamento dei dati personali. Il canone della limitazione, invece, impone di circoscrivere il trattamento ai soli dati indispensabili per la realizzazione dello scopo perseguito; così, a esempio, qualora sono una parte dei dati sia necessaria per far valere un proprio diritto in giudizio, «il giudice nazionale deve prendere in considerazione l'adozione di misure appropriate in materia di protezione dei dati, quali

la pseudonimizzazione […] dei nomi degli interessati o qualsiasi altra misura destinata a ridurre al minimo l'ostacolo al diritto alla protezione dei dati personali costituito dalla produzione di tale documento. Siffatte misure possono comprendere, in particolare, la limitazione dell'accesso del pubblico al fascicolo o l'ordine alle parti a cui i documenti contenenti dati personali sono stati comunicati di non utilizzare tali dati per finalità della prova durante il procedimento giurisdizionale di cui trattasi» (in tal senso CGUE, 2 marzo 2023, C-268/21). E, ancora, risponde al principio di minimizzazione, sotto il profilo quantitativo, la limitazione di una comunicazione commerciale ai soli «nomi e cognomi dei clienti, atteso che il loro appellativo e/o la loro identità di genere sono un'informazione che non pare essere strettamente necessaria in tale contesto» (CGUE, 9 gennaio 2025, C-394/23).

13. Il principio di esattezza e di limitazione della conservazione

I dati personali, prosegue l'art. 5, co. 1, lett. d) GDPR, devono essere esatti e aggiornati: la norma, che istituisce un obbligo per il titolare di fedeltà contenutistica del contenuto dei dati alla realtà da essi rappresentati, attribuisce, al contempo, all'interessato una serie di prerogative. Il primo, infatti, deve adottare tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati; il secondo, se del caso anche esercitando il diritto di accesso, ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo nonché l'integrazione di quelli incompleti. Il principio di limitazione della finalità trova completamento sotto il profilo temporale nella previsione dell'art. 5, co. 1, lett. e) GDPR, il quale limita la possibilità di identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono stati trattati (*principio di limitazione della conservazione*): pertanto, una volta conseguita la finalità originariamente stabilita, un ulteriore trattamento che consenta l'identificazione dell'interessato (con esclusione dei trattamenti per finalità di archiviazione nel pubblico interesse, di ricerca scientifica o storica) deve ritenersi non più consentito (cfr. CGUE, 20 ottobre 2022, C-77/21, secondo cui «il "principio della limitazione della conservazione" osta alla conservazione, da parte del titolare del trattamento, in una banca dati creata al fine di effettuare test e di correggere errori, di dati personali precedentemente raccolti per altre finalità, per un arco di tempo superiore a quello necessario alla realizzazione di tali test e alla correzione di tali errori»). All'obbligo del responsabile del trattamento di impedire l'ulteriore identificazione dell'interessato corrisponde il diritto di quest'ultimo di ottenere la cancellazione o la trasformazione in forma anonima dei dati personali.

14. Il principio di sicurezza e riservatezza

L'art. 5, co. 1, lett. f) GDPR richiede, infine, che i dati personali siano trattati in modo da garantirne un'adeguata sicurezza e riservatezza contro il rischio di trattamenti non autorizzati o illeciti, di perdita, distruzione o danni accidentali ai dati. A tal fine, l'art. 32 GDPR, prescrive al titolare e al responsabile di adottare – tenuto conto

dello stato dell'arte, dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto, delle finalità del trattamento, delle esigenze di protezione dei dati specificamente coinvolti e, dunque, dei rischi che presenta il trattamento (cfr., altresì, i considerando 75, 76 e 83 GDPR) – ogni misura tecnica e organizzativa idonea ad evitare una violazione dei dati personali e indica, a titolo esemplificativo, tra le misure da adottare: 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.

15. Il principio di accountability

L'art. 32 GDPR rappresenta una specificazione, in materia di sicurezza, della più generale disciplina dettata all'art. 24 GDPR, il quale obbliga il titolare e il responsabile del trattamento, tenuto conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, nonché dei rischi per i diritti e le libertà delle persone fisiche, ad adottare ogni altra misura tecnica e organizzativa adeguata per garantire che il trattamento sia effettuato in conformità al regolamento (cfr., altresì, il considerando 74 GDPR). La norma dà espresso riconoscimento al c.d. principio di accountability (da tradurre come responsabilizzazione e non responsabilità) il quale si concretizza in un mutamento di approccio da parte del legislatore europeo: in luogo di prescrizione dirette e precise, alla cui mancata applicazione consegue una sanzione, il regolamento prevede un obiettivo generale (la conformità ai principi del regolamento), affidando al titolare la scelta delle modalità concrete più adeguate per conseguirlo e rimettendo all'autorità di controllo o al giudice la successiva valutazione in merito alla loro adeguatezza.

Oltre all'art. 24 GDPR e al già richiamato art. 32 GDPR in materia di sicurezza fa diretto riferimento al principio di *accountability* anche l'art. 5, co. 2 GDPR, il quale dispone che «il titolare del trattamento è competente per il rispetto del paragrafo 1 [che menziona i principi applicabili al trattamento] e in grado di comprovarlo», così evidenziando il duplice profilo prescrittivo e probatorio che dà contenuto al principio: all'obbligo di conformarsi alle prescrizioni del regolamento si affianca infatti l'obbligo di dimostrare la correttezza e l'adeguatezza della misura adottata e, più in generale, la conformità al regolamento. A tal fine particolare importanza riveste il registro delle attività di trattamento che il titolare e il responsabile devono tenere ai sensi dell'art. 30 GDPR: la sua omissione, tuttavia, sebbene renda meno agevole dimostrare la conformità del trattamento ai principi del regolamento, non dimostra di per sé che i diritti e le libertà degli interessati siano stati violati (così CGUE, 4 maggio 2023, C-60/22). Sono espressione del principio di *accountability* anche l'art. 12 GDPR, là dove rimette al titolare la scelta delle «misure appropriate per fornire all'interessato tutte le informazioni di cui agli artt. 13 e 14 e le comunicazioni di cui agli articoli da 15 a 22»; l'art. 7 GDPR, il quale rimette al titolare del trattamento la scelta della modalità di acquisizione del consenso e del conseguente

onere probatorio; l'art. 6, co. 1, lett. f) GDPR, il quale impone al titolare del trattamento di compiere la valutazione comparativa tra il proprio legittimo interesse e gli interessi e i diritti dell'interessato.

Nella scelta della misura più appropriata, il titolare del trattamento, nell'esercizio della discrezionalità di cui dispone, deve tenere conto tra gli altri, e specie in materia di sicurezza, del livello di *rischio* che il trattamento presenta per i diritti e le libertà dell'interessato (art. 32, par. 1, GDPR). A tal fine il titolare, prima di avviare il trattamento, deve svolgere una valutazione di impatto qualora prevede di utilizzare una nuova tecnologia o, indipendentemente dal mezzo utilizzato, allorquando, considerati la natura, l'oggetto, il contesto e le finalità del trattamento valuti l'esistenza di un rischio elevato per i diritti e le libertà delle persone fisiche (art. 35, par. 1 GDPR; v., altresì, provvedimento del Garante per la protezione dei dati personali n. n. 467 dell'11 ottobre 2018), come accade, a esempio, nelle ipotesi: a) di trattamento che implica una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche; b) di trattamento, su larga scala, di categorie particolari di dati personali di cui all'art. 9, par. 1, o di dati relativi a condanne penali e a reati di cui all'art. 10; c) di trattamento che implica la sorveglianza sistematica su larga scala di una zona accessibile al pubblico. La valutazione di impatto che il titolare del trattamento deve svolgere, consultando il responsabile del trattamento e, se del caso, gli interessati o i loro rappresentanti, e che, dovrà essere periodicamente riesaminata (art. 35, par. 11 GDPR), include gli adempimenti di cui all'art. 35, par. 7 GDPR, tra i quali spicca la individuazione e la valutazione dei rischi per i diritti e le libertà degli interessati nonché la successiva illustrazione delle misure predisposte per affrontare tali rischi e rendere il trattamento conforme al Regolamento.

Qualora a seguito della valutazione di impatto dovesse emergere che, tenuto conto della tecnologia disponibili e dei costi di attuazione (considerando 84 GDPR) le misure adottate dal titolare non sono in grado di ridurre il rischio (il quale, dunque, persiste elevato) quest'ultimo sarà obbligato a consultare l'autorità di controllo, la quale – anche esercitando i poteri di indagine previsti dall'art. 58 – là dove dovesse accertare che il trattamento violi il Regolamento entro il termine di otto settimane (prorogabile di ulteriori sei settimane) dovrà emanare un parere scritto.

Strettamente connessi con il principio di responsabilizzazione e con la valutazione d'impatto, sono i c.d. principi della *privacy by design* e *privacy by default*, sanciti all'art. 25 (cfr., altresì, EDPB Linee guida 4/2019 sull'articolo 25, Protezione dei dati fin dalla progettazione e per impostazione predefinita), i quali – tenuto conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione del contesto e delle finalità del trattamento così come dei rischi del trattamento – impongono, sin dalla progettazione del trattamento (dunque prima che il trattamento sia avviato), nonché per impostazione predefinita, l'adozione di soluzioni tecniche e organizzative (la cui individuazione in concreto spetta al titolare di determinare) adeguate per rendere conforme il trattamento ai principi del Regolamento.

Ciò comporta, a esempio, che il titolare che intenda trattare dati personali per finalità di vendita *online* di beni dovrà configurare il *layout* del sito internet in mo-

do da fornire le informazioni in conformità a quanto prescritto dall'art. 12 GDPR: dovrà, perciò, adottare un approccio multilivello, evidenziando immediatamente i punti più importanti e, mediante la creazione di menu a discesa e collegamenti ad altre pagine, mettere a disposizione dell'interessato le ulteriori informazioni di dettaglio; dovrà, ancora, rendere visibile l'informativa privacy su tutte le pagine del sito di modo che l'interessato acceda sempre alle informazioni con un semplice *clic*; dovrà, infine, mettere a disposizione le informazioni nel giusto contesto e al momento adeguato, utilizzando ad esempio *snippet* informativi o *pop-up*. Il medesimo titolare dovrà, poi, predisporre il modulo d'ordine per la raccolta dei dati personali dei clienti in conformità al principio di minimizzazione: dopo aver individuato i dati personali strettamente necessari per l'acquisto dei beni, dovrà, ad esempio, rendere opzionale la compilazione di quei campi del modulo d'ordine che richiedono dati ulteriori rispetto a quelli necessari per l'esecuzione del contratto. Sempre avuto riguardo al principio di minimizzazione, il titolare del trattamento – in un altro esempio: un ospedale che gestisce le informazioni sullo stato di salute dei pazienti – dovrà, per impostazione predefinita, consentire l'accesso a tali informazioni solo ai membri del personale medico ai quali sia affidata la cura del paziente nel reparto specifico cui questi è assegnato. Con riferimento, invece, al principio di limitazione della conservazione, il titolare del trattamento dovrà anzitutto definire e adottare una procedura interna per la conservazione e la cancellazione dei dati, in base alla quale i dipendenti cancelleranno manualmente i dati personali dopo la fine del periodo della loro conservazione e, poi, per rendere più efficace la cancellazione, predisporre un meccanismo di cancellazione dei dati automatico. In attuazione del principio di integrità e sicurezza, il titolare del trattamento dovrà, infine, a titolo esemplificativo, predisporre un sistema di gestione della sicurezza delle informazioni, limitare l'accesso soltanto a taluni dipendenti, dotati di chiavi di accesso, predisporre una segregazione della rete in modo tale che l'eventuale *malware* che abbia superato il perimetro di *security* non sia in grado di paralizzare tutti i dispositivi aziendali connessi; prevedere la pesudonimizzazione dei dati.

Sez. III. La violazione dei dati personali

16. Introduzione. La nozione

La violazione dei dati personali, spesso nota con l'espressione inglese di *data breach*, è definita dal legislatore europeo come «la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati» (art. 4, n. 12) GDPR). A tale nozione fanno riferimento alcune regole (artt. 33-34 GDPR), che al ricorrere, per l'appunto, di una violazione dei dati personali, gravano il titolare del trattamento e, in parte, il responsabile del trattamento di una serie di obblighi.

Prima di esaminare nel dettaglio i vari elementi che compongono la nozione e la disciplina, è utile soffermarsi su alcuni aspetti preliminari per ricostruire la storia e la finalità dell'istituto in esame.

Le norme sulla violazione dei dati personali rappresentano una novità introdotta dal GDPR. La direttiva 95/46/CE, infatti, non disciplinava le conseguenze di un'eventuale violazione dei dati personali, né tanto meno ne forniva una definizione. In realtà, già si prevedevano obblighi di sicurezza in capo al titolare del trattamento «al fine di garantire la protezione dei dati personali dalla distruzione accidentale o illecita, dalla perdita accidentale o dall'alterazione, dalla diffusione o dall'accesso non autorizzati, […] o da qualsiasi altra forma illecita di trattamento di dati personali» (art. 17, par. 1, direttiva 95/46); tuttavia, mancavano specifiche disposizioni per l'ipotesi in cui tali circostanze, oggi qualificabili come violazioni di dati personali, si verificassero.

Prima dell'adozione del GDPR, il legislatore europeo si era comunque già occupato della violazione dei dati personali in un intervento di modifica della direttiva e-privacy, contenuto nella direttiva 2009/136/CE. A livello di diritto interno, l'art. 4, co. 3, lett. g-*bis*) del codice privacy, introdotto in attuazione di quest'ultima direttiva dal d.lgs. n. 69/2012, definiva la violazione dei dati personali come la «violazione della sicurezza che comporta anche accidentalmente la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso ai dati personali trasmessi, memorizzati o comunque elaborati nel contesto della fornitura di un servizio di comunicazione accessibile al pubblico». Tale fattispecie, in armonia con il disposto della direttiva comunitaria, veniva presa in considerazione, dall'abrogato art. 32-*bis*, cod. privacy, solo nell'ambito dei servizi di comunicazione elettronica accessibili al pubblico (ad esempio, servizi telefonici, servizi di accesso a Internet), il cui fornitore veniva obbligato, al verificarsi di una siffatta violazione, di informare il Garante per la protezione dei dati personali e, qualora la violazione rischiasse di arrecare pregiudizio ai dati personali o alla riservatezza dell'utente contraente del servizio o di altra persona, di compiere una comunicazione a questi ultimi. Simili obblighi informativi, in caso di violazioni dei dati, venivano imposti anche alle banche (v. provvedimento del Garante per la protezione dei dati personali n. 192 del 12 maggio 2011), ai titolari dei trattamenti di dati biometrici (v. provvedimento del Garante per la protezione dei dati personali n. 513 del 12 novembre 2014), alle strutture sanitarie (v. provvedimento del Garante per la protezione dei dati personali n. 331 del 4 giugno 2015) e alle amministrazioni pubbliche (v. provvedimento del Garante per la protezione dei dati personali n. 393 del 2 luglio 2015).

Sono diverse le analogie con le norme adesso previste dal GDPR. Tuttavia, la differenza più significativa risiede nell'ambito applicativo soggettivo: mentre, in passato, gli obblighi da osservare in caso di *data breach* incombevano soltanto su alcuni soggetti, adesso gravano su qualunque titolare del trattamento di dati personali.

Come risulta ormai chiaro, le norme sulla violazione dei dati personali devono essere lette in stretta connessione agli obblighi di sicurezza del titolare del trattamento (art. 32 GDPR), i quali rappresentano un'espressa concretizzazione del principio sancito dall'art. 5, par. 1, lett. f) GDPR (v. *supra* in questo cap., sez. II, § 14). La stessa nozione sopra richiamata (art. 4, n. 12 GDPR), infatti, definisce la violazione dei dati personali come una «violazione di sicurezza».

Non bisogna, però, intendere che quest'ultima consista necessariamente in una violazione degli obblighi previsti dall'art. 32, relativi all'adozione di misure

tecniche e organizzative adeguate a garantire un livello di sicurezza appropriato al rischio connesso al trattamento dei dati. La sicurezza, infatti, può risultare violata anche in assenza di condotte censurabili del titolare o del responsabile del trattamento (CGUE, 14 dicembre 2023, C-340/21, § 31). La violazione dei dati personali va intesa, dunque, come un incidente di sicurezza informatica da cui discende una situazione pregiudizievole per i dati personali trattati – quale la distruzione, la perdita, la modifica, la divulgazione o l'accesso non autorizzati – che può comportare un rischio per i diritti e le libertà delle persone fisiche cui i dati si riferiscono (art. 33, par. 1 GDPR).

La causa dell'incidente potenzialmente rischioso può essere di natura accidentale o illecita. In quest'ultimo caso, l'illecito (ad esempio, una frode informatica) è solitamente imputabile a terzi diversi dal titolare e dall'eventuale responsabile del trattamento, i quali, tuttavia, possono essere comunque ritenuti (in parte) responsabili della violazione di sicurezza, laddove non abbiano preventivamente adottato le misure volte a proteggere i dati personali dall'esterno. In ogni caso, al di là del concorso nella causa della violazione, il titolare e il responsabile del trattamento possono essere ritenuti responsabili del rischio generato dalla violazione stessa, laddove non abbiano eseguito in modo adeguato e tempestivo gli adempimenti necessari dopo il *data breach*. Il rischio, che deriva dalla violazione di sicurezza, dev'essere affrontato secondo tali modalità per evitare che lo stesso si traduca in danni per gli interessati.

La disciplina predisposta dal legislatore europeo mira, quindi, ad anticipare la tutela delle persone fisiche coinvolte a uno stadio precedente rispetto al concretizzarsi dei danni, peraltro non sempre facilmente riparabili (cfr. *infra* cap. *Il risarcimento del danno da illecito trattamento dei dati personali*).

Tra i pregiudizi che gli interessati al trattamento possono subire in ragione di una violazione dei dati personali, si possono citare, a titolo esemplificativo: la perdita del controllo sui dati personali che li riguardano, la limitazione dei loro diritti, la decifratura non autorizzata della pseudonimizzazione, la discriminazione, il furto o l'usurpazione d'identità, il pregiudizio alla reputazione, la perdita di riservatezza dei dati personali protetti da segreto professionale, perdite finanziarie (v. considerando 85 GDPR).

Per definire in modo completo il significato della nozione di violazione di sicurezza, occorre altresì precisare cosa si intende per «distruzione», «perdita» e «modifica» dei dati personali, oltre che per «divulgazione» e «accesso» non autorizzati. A tal fine, preziose indicazioni provengono dalle *Linee guida n. 9/2022 sulla notifica delle violazioni dei dati personali*, adottate il 28 marzo 2023 dal Comitato europeo per la protezione dei dati (European Data Protection Board)[2].

[2] Le Linee guida 9/2022 hanno aggiornato le precedenti Linee guida sulla notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679, adottate dal Gruppo di lavoro Art. 29 il 3 ottobre 2017 ed emendate il 6 febbraio 2018. Ancora prima, il medesimo Gruppo di lavoro aveva adottato il Parere 03/2014 sulla notifica delle violazioni, riferito, tuttavia, all'obbligo dei fornitori di servizi di comunicazione elettronica ai sensi della direttiva 2002/58/CE.

In tale documento, si chiarisce che: la «distruzione» dei dati personali si verifica quando i dati non esistono i più, o comunque non esistono più in una forma che possa permetterne un qualsiasi uso da parte del titolare del trattamento; la «perdita» dei dati personali sottende una situazione in cui i dati possono ancora essere presenti, ma il titolare del trattamento ne ha perso il controllo o l'accesso, o non ne è più in possesso; la «modifica» dei dati personali ha luogo quando i dati perdono la loro integrità; la «divulgazione» e l'«accesso» non autorizzati sono, infine, due ipotesi nelle quali i dati personali sono, rispettivamente, oggetto di una comunicazione a destinatari non autorizzati al trattamento o, in assenza di comunicazione, di un accesso da parte di terzi che non avrebbero dovuto trattare i medesimi dati.

Le fattispecie appena descritte sono classificabili, in base ai principi di sicurezza informatica, all'interno di tre diverse tipologie di violazioni: la violazione della riservatezza; la violazione dell'integrità; la violazione della disponibilità. Mentre la divulgazione e l'accesso non autorizzati realizzano un *vulnus* alla riservatezza dei dati, la modifica ne intacca l'integrità, e la perdita, al pari della distruzione, fa sì che i dati non siano più nella disponibilità del titolare. In base alle circostanze, la gravità della violazione può variare: il grado massimo si raggiunge quando essa presenta una combinazione delle tre tipologie menzionate.

Si pensi, a esempio, a un attacco informatico che riesca, da un lato, a cifrare i dati personali in possesso del titolare (c.d. attacco *ransomware*), con conseguente perdita di disponibilità dei dati in mancanza di un *backup*, cioè di una copia di sicurezza, e che riesca, d'altro lato, anche ad esportarli (c.d. esfiltrazione) e a modificarli, con conseguente violazione di riservatezza e integrità. All'estremo opposto, come incidente meno grave, si pone il caso di una semplice perdita temporanea di disponibilità dei dati, che talvolta, come evidenziano le *Linee guida 9/2022*, potrebbe anche non trattarsi di una violazione di sicurezza, come quando la perdita temporanea è dovuta a un intervento programmato di manutenzione del sistema informatico su cui i dati sono conservati. Tuttavia, ciò non vale per altre ipotesi in cui si verifica una mancanza temporanea di controllo dei dati: ad esempio, se questa è imputabile a un'interruzione prolungata di corrente elettrica, pur non presentando solitamente rischi per i diritti e le libertà degli interessati, dovrebbe essere comunque considerata una violazione, con le conseguenze che ne derivano per il titolare del trattamento.

17. L'obbligo di documentazione

La violazione dei dati personali è fonte di una serie di obblighi per il titolare e il responsabile del trattamento. Alcuni di tali obblighi sorgono qualora la violazione abbia determinate caratteristiche; altri, invece, rappresentano una costante di qualsiasi violazione dei dati personali. Nel primo gruppo, come vedremo, rientrano la notifica all'autorità di controllo e la comunicazione agli interessati, da parte del titolare del trattamento; nel secondo, occorre annoverare l'obbligo di informazione del responsabile del trattamento nei confronti del titolare e l'obbligo di documentazione dell'incidente gravante su quest'ultimo.

In particolare, a tal riguardo, l'art. 33, par. 5 GDPR prevede che il titolare del trattamento documenti qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione dev'essere conservata in quanto la stessa potrà essere esaminata dall'autorità di controllo per verificare che il titolare abbia agito in conformità agli (altri) obblighi previsti dal GDPR, in caso di violazione dei dati personali. L'obbligo di documentazione risulta, dunque, strumentale all'attività di vigilanza sull'applicazione del GDPR, svolta dall'autorità di controllo (v. *infra* cap. *La regolamentazione e la tutela amministrativa*, § 1).

Al contempo, la documentazione serve allo stesso titolare del trattamento per (mettersi in grado di) dimostrare di aver operato nel rispetto della disciplina in materia di protezione dei dati personali. Da quest'angolo di visuale, l'obbligo in esame costituisce una chiara concretizzazione del principio di responsabilizzazione (*accountability*), sancito dall'art. 5, par. 2 GDPR e attuato, in termini generali, dagli obblighi del titolare del trattamento di cui all'art. 24, par. 1 GDPR (v. *supra* in questo cap., sez. II, § 15). Per il rispetto del suddetto principio, oltre alla documentazione raccolta, assume rilevanza anche la conoscenza, da parte dei dipendenti del titolare, delle procedure da adottare in caso di *data breach*: a tal fine, può risultare utile, a livello interno, la redazione preventiva di un manuale per la gestione delle violazioni dei dati.

Per conservare la documentazione relativa alle violazioni di sicurezza, è implicito, come specificano le *Linee guida 9/2022*, che il titolare del trattamento tenga un registro delle violazioni in questione. Non deve necessariamente trattarsi di un registro separato da quello relativo alle attività di trattamento di cui all'art. 30, par. 1 GDPR, potendo costituire semplicemente parte di quest'ultimo.

Il titolare del trattamento è, quindi, abbastanza autonomo nella scelta del metodo con cui registrare le informazioni relative a una violazione dei dati personali; è, invece, vincolato rispetto al contenuto, che deve includere tanto le cause dell'incidente di sicurezza, quanto gli effetti, con speciale riferimento alle azioni intraprese dal titolare per porvi rimedio. A quest'ultimo riguardo, pur nel silenzio dell'art. 33, par. 5 GDPR, il Comitato europeo per la protezione dei dati raccomanda di documentare anche le ragioni che hanno condotto alle azioni in questione. Se, ad esempio, il titolare del trattamento non notifica la violazione dei dati personali all'autorità di controllo, è bene che nel registro siano riportati i motivi in base ai quali il titolare ritiene che la violazione non presenti un rischio per i diritti e le libertà delle persone fisiche, cui i dati violati si riferiscono.

L'obbligo di documentazione implica la conservazione delle informazioni relative alla violazione di sicurezza; pertanto, laddove tali informazioni facciano esplicito riferimento a dati personali, si pone il problema di definire il periodo di conservazione di tali dati. Occorre rifarsi al principio generale secondo cui i dati possono essere 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 (art. 5, par. 1, lett. e) GDPR). Nel caso in questione, la conservazione è ammessa finché il titolare del trattamento può essere chiamato a fornire prova, dinanzi all'autorità di controllo, del rispetto della procedura relativa al *data breach* e, più in generale, del rispetto del principio di *accountability*.

18. La notifica all'autorità di controllo

Se la documentazione è un'attività sempre necessaria nel caso in cui si verifichi una violazione di dati personali, non può dirsi altrettanto per la notifica all'autorità di controllo, cioè il Garante per la protezione dei dati personali. Il titolare del trattamento, infatti, può esimersi dalla notifica quando ritiene improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche (art. 33, par. 1 GDPR).

Nella valutazione di tale rischio, il titolare può avvalersi del responsabile della protezione dei dati (meglio noto come *Data Protection Officer*: *DPO*), che, quando presente (v. art. 37, parr. 1 e 4 GDPR), deve fornire consulenza in merito agli obblighi derivanti dalla disciplina europea e nazionale sulla protezione dei dati personali (art. 39, par. 1, lett. a)). Il *DPO* (sulla cui figura, v. *supra* cap. *Le definizioni fondamentali*, § 7), inoltre, è indicato come il punto di contatto presso cui l'autorità di controllo può ottenere informazioni aggiuntive, circa la violazione dei dati personali, rispetto a quelle inserite nella notifica effettuata dal titolare. Per tale ragione, si devono almeno comunicare il nome e i dati di contatto (ad esempio, l'indirizzo e-mail) del responsabile della protezione dei dati (art. 33, par. 3, lett. b)).

Prima di esaminare i fattori da considerare per la valutazione dei rischi della violazione, propedeutica all'eventuale notifica al Garante, è bene evidenziare che il titolare deve preliminarmente venire a conoscenza del *data breach*. Ciò deve avvenire il prima possibile: infatti, solo se si prende consapevolezza dell'incidente di sicurezza in tempi rapidi, è possibile effettuare la notifica all'autorità di controllo «senza ingiustificato ritardo», come richiede l'art. 33, par. 1. Inoltre, la stessa norma impone al titolare del trattamento, una volta appresa la violazione, di procedere con la notifica, ove possibile, entro 72 ore; altrimenti, il titolare deve specificare all'autorità di controllo i motivi del ritardo.

La *ratio* alla base di tali prescrizioni è che prima si interviene, informando il Garante per la protezione dei dati personali, meglio si riesce a mitigare i rischi discendenti dal *data breach*. Coerentemente con tale disegno, occorre che il titolare del trattamento, al fine di agire in modo tempestivo, si doti di tutte le misure tecnologiche e organizzative adeguate per stabilire immediatamente se c'è stata violazione dei dati personali (v. considerando 87 GDPR). Talvolta, il titolare potrebbe semplicemente sospettare che una violazione di dati personali abbia avuto luogo; in casi del genere, svolgerà celermente una verifica interna per accertarne il reale avvenimento e, in tale frangente temporale, non potrà considerarsi ancora consapevole della violazione per il decorso del termine delle 72 ore entro cui effettuare la notifica (v. le *Linee guida 9/2022*).

Da non trascurare, inoltre, il ruolo del responsabile del trattamento, il quale, con l'obbligo di informare tempestivamente il titolare di eventuali incidenti di sicurezza (art. 33, par. 2 GDPR), contribuisce a mettere quest'ultimo nelle condizioni di notificare la violazione al Garante senza ingiustificato ritardo.

Da quando il titolare del trattamento viene a conoscenza del *data breach*, egli deve procedere senza indugio alla valutazione del rischio per i diritti e le libertà delle persone fisiche, vale a dire il rischio che la violazione dei dati personali comporti discriminazioni, furti o usurpazioni di identità, perdite finanziarie, pregiudizi alla

reputazione, perdita di riservatezza dei dati personali protetti da segreti professionali, decifratura non autorizzata di dati pseudonimizzati, perdita del controllo dei dati personali da parte degli interessati, o qualsiasi altro danno economico o sociale significativo (v. considerando 75 e 85 GDPR).

La valutazione di tali rischi, come si è visto (v. *supra* in questo cap., sez. II, § 15), ricorre anche nell'ambito della valutazione di impatto sulla protezione dei dati (v. art. 35, par. 7, lett. c) GDPR). Non bisogna, tuttavia, pensare che la valutazione dei rischi susseguente a una violazione di dati personali coincida con quella oggetto di una *data protection impact assessment* (*DPIA*). Invero, sebbene nella *DPIA* si faccia riferimento anche ai rischi connessi a un eventuale *data breach*, non può trascurarsi che i rischi in essa valutati riguardano un evento del tutto ipotetico, con la conseguenza che la probabilità del loro verificarsi può essere ben diversa rispetto a quella inerente a un incidente di sicurezza che si è concretamente verificato. D'altronde, in una *DPIA* si prendono in considerazione i dati personali genericamente coinvolti in un determinato trattamento, mentre nella valutazione dei rischi successiva a un *data breach* si tiene conto soltanto dei dati personali violati.

I rischi possono variare in base a diversi fattori. Tra questi, le *Linee guida 9/2022* suggeriscono di valorizzare: il tipo di violazione; la natura, la sensibilità e il volume dei dati violati; la facilità di identificazione degli interessati, così come il numero e le caratteristiche degli stessi, oltre alla gravità di conseguenze che la violazione può causare nei loro confronti. Invero, la perdita di disponibilità, dovuta a un attacco informatico, di dati particolarmente sensibili (ad esempio, i dati delle cartelle cliniche dei pazienti di un ospedale) presenta rischi maggiori dell'accesso non autorizzato, da parte di un ex dipendente del titolare, a dati comuni di un gruppo, pur numeroso, di interessati (ad esempio, il nome, il cognome e la data di nascita dei clienti possessori della carta fedeltà di un supermercato). A sua volta, quest'ultima violazione risulta più rischiosa dell'invio involontario, al destinatario sbagliato, di un'e-mail contenente informazioni di non particolare rilievo, relative ad un solo interessato (ad esempio, un'e-mail di conferma dell'ordine di acquisto di una t-shirt, effettuato da un singolo cliente).

Al contempo, l'adozione preventiva di tecniche di protezione dei dati può ridurre sensibilmente i rischi, anche a fronte di violazioni che colpiscano dati rilevanti (ad esempio, l'esfiltrazione da un sito web delle password degli utenti è poco probabile che comporti rischi per gli interessati nella misura in cui le password siano crittografate e l'autore dell'attacco informatico non abbia accesso alla chiave crittografica). Quest'ultimo esempio è tratto dall'accurata casistica delle violazioni di dati personali più frequenti, stilata dal Comitato europeo per la protezione dei dati, che fornisce altresì le istruzioni necessarie sulle azioni da intraprendere da parte del titolare del trattamento (v. *EDPB, Linee guida 01/2021 su esempi riguardanti la notifica di una violazione dei dati personali*).

Se dalla valutazione, che il titolare del trattamento è chiamato a compiere, risulta un rischio per i diritti e le libertà degli interessati, la notifica al Garante per la protezione dei dati personali è obbligatoria.

Le informazioni da fornire devono comprendere almeno: la descrizione della natura della violazione dei dati personali, compresi, ove possibile, le categorie e il

numero approssimativo di interessati in questione, nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione; la comunicazione del nome e dei dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere informazioni; la descrizione delle probabili conseguenze della violazione dei dati personali; la descrizione delle misure adottate, o di cui si propone l'adozione, da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e, se del caso, per attenuarne i possibili effetti negativi (art. 33, par. 3 GDPR).

È possibile che il titolare non riesca a raccogliere tutte le informazioni da notificare all'autorità di controllo entro il breve termine di 72 ore dalla scoperta della violazione dei dati personali. Per tale ragione, l'art. 33, par. 4 permette di fornire le informazioni mancanti dopo la notifica, purché ciò avvenga «senza ulteriore ingiustificato ritardo». A fronte di attacchi informatici particolarmente sofisticati, può darsi, ad esempio, che solo un'indagine di polizia riesca a ricostruire la natura e la portata dell'incidente di sicurezza; in tal caso, una volta ottenute le ulteriori informazioni sulla violazione dei dati personali, il titolare può integrare la notifica in una fase successiva.

19. La comunicazione agli interessati

La notifica all'autorità di controllo e l'adozione di misure idonee ad attenuare i rischi del *data breach*, da documentare, a livello interno, insieme alle caratteristiche della violazione, non esauriscono gli adempimenti del titolare del trattamento. Come si è anticipato, infatti, la violazione di sicurezza richiede anche la comunicazione agli interessati, i cui dati sono stati violati, laddove il rischio per i loro diritti e le loro libertà risulti elevato. Nell'esempio sopra citato di un attacco informatico che renda indisponibili i dati delle cartelle cliniche dei pazienti di un ospedale, non vi è dubbio che si ricada in tale fattispecie. Ma, volendo cambiare tipologia di violazione, lo stesso varrebbe anche in caso di furto di un supporto materiale su cui sono memorizzati dati personali non cifrati di un numero molto significativo di soggetti (ad esempio, il furto del computer portatile del dipendente di una società di servizi contenente una lista di oltre 100.000 clienti, comprendente, oltre che il nome e il cognome, il sesso, la data di nascita e l'indirizzo di residenza: l'esempio è tratto dalle *Linee guida 01/2021*).

Valutata la gravità del rischio derivante dal *data breach*, il titolare del trattamento, senza ingiustificato ritardo, deve comunicare agli interessati la violazione, descrivendone la natura e le probabili conseguenze e informandoli delle misure adottate o di cui si propone l'adozione per porvi rimedio, facendo altresì riferimento ai dati di contatto del responsabile della protezione dei dati (art. 34, parr. 1-2 GDPR). Ove opportuno, la comunicazione dovrebbe anche fornire raccomandazioni agli interessati sulle misure da impiegare per proteggere sé stessi dai possibili effetti negativi della violazione (v. considerando 86 GDPR): ad esempio, a seguito di un attacco informatico a un sito web, potrebbe suggerire il cambio di password, nel caso in cui vi sia il dubbio che l'autore dell'attacco abbia avuto accesso alle credenziali degli utenti. D'altronde, l'obbligo di comu-

nicazione mira proprio a mettere gli interessati nelle condizioni di prendere consapevolezza dei rischi e di agire, ove possibile, con misure di autoprotezione.

La scelta del mezzo comunicativo è rimessa al titolare del trattamento, che, su raccomandazione del Comitato europeo per la protezione dei dati (v. le *Linee guida 9/2022*), dovrebbe comunque preferire il canale più idoneo a far pervenire correttamente la comunicazione a tutti gli interessati. In quest'ottica, il titolare potrebbe anche ricorrere contemporaneamente a diversi canali, come l'invio di messaggi telematici (ad esempio, e-mail, SMS), o cartacei tramite i servizi postali, oppure la pubblicazione di banner su siti web di primo piano. Non è, invece, sufficiente la pubblicazione di un comunicato stampa.

In ogni caso, la comunicazione dev'essere trasparente: il titolare deve utilizzare un linguaggio semplice e chiaro per gli interessati (art. 34, par. 2 GDPR) e deve evitare di inviare le informazioni sul *data breach* insieme ad altre informazioni che, non riguardando la violazione, potrebbero sviare l'attenzione dei destinatari. Sul piano della comprensibilità del messaggio, inoltre, è di particolare rilievo la lingua in cui la comunicazione viene scritta. Il titolare dovrebbe impiegare la lingua già utilizzata in altre occasioni di contatto con gli interessati; tuttavia, se non vi sono state precedenti interazioni, può essere accettata, stando alle indicazioni del Comitato europeo per la protezione dei dati, la lingua del Paese in cui il titolare del trattamento ha sede.

In casi particolari, nonostante la violazione possa astrattamente comportare un rischio elevato per i diritti e le libertà delle persone fisiche interessate, il titolare del trattamento è esonerato dalla comunicazione. Ciò avviene quando: a) il titolare ha adottato, prima della violazione, misure adeguate di protezione dei dati, quali la cifratura; b) il titolare adotta, dopo la violazione, misure atte a scongiurare il sopraggiungere del rischio elevato, come, ad esempio nel caso in cui riesca a identificare l'autore del *data breach*, impedendogli di fare alcunché coi dati violati (art. 34, par. 3 GDPR). Una terza fattispecie in cui il titolare può legittimamente astenersi dal comunicare agli interessati la violazione, sebbene quest'ultima presenti realmente un rischio elevato per i diritti e le libertà degli interessati, si ha quando tale comunicazione richiederebbe sforzi sproporzionati. È il caso in cui i dati di contatto degli interessati sono stati persi a causa della violazione o, già da prima, non erano nella disponibilità del titolare del trattamento. Questi deve, comunque, procedere a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia (art. 34, par. 3, lett. c) GDPR).

Se il titolare ritiene che ricorra una delle condizioni appena descritte, può evitare di comunicare la violazione dei dati personali agli interessati. Nel rispetto del principio di responsabilizzazione (*accountability*), deve essere in grado di dimostrare al Garante per la protezione dei dati che la condizione di esonero sia soddisfatta. L'autorità di controllo può, da par suo, decidere che effettivamente si ricada in una delle ipotesi sopra menzionate, confermando la legittimità della scelta del titolare; tuttavia, può anche richiedere a quest'ultimo di provvedere alla comunicazione non ancora effettuata (art. 34, par. 4 GDPR), esercitando, se del caso, i propri poteri per sanzionare l'omissione.

Riferimenti bibliografici

Barba Angelo, Pagliantini Stefano (a cura di). 2019. *Delle persone. Leggi collegate*, II. Torino: Utet.

Bolognini, Luca. 2016. "I principi del trattamento." In Bistolfi C., Bolognini L., Pelino E., *Il Regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*. Milano: Giuffrè.

Caggia, Fausto. 2019. "Libertà ed espressione del consenso." In Vincenzo Cuffaro, Roberto D'Orazio e Vincenzo Ricciuto, *I dati personali nel diritto europeo*. Torino: Giappichelli, pp. 249-73.

Dell'Utri, Marco. 2019. "Principi generali e condizioni di liceità del trattamento dei dati personali." In Cuffaro Vincenzo, D'Orazio Roberto, Ricciuto Vincenzo (a cura di), *I dati personali nel diritto europeo*. Torino: Giappichelli.

Finocchiaro, Giusella. 2017. "Il quadro d'insieme sul Regolamento europeo sulla protezione dei dati personali." In Finocchiaro Giusella (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*. Bologna: Zanichelli.

Garofalo, Andrea M. 2022. "Il campo di applicazione del GDPR e i principi del trattamento." In Magri Geo, Martinelli Silvia, Thobani Shaira (a cura di), *Manuale di diritto privato delle nuove tecnologie*. Torino: Giappichelli.

Iamiceli, Paola, Cafaggi, Fabrizio, Angiolini Chiara (a cura di). 2022. *Casebook Effective Data Protection and Fundamental Rights*. Scuola Superiore della Magistratura.

Irti, Claudia. 2021. *Consenso "negoziato" e circolazione dei dati personali*. Torino: Giappichelli.

Kamara, Irene, De Hert, Paul. 2018. "Understanding the balancing act behind the legitimate interest of the controller ground: a pragmatic approach." *Bruxelles Privacy Hub Working Paper* n. 12.

Lucchini Guastalla, Emanuele. 2019. "Privacy e Data Protection: principi generali." In Tosi Emilio (a cura di), *Privacy Digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*. Milano: Giuffrè.

Malgieri, Gianclaudio. 2021. "Art. 5." In D'Orazio Roberto, Finocchiaro Giusella, Pollicino Oreste, Resta Giorgio, *Codice della privacy e data protection*. Milano: Giuffrè.

Messinetti, Davide. 1998. "Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali." *Riv. crit. dir. privato* 3.

Panetta, Rocco (a cura di). 2019. *Circolazione e protezione dei dati personali tra libertà e regole di mercato. Commentario al regolamento UE n. 2016/679 e al novellato d.lgs. n. 196/2003*. Milano: Giuffrè.

Renna, Mario. 2020. "Violazione dei dati personali, sicurezza del trattamento e protezione dai rischi". *Rivista del mercato assicurativo e finanziario* 2: 197-221.

Resta, Giorgio. 2000. "Revoca del consenso ed interesse al trattamento nella legge sulla protezione dei dati personali." *Rivista critica del diritto privato* 2: 299-333.

Resta, Giorgio, Zeno-Zencovich, Vincenzo. 2018. "Volontà e consenso nella fruizione dei servizi in rete." *Riv. trim. dir. proc. civ* 2.

I diritti dell'interessato

Antonello Iuliani

Abstract: This chapter examines the data subject rights, providing a detailed analysis of their content, also in light of jurisprudential developments in the field.

Keywords: Data subjetc rights

1. Introduzione

Con l'espressione «diritti dell'interessato», che parrebbe di primo acchito evocare l'autonomia delle singole attribuzioni, il Reg. UE 2016/679 (d'ora in avanti: GDPR) indica, agli artt. 12-23, l'insieme dei poteri, delle facoltà e dei rimedi specifici (dunque, non solo posizioni sostantive) che compongono il contenuto unitario del diritto alla protezione dei dati personali e alle quali il legislatore affida il compito di consentire all'interessato di esercitare il controllo sulle proprie informazioni di carattere personale. La scelta del legislatore europeo di disciplinare le modalità di esercizio del diritto fondamentale alla protezione dei dati personali innova rispetto alla concettualizzazione classica dei diritti fondamentali, la quale si sofferma piuttosto sui rimedi necessari per reagire (*ex post*) alle compressioni intollerabili della libertà del titolare da parte di terzi. Si tratta di una prospettiva che valorizza la dimensione cooperativa nella realizzazione della persona che chiama in gioco *ex ante* l'attività del titolare in una logica non dissimile da quella propria del rapporto obbligatorio.

2. Il diritto alle informazioni

Privilegiando un'articolazione dell'esposizione che ricalca la topografia del GDPR occorre muovere dagli obblighi informativi che gravano sul titolare, i quali – in attuazione del dovere di trasparenza prescritto all'art. 5, par. 1, lett. a) GDPR – intendono rimediare, non diversamente da quanto accade in materia

Antonello Iuliani, Università digitale Pegaso, Italy, antonello.iuliani@unipegaso.it, 0000-0001-9931-6934

Referee List (DOI 10.36253/fup_referee_list)
FUP Best Practice in Scholarly Publishing (DOI 10.36253/fup_best_practice)

consumeristica, alla strutturale e fisiologica asimmetria informativa che caratterizza la posizione dell'interessato, al fine di assicurare a quest'ultimo la pienezza del proprio diritto alla protezione dei dati personali. La natura strumentale degli obblighi di informazione rispetto all'esercizio degli altri diritti dell'interessato emerge con particolare evidenza sia dagli artt. 13, co. 2, lett. b) e 14, co. 2, lett. c) GDPR – che prevedono l'obbligo per il titolare di informare l'interessato sull'esistenza del diritto di chiedere l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati – sia dall'art. 12 par. 3 GDPR – che impone al titolare (ad eccezione dell'ipotesi in cui sia impossibile identificare l'interessato) di fornire, senza giustificato ritardo, e al più tardi entro un mese dalla richiesta (termine prorogabile di due mesi), le informazioni relative alle azioni intraprese a seguito di una delle richieste formulata in sede di esercizio dei summenzionati «diritti». Sempre l'art. 12 GDPR detta le regole generali sulle modalità di comunicazione delle informazioni (ai sensi degli artt. 13 e 14 GDPR; ai sensi degli artt. 15-22 GDPR e ai sensi dell'art. 34 GDPR), le quali devono essere fornite, di regola, gratuitamente; per iscritto o con altri mezzi, anche elettronici, o, su richiesta dell'interessato anche oralmente; «in forma concisa, trasparente, intellegibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori».

Se ne ricava che la comunicazione all'interessato deve essere: (i) calibrata sulle capacità di comprensione dell'uomo medio e, qualora, l'interessato sia un minore, «utilizzare un linguaggio semplice e chiaro che un minore possa capire facilmente» (così il considerando 58 GDPR); (ii) esaustiva ma non sovrabbondante; (iii) organizzata in modo da facilitare la comprensione da parte dell'interessato, a esempio, mediante un'offerta stratificata o multilivello che consenta di reperire immediatamente le informazioni essenziali e progressivamente quelle più di dettaglio. Significativo, a riguardo, è il provvedimento dell'Autorità garante del 7 marzo 2019, n. 59 (*Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario*), che ha evidenziato «con specifico riferimento all'attività posta in essere da titolari del trattamento operanti in ambito sanitario che effettuano una pluralità di operazioni connotate da particolare complessità (es. aziende sanitarie)» l'opportunità «di fornire all'interessato le informazioni previste dal Regolamento in modo progressivo. Ciò significa che nei confronti della generalità dei pazienti afferenti a una struttura sanitaria potrebbero essere fornite solo le informazioni relative ai trattamenti che rientrano nell'ordinaria attività di erogazione delle prestazioni sanitarie (cfr. art. 79 del Codice). Gli elementi informativi relativi a particolari attività di trattamento (es. fornitura di presidi sanitari, modalità di consegna dei referti medici on-line, finalità di ricerca) potrebbero essere resi, infatti, in un secondo momento, solo ai pazienti effettivamente interessati da tali servizi e ulteriori trattamenti. Ciò andrebbe a beneficio di una maggiore attenzione alle informazioni veramente rilevanti, fornendo la piena consapevolezza circa gli aspetti più significativi del trattamento».

Il contenuto dell'obbligo di informazione è delineato, in misura sostanzialmente omogenea, agli artt. 13 e 14 GDPR a seconda che i dati siano raccolti presso l'interessato, su iniziativa di quest'ultimo o anche mediante monitoraggio, dunque passivamente (art. 13) o siano ottenuti da altra fonte (altro titolare, fonte pubblicamente accessibile quale una pagina web, fonte istituzionale come un pubblico registro) (art. 14). Il titolare deve in entrambi i casi comunicare all'interessato l'identità e i dati di contatto del titolare e del suo rappresentante; l'identità e i dati di contatto del responsabile della protezione dei dati personali; le finalità del trattamento e la sua base giuridica nonché la diversa finalità per la quale il titolare intende trattare ulteriormente i dati personali (artt. 13, par. 3 e 14 par. 4 GDPR); gli eventuali destinatari del trattamento o le categorie di destinatari; ove previsto, l'intenzione del titolare di trasferire dati a un destinatari in un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione.

I paragrafi 2 degli artt. 13 e 14 GDPR completano il catalogo delle informazioni che il titolare, al fine di conformarsi all'obbligo di correttezza e trasparenza, deve fornire all'interessato: spiccano, oltre all'informazione sull'esistenza di un processo decisionale automatizzato, compresa la profilazione, e le informazioni sulla logica utilizzata [cfr., sul punto, Cass. 25 maggio 2021, n. 14381, secondo la quale «nel caso di una piattaforma web preordinata all'elaborazione di profili reputazionali di singole persone fisiche o giuridiche, incentrata su un sistema di calcolo con alla base un algoritmo finalizzato a stabilire i punteggi di affidabilità, il requisito di consapevolezza (del consenso, n.d.a.) non può considerarsi soddisfatto ove lo schema esecutivo dell'algoritmo e gli elementi di cui si compone restino ignoti o non conoscibili da parte degli interessati»], le informazioni funzionali a rendere l'interessato pienamente consapevole, e cioè a dire le informazioni relative: ai diritti che la normativa gli accorda (art. 13, par. 2, lett. b) e 14, par. 2, lett. c) GDPR); al potere di revocare il consenso (art. 13, par. 2, lett. c) e 14, par. 2, lett. d) GDPR); alla tutela in via amministrativa tramite reclamo all'autorità garante (artt. 13, par. 2, lett. d) e 14, par. 2, lett. e) GDPR).

Le informazioni che il titolare è tenuto a comunicare non si esauriscono in quelle previste dagli artt. 13 e 14 GDPR, potendo, come già detto, egli essere tenuto, alla stregua del dovere di correttezza, a fornire all'interessato ogni altra informazione che tenuto conto «delle circostanze e del contesto specifici in cui i dati personali sono trattati», si riveli necessaria. D'altra parte, il dovere di correttezza – che, ricordiamo, grava anche sull'interessato – consente al titolare di rifiutare di fornire un'informazione, anche relativa ad un'azione intrapresa ai sensi degli articoli da 15 a 22 GDPR, o di addebitare a quest'ultimo un contributo spese, qualora la richiesta sia manifestamente infondata o eccessiva, in particolare per il suo carattere ripetitivo (art. 12, par. 5 GDPR). L'obbligo di informazione è, inoltre, escluso se l'interessato dispone già dell'informazione (art. 13, par. 4 GDPR) e se la registrazione o la comunicazione dei dati personali sono previste per legge o se informare l'interessato si rivela impossibile o richiederebbe uno sforzo sproporzionato (a es., per il numero di interessati e

l'antichità dei dati, nel caso di trattamenti eseguiti ai fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici) (art. 14, par. 5 GDPR).

Per quanto riguarda il momento in cui devono essere comunicate le informazioni questo varia a seconda che i dati siano raccolti presso l'interessato o siano ottenuti da altra fonte: nel primo caso, nonostante il tenore letterale suggerisca una contestualità tra raccolta dei dati personali e comunicazione delle informazioni, è preferibile reputare che l'informativa debba sempre precedere la raccolta; si tratta di una generalizzazione della soluzione prevista nel caso in cui il trattamento (e, dunque, la raccolta) sia basato sul consenso – che, per l'appunto, deve essere informato e, dunque, seguire l'informazione – ovvero su un obbligo di legge o contrattuale – nel qual caso, ai sensi dell'art. 13, par. 2, lett. e) GDPR, l'interessato deve essere edotto delle conseguenze della mancata comunicazione dei dati personali (donde, ancora, una precedenza dell'informazione rispetto al trattamento). Nel secondo caso l'informativa deve essere fornita: a) entro un termine ragionevole e, comunque, al più tardi entro un mese; b) nel caso in cui i dati personali siano destinati alla comunicazione con l'interessato, al momento della prima comunicazione all'interessato (e comunque non oltre il mese); c) nel caso in cui sia prevista la comunicazione ad altro destinatario, non oltre la prima comunicazione dei dati personali (e comunque non oltre il mese).

3. Il diritto di accesso

Nel porre l'attenzione sul nesso di complementarità e di reciproca strumentalità che sussiste tra i «diritti» attribuiti all'interessato, merita anzitutto di osservare come il diritto di accesso previsto all'art. 15 GDPR si apprezzi sul presupposto dell'assolvimento dell'obbligo informativo – consentendo all'interessato di verificare la veridicità delle informazioni ricevute – e sia a sua volta strumentale all'esercizio di quei diritti volti a inibire e/o a conformare l'attività di trattamento. Meglio di altri, consente, dunque, di apprezzare la dimensione dinamica del diritto alla protezione dei dati personali che si realizza, anzitutto, nel controllo nel tempo – a «intervalli ragionevoli», così recita il considerando 63 GDPR – sui propri dati personali, «per essere consapevole del trattamento e verificarne la liceità». Precipitato del principio di trasparenza, il diritto di accesso consiste nel diritto dell'interessato – che «non è tenuto a motivare la richiesta di accesso ai dati» (così CGUE, 26 ottobre 2023, C-307/22) – di ricevere dal titolare la conferma dello svolgimento o meno di un trattamento dei propri dati personali, di accedere direttamente a questi ultimi (nei limiti in cui tale accesso non pregiudichi i diritti e le libertà altrui, compreso il segreto industriale e aziendale e la proprietà intellettuale) ovvero di ottenerne, a titolo gratuito, una copia, nonché, più in generale, di conoscere una serie di informazioni essenziali relative al trattamento (sostanzialmente riproduttive di quelle indicate agli artt. 13 e 14 GDPR), ivi compresa l'identità stessa dei destinatari ai quali i dati sono stati o saranno comunicati «a meno che non sia impossibile identificare detti destinatari o che il titolare non dimostri che le richieste di accesso

dell'interessato sono manifestamente infondate o eccessive, nel qual caso il titolare può indicare unicamente le categorie di destinatari di cui trattasi» (così CGUE, 12 gennaio 2023, C-154/21) e, se del caso, «le informazioni relative all'identità delle persone che hanno consultato i dati personali» (così CGUE, 22 giugno 2023, C-579/21, sulla base di una interpretazione che qualifica tali dati come personali dell'interessato). Nel contenuto del diritto di accesso acquista un ruolo centrale – in confronto con il più modesto contenuto dell'art. 12, lett. a) della dir. 95/46 che faceva riferimento alla «comunicazione» – la facoltà di acquisire una copia dei dati personali, la quale «deve presentare tutte le caratteristiche [in termini di esaustività, intellegibilità e comprensibilità] che consentano all'interessato di esercitare effettivamente i suoi diritti a norma di tale regolamento e, pertanto, deve riprodurre integralmente e fedelmente tali dati», e perciò comprendere non solo l'elenco dei dati personali sotto forma di tabella sintetica, ma anche la trasmissione di estratti o di documenti interi, nonché di estratti di banche dati, nei quali sono riprodotti detti dati (così CGUE, 4 maggio 2023, C- 487/21). Così, a esempio, il diritto del paziente di ottenere una copia della cartella clinica (v. considerando 63 GDPR) implica il diritto di ottenere una copia integrale dei documenti in essa contenuti quali «risultati di esami, pareri di medici curanti e terapie o interventi praticati» (così CGUE, 26 ottobre 2023, C-307/22).

4. Il diritto alla rettifica

Può capitare che, proprio a seguito dell'esercizio del diritto di accesso, l'interessato si renda conto della parzialità delle informazioni raccolte, della loro inesattezza o del loro carattere non aggiornato; per rimediare a tale situazione il Regolamento attribuisce all'interessato il diritto di ottenere, senza ingiustificato ritardo e in ogni caso entro un mese dal ricevimento della richiesta, la rettifica dei propri dati personali inesatti, ovvero l'aggiornamento o l'integrazione di quelli incompleti (art. 16 GDPR). Si tratta di un insieme di facoltà di natura strumentale, funzionali tra l'altro ad assicurare all'interessato, in un'ottica non necessariamente conflittuale ma anzitutto collaborativa e partecipativa, la piena rispondenza di sé alla propria rappresentazione collettiva (identità personale). In questa prospettiva, ad esempio, «il titolare di un organo di informazione è tenuto a garantire la contestualizzazione e l'aggiornamento della notizia di cronaca, successivamente spostata nell'archivio storico anche se pubblicato su Internet, al fine di consentire alla medesima di mantenere i caratteri di verità ed esattezza e quindi di liceità e correttezza, a tutela del diritto dell'interessato al trattamento alla propria identità personale o morale nonché a salvaguardia del diritto del cittadino utente di ricevere un'informazione completa e corretta» (Cass. 5 aprile 2012, n. 5525). Sempre al fine di assicurare l'effettività del diritto all'identità personale, è stato stabilito che l'esercizio del diritto di rettifica dei dati personali relativi all'identità di genere di una persona fisica, contenuti in un registro pubblico non può essere subordinata alla prova di un trattamento chirurgico di riassegnazione sessuale (CGUE, 13 marzo 2025, C-247/23).

5. Il diritto alla limitazione del trattamento

Accade di frequente che, richiesta la rettifica dei dati personali, trascorra un certo periodo di tempo, necessario per consentire al titolare di svolgere le opportune verifiche, prima che essi siano corretti, durante il quale i dati personali continuano a circolare. Proprio per impedire, tra gli altri, tale esito l'interessato può, ai sensi dell'art. 18, par. 1, lett. a) GDPR, domandare al titolare la limitazione del trattamento, per tale intendendosi «il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro». Si tratta di una facoltà di natura cautelare e strumentale, sia perché il suo esercizio impedisce che il titolare, in presenza di un trattamento illecito o di un trattamento che abbia assolto la sua finalità, cancelli i dati personali che dovessero essere necessari all'interessato per far valere in giudizio un proprio diritto, sia perché il suo esercizio sospende, in attesa che sia il titolare decida sull'opposizione manifestata dal titolare o sulla richiesta di rettifica, ogni ulteriore trattamento diverso dalla mera conservazione dei dati personali. Lo si ricava dal par. 2, a mente del quale se il trattamento è limitato i dati personali possono essere oggetto di un trattamento diverso dalla mera conservazione solo se: a) l'interessato ha prestato il consenso; il trattamento è necessario b) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria (va da sé, da parte del titolare o di un soggetto diverso dall'interessato); c) per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante dell'Unione o di uno Stato membro.

6. Il diritto alla cancellazione

Se il diritto alla limitazione ha una chiara natura rimediale – che si ricava dalla strumentalità dei dati rispetto all'esercizio di un diritto o alla difesa in giudizio – il diritto alla cancellazione, a differenza che in passato, ha invece un ambito applicativo che travalica le ipotesi di trattamento illecito. Invero, di là dall'ipotesi prevista dall'art. 17, par. 1, lett. d) GDPR, l'interessato ha diritto di ottenere la cancellazione dei dati personali che lo riguardano, senza ingiustificato ritardo, quando: a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati; b) l'interessato ha revocato il consenso su cui si basa il trattamento conformemente all'articolo 6, par. 1, lettera a) GDPR, o all'articolo 9, par. 2, lettera a) GDPR e non sussiste altro fondamento giuridico per il trattamento; c) l'interessato si è opposto al trattamento ai sensi dell'articolo 21, par. 1 GDPR e «non sussistano motivi legittimi prevalenti sugli interessi, nonché sui diritti e sulle libertà di questa persona ai sensi dell'articolo 21, par. 1, del RGPD, circostanza che spetta al titolare del trattamento dimostrare» (CGUE, 7 dicembre 2023, C-26/22 e C-64/22); d) l'interessato si è opposto al trattamento ai sensi dell'articolo 21, par. 2 GDPR (finalità di marketing diretto); e) i dati personali devono essere cancellati per adempiere un obbligo giuridico 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 a minori.

Merita di precisare come, di là dalle «situazioni-presupposto» indicate alla lett. b) e c) nelle quali l'iniziativa è dell'interessato, nelle altre ipotesi la cancellazione integra anche un obbligo che il titolare è tenuto ad assolvere di propria iniziativa.

Il par. 2 dell'articolo in commento, in linea di continuità con quanto previsto dall'art. 19 GDPR, prevede, poi, a carico del titolare che abbia reso pubblici i dati personali dell'interessato e che è tenuto alla loro cancellazione (es. l'editore di un giornale online), l'obbligo di informare gli ulteriori titolari del trattamento che stanno trattando quei dati personali (es. il motore di ricerca, le piattaforme di condivisione di file audio e video) della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali. Secondo la giurisprudenza, il titolare del trattamento dovrebbe porre in essere «ogni iniziativa volta a rendere edotti (e persuadere) i terzi che se ne siano appropriati circa l'illegittima diffusione» dei dati personali. Si tratta di un'attività che, tuttavia, «non implica la certezza dell'adempimento richiesto ai terzi, ma presuppone la doverosa attività volta a ottenere la cessazione dell'illegittimo trattamento dei dati personali da parte dei terzi, venendo cioè in rilievo solo un'obbligazione di mezzi, non certo di risultato» (così Cass. 5 aprile 2024, n. 9068).

6.1. Il diritto all'oblio

Naturalmente, il diritto alla protezione dei dati personali non è un diritto assoluto, ma – come sottolinea il considerando 4 del Regolamento – deve essere considerato in relazione alla sua funzione sociale ed essere bilanciato con gli altri diritti fondamentali, di talché all'interessato può essere negata la cancellazione qualora i dati personali siano necessari, tra l'altro, per l'esercizio del diritto alla libertà di espressione o di informazione (art. 17, par. 3, lett. a) GDPR).

L'esito del bilanciamento può, tuttavia, assumere esiti differenti in ragione del trascorrere del tempo: una notizia legittimamente divulgata al momento della sua pubblicazione, col trascorrere del tempo può sollecitare un interesse alla sua rimozione. In quest'accezione si può parlare di diritto alla cancellazione come sinonimo di diritto all'oblio, inteso, come interesse di ogni persona a non restare indeterminatamente esposta alla reiterata pubblicazione di una notizia in passato legittimamente divulgata allorquando, in considerazione del tempo trascorso, sia da considerarsi venuto meno l'interesse pubblico alla notizia stessa. A dispetto della rubrica dell'art. 17 GDPR, non v'è assoluta coincidenza tra il diritto alla cancellazione e il diritto all'oblio; per un verso, come è evidente, l'ambito di applicazione del diritto alla cancellazione è più ampio di quello del diritto all'oblio; per altro verso, di diritto all'oblio si discute anche (seppure impropriamente) con riguardo alla richiesta di contestualizzazione e aggiornamento di una notizia (non più attuale) e, dunque, ad una pretesa che va ricondotta, più correttamente, al diritto alla rettifica.

È possibile isolare almeno tre modi di declinare il diritto all'oblio: il primo, più risalente, è quello che emerge dal conflitto tra il diritto alla riservatezza e il diritto di cronaca (o, come affermato di recente da Cass. s.u. 22 luglio 2019, n. 19681, «il diritto alla rievocazione storica (storiografica) di quei fatti») e si manifesta nella cancellazione di una notizia che, al momento della sua ripubblicazione, non è più attuale. La prevalenza del diritto alla riservatezza mediante l'accoglimento della domanda di cancellazione (o di anonimizzazione) è legata ai consueti criteri dell'assenza di un contributo arrecato dalla diffusione dell'immagine o della notizia ad un dibattito di interesse pubblico; della prevalenza di un interesse divulgativo o, peggio, meramente economico o commerciale del soggetto che diffonde la notizia o l'immagine; dello scarso grado di notorietà del soggetto rappresentato.

Il secondo modo di declinare il diritto all'oblio è quello che emerge dal conflitto tra il diritto alla riservatezza e l'esercizio della libertà di iniziativa economica di un motore di ricerca e si manifesta nella richiesta di soppressione, dall'elenco dei risultati che appare a seguito di una ricerca effettuata a partire dal nome di una persona, dei *link* verso pagine web pubblicate da terzi e contenenti informazioni relative a tale persona (c.d. *deindicizzazione*).

Dalla lettura della giurisprudenza si ricava che: a) la richiesta di deindicizzazione di un link ad un sito internet di un giornale online – il cui fondamento può essere rintracciato nell'art. 17 GDPR (sul presupposto della sopravvenuta inesattezza delle informazioni o dell'esaurimento delle finalità del trattamento) ovvero nell'art. 21 GDPR (sul presupposto che col trascorrere del tempo il bilanciamento tra il legittimo interesse del titolare e il diritto alla riservatezza penda in favore dell'interessato) – può essere formulata nei confronti del motore di ricerca indipendentemente da una preventiva domanda di cancellazione nei confronti del gestore del sito internet (CGUE, 13 maggio 2014, C-131/12); b) il diritto alla deindicizzazione può essere esercitato senza la necessità di provare che «l'inclusione dell'informazione in questione nell'elenco dei risultati arrechi un pregiudizio all'interessato» con il solo limite della eventuale prevalenza di «un interesse preponderante del pubblico ad avere accesso, nel contesto di una ricerca siffatta a dette informazioni» per il ruolo ricoperto dall'interessato nella vita pubblica (CGUE, 13 maggio 2014, C-131/12); ciò significa che una volta che l'interessato abbia domandato la deindicizzazione «per motivi connessi alla sua situazione particolare» (art. 21 GDPR) «se il fornitore del motore di ricerca non dimostra l'esistenza di un motivo legittimo prevalente, l'interessato ha il diritto di ottenere la deindicizzazione ai sensi dell'articolo 17, par. 1, lettera c), del RGPD» (così *EDPB Linee guida 5/2019 sui criteri per l'esercizio del diritto all'oblio nel caso dei motori di ricerca, ai sensi del RGPD, adottate il 7 luglio 2020*); c) l'interessato che ha formulato una richiesta di deindicizzazione sul presupposto dell'inesattezza dei dati (art. 17, par. 1, lett. a) GDPR), deve apportare elementi di prova «pertinenti e sufficienti idonei a suffragare la sua richiesta e atti a dimostrare il carattere manifestamente inesatto delle informazioni» ma l'eventuale deindicizzazione «non è subordinata alla condizione che la questione dell'esattezza del contenuto indicizzato sia stata risolta, alme-

no provvisoriamente, nel quadro di un'azione legale intentata da detta persona contro il fornitore di tale contenuto» (CGUE, 8 dicembre 2022, C-460/20); d) il motore di ricerca non è tenuto alla deindicizzazione su tutte le versioni del motore di ricerca, ma solo nelle versioni corrispondenti a tutti gli Stati membri, ferma restando la competenza dell'autorità di controllo o dell'autorità giudiziaria nazionali a richiedere al gestore di effettuare una deindicizzazione su tutte le versioni del suddetto motore (CGUE, 24 settembre 2019, C-507/17); d) qualora il gestore di un motore di ricerca dovesse opporsi alla deindicizzazione in ragione del persistente interesse della collettività ad accedere a quel risultato di ricerca, «tale gestore è in ogni caso tenuto, al più tardi al momento della richiesta di deindicizzazione, a sistemare l'elenco dei risultati in modo tale che l'immagine globale che ne risulta per l'utente di Internet rifletta la situazione attuale», il che necessita che compaiano per primi, nell'elenco dei risultati, i link verso le pagine contenenti le informazioni aggiornate (CGUE, 24 settembre 2019, C-136/17).

Il terzo modo di declinare il diritto all'oblio emerge dal conflitto tra il diritto alla protezione dei dati personali e il diritto all'informazione (che si risolve, in particolare, nell'istanza di conservazione della memoria del passato in funzione storica e archivistica) e si manifesta nella richiesta di rimozione degli articoli in questione dell'archivio online di un quotidiano. Una recente pronuncia della Cassazione (Cass. 31 gennaio 2023, n. 2893) – che, sul punto, si è discostata dalla soluzione offerta dalla Corte Edu, nel caso Hurbain (4 luglio 2023) – ha affermato che «la cancellazione tout court degli articoli dall'archivio online del quotidiano annichilirebbe con l'iperprotezione dei diritti alla riservatezza degli interessati la funzione di memoria storica e documentale dell'archivio del giornale» e che «una via adeguata di contemperamento non è neppure quella della manipolazione del testo con l'introduzione di pseudonimi sostitutivi o omissioni nominative». In tal modo, «la memoria storica dell'archivio diverrebbe incompleta e falsata e così se ne perderebbe la funzione». Un punto di equilibrio accettabile è rappresentato dalla «richiesta di aggiornamento mediante la mera apposizione agli articoli di una nota informativa volta a dar conto del successivo esito dei procedimenti giudiziari con l'assoluzione degli interessati e il risarcimento del danno per ingiusta detenzione».

7. L'obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento

Nell'ipotesi in cui l'interessato abbia ottenuto la rettifica, la cancellazione ovvero la limitazione di trattamento dei propri dati personali, il titolare, ai sensi dell'art. 19 GDPR è tenuto, per un verso, a comunicare ai destinatari (secondo la definizione offerta dall'art. 1, par. 1, n. 9) GDPR) le rettifiche, le cancellazioni e le limitazioni di trattamento effettuate, a meno che ciò non si riveli impossibili o eccessivamente oneroso; per altro verso, a informare l'interessato dell'identità dei destinatari ai quali ha effettuato la predetta comunicazione.

8. Il diritto di opposizione

Manifestazione massima del potere autodeterminativo dell'interessato, funzionalmente affine alla revoca del consenso dalla quale, però, si differenzia anzitutto perché è concesso unicamente per i trattamenti effettuati ai sensi dell'art. 6, par. 1, lett. e) ed f) GDPR, compresa la profilazione sulla base di tali disposizioni, il diritto di opposizione consente all'interessato – in ogni tempo – di inibire l'ulteriore prosecuzione del trattamento e, dunque, ferma restando la liceità delle operazioni svolte prima dell'opposizione, di esercitare un potere di controllo sull'estensione del trattamento di dati che lo riguardino.

Ciò si verifica: (i) senza condizionamenti – e anche in via preventiva (cfr. art. 130, co. 3-bis, d.lgs. 196/2003) – qualora i dati sono trattati per finalità di marketing diretto (art. 21, par. 2 e 3 GDPR); (ii) qualora sopravvengano motivi connessi alla situazione particolare dell'interessato e, all'esito di una ponderazione di interessi, emerga che il titolare non abbia motivi legittimi cogenti per procedere al trattamento «che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria»; (iii) qualora sopravvengano motivi connessi alla situazione particolare dell'interessato e il trattamento per finalità di ricerca, storiche o statistiche non si riveli necessario per l'esecuzione di un compito di interesse pubblico.

Se ne ricava un ulteriore tratto di differenza rispetto alla revoca del consenso, la quale, a differenza dell'opposizione, in nessun caso necessita della dimostrazione da parte dell'interessato di ragioni sopravvenute legate alla propria situazione personale. A integrazione di quanto previsto dagli artt. 13 e 14, l'art. 21, par. 4 GDPR stabilisce (perlomeno con riferimento alle opposizioni disciplinate dai paragrafi 1 e 2) che l'interessato debba essere edotto della possibilità di opporsi in termini chiari e «separati da qualsiasi altra informazione», al più tardi al momento della prima comunicazione all'interessato.

9. Processi decisionali automatizzati e diritti dell'interessato

La specifica previsione del diritto di opposizione anche nel caso in cui il trattamento, necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare ovvero per il perseguimento del legittimo interesse del titolare o di terzi, consista e abbia come finalità la profilazione dell'interessato (a es. per finalità di *marketing* diretto), sembrerebbe discordare con la disciplina dettata dall'art. 22 GDPR.

La norma, infatti, dopo aver stabilito un divieto generale (così, infatti, va intesa l'espressione «l'interessato ha il diritto di non essere sottoposto…») nei confronti della «decisione basata unicamente sul trattamento automatizzato, compresa la profilazione», che produca effetti giuridici o incida in modo analogo significativamente sull'interessato, prevede una serie di eccezioni. Per i dati comuni esse consistono: (i) nel consenso esplicito dell'interessato; (ii) nella necessità della decisione automatizzata per la conclusione o l'esecuzione del

contratto; (iii) nell'autorizzazione da parte del diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento. Per le categorie particolari di dati, alle summenzionate esenzioni, si aggiungono: (i) il consenso esplicito dell'interessato; (ii) la necessarietà 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.

La discordanza poc'anzi segnalata è, tuttavia, solo apparente e dipende dalla circostanza che la profilazione – cioè a dire «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» (art. 4, par. 1, n. 4 GDPR) – non necessariamente dà origine ad un processo decisionale nel quale è assente ogni valutazione significativa da parte dell'uomo ed è capace di produrre effetti giuridici o incidere in modo altrettanto significativo sull'interessato.

Nel campo di applicazione del divieto di cui all'art. 22 GDPR – oltre ai casi di decisioni assunte esclusivamente sulla base di trattamenti automatizzati diversi dalla proliferazione – ricadono, infatti, unicamente le ipotesi in cui: (i) la profilazione è la base per l'assunzione di una decisione che non implica alcuna previa valutazione significativa da parte di un essere umano (così nell'ipotesi in cui al risultato del calcolo della solvibilità di una persona sotto forma di tasso di probabilità relativo alla capacità di tale persona di onorare impegni di pagamento in futuro, svolto da una società che fornisce informazioni commerciale, segua la decisione *meramente formale* della banca di diniego alla concessione di un prestito; cfr., al riguardo, CGUE, 7 dicembre 2023, C-634/21); (ii) la decisione così assunta produce effetti giuridici o incide in modo analogo significativamente sull'interessato.

Come esempi del primo tipo le *Linee guida WP29 sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione*, adottate il 3 ottobre 2017, riportano la cancellazione di un contratto, la concessione o la negazione del diritto a una prestazione sociale; il rifiuto di ammissione in un paese o negazione della cittadinanza. Come esempi del secondo tipo, si menzionano le decisioni che influenzano le circostanze finanziarie di una persona, come la sua ammissibilità al credito; le decisioni che influenzano l'accesso di una persona ai servizi sanitari; le decisioni che negano a una persona un'opportunità di impiego o pongono tale persona in una posizione di notevole svantaggio; le decisioni che influenzano l'accesso di una persona all'istruzione, ad esempio le ammissioni universitarie (cfr., altresì, il considerando 71 GDPR).

In ragione dei potenziali effetti discriminatori o, comunque, iniqui di una decisione inferenziale induttiva puramente algoritmica (cfr. il considerando 71 GDPR), oltre alle già menzionate previsioni dettate dall'art. 13, par. 1,

lett. c) e par. 2, lett. f) GDPR, dall'art. 14, par. 1, lett. c) e par. 2, lett. g) GDPR e dall'art. 15, par. 1, lett. h) GDPR – che impongono al titolare di informare l'interessato non solo dell'esistenza di un trattamento per finalità di profilazione (e, quindi, del diritto di opporsi al trattamento qualora esso si basi sul legittimo interesse del titolare), indipendentemente dal fatto che si ricada nella fattispecie dell'art. 22 GDPR, ma anche, e a maggior ragione, di informare l'interessato dell'esistenza di un processo decisionale basato esclusivamente su un trattamento automatizzato, compresa la profilazione, e, quindi, della logica utilizzata (cfr., a riguardo, CGUE, 27 febbraio 2025, C-203/22) nonché dell'importanza e delle conseguenze previste per l'interessato – l'artt. 22, par. 3 GDPR, impone al titolare, qualora la decisione automatizzata sia necessaria per la conclusione o l'esecuzione di un contratto o si basi sul consenso esplicito dell'interessato, di adottare misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, tra le quali, almeno, il diritto dell'interessato di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione, di ottenere una spiegazione della decisione conseguita dopo tale valutazione e di contestare la decisione. In ogni caso, come si legge nel considerando 71 GDPR – è opportuno che «il titolare del trattamento utilizzi procedure matematiche o statistiche appropriate per la profilazione, metta in atto misure tecniche e organizzative adeguate al fine di garantire, in particolare, che siano rettificati i fattori che comportano inesattezze dei dati e sia minimizzato il rischio di errori e al fine di garantire la sicurezza dei dati personali secondo una modalità che tenga conto dei potenziali rischi esistenti per gli interessi e i diritti dell'interessato e impedisca, tra l'altro, effetti discriminatori nei confronti di persone fisiche sulla base della razza o dell'origine etnica, delle opinioni politiche, della religione o delle convinzioni personali, dell'appartenenza sindacale, dello status genetico, dello stato di salute o dell'orientamento sessuale, ovvero un trattamento che comporti misure aventi tali effetti. Il processo decisionale automatizzato e la profilazione basati su categorie particolari di dati personali dovrebbero essere consentiti solo a determinate condizioni».

10. Il diritto alla portabilità dei dati personali

Espressione della crescente tendenza alla circolazione dei dati personali, il diritto alla portabilità, previsto all'art. 20 GDPR, consiste, anzitutto, nel diritto di «ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti da un titolare di trattamento». Il diritto alla portabilità appare, dunque, concettualmente, come uno sviluppo del diritto di accesso (col quale ha in comune il risultato di fornire all'interessato copia dei dati oggetto di trattamento) dal quale, tuttavia, si differenzia giacché accentua la dimensione dinamica (circolatoria) del potere di controllo sulle proprie informazioni e, in questa misura, diviene strumento di regolazione del mercato e di promozione della concorrenza. La portabilità infatti, nella misura in cui rafforza le possibilità di scelta tra più fornitori, attenu-

ta il vincolo di dipendenza dell'interessato da un determinato soggetto (c.d. vincoli di *lock-in*) e, nel contempo, assume una spiccata valenza pro-concorrenziale e anti-monopolistica eliminando le barriere tecniche e giuridiche nella competizione tra operatori (cfr. *EDPB Linee-guida sul diritto alla "portabilità dei dati", adottate il 5 aprile 2017*). A tal fine assume particolare importanza l'esigenza di assicurare, quanto più possibile, l'interoperabilità dei formati, come sottolineato dal considerando n. 38 GDPR, il quale tuttavia esclude l'esistenza di un «obbligo per i titolari del trattamento di adottare o mantenere sistemi di trattamento tecnicamente compatibili» (considerando 68 GDPR). L'esercizio di tale diritto è subordinato alla presenza di tre requisiti: a) il trattamento dei dati dovrà avvenire sulla base del consenso o della necessità contrattuale (con esclusione, dunque, *inter alia*, dei trattamenti svolti dai titolari «nell'esercizio delle loro funzioni pubbliche» e di quelli «necessari per l'adempimento di un obbligo legale 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»; cfr. art. 20, par. 3) GDPR); b) il trattamento dovrà avvenire con mezzi automatizzati; c) i dati personali oggetto del trattamento devono riguardare l'interessato ed essere forniti da quest'ultimo (con esclusione, dunque, dei dati anonimi e dei dati inferenziali, cioè a dire di quelli che, a differenza dei dati anche passivamente forniti dall'interessato (c.d. dati grezzi: cronologia di navigazione o delle ricerche, i dati di traffico e di localizzazione), sono 'creati' dal titolare). A queste condizioni, il titolare potrà ottenere non soltanto che gli siano forniti i propri dati personali così da conservarli sul proprio terminale ovvero trasmetterli a un altro titolare senza impedimenti da parte dell'originario titolare (par. 1), ma potrà ottenere anche che tali dati siano traferirti direttamente al nuovo titolare qualora ciò sia tecnicamente fattibile (par. 2). Oltre alle condizioni e ai limiti sopra elencati, l'esercizio del diritto alla portabilità non può ledere i diritti e le libertà dei terzi: così, a esempio, la portabilità va esclusa qualora abbia ad oggetto informazioni riguardanti contemporaneamente più persone fisiche individuabili (es. mittente e destinatario di una comunicazione) sempre che il suo esercizio impedisca al terzo di esercitare i suoi diritti in qualità di interessato. Tra i diritti dei terzi figurano anche i diritti di proprietà intellettuale, le informazioni commerciali riservate e i segreti industriali che tutelano i *software*: in questo caso, tuttavia, la presenza di tali interessi non è da sola in grado di giustificare un diniego alla richiesta di portabilità, ma sarà al più capace di imporre di adeguare le concrete modalità di esercizio del diritto al rispetto dei diritti altrui. Il par. 3 chiarisce, infine, che l'esercizio del diritto alla portabilità determina semplicemente una duplicazione dei dati personali e non comporta affatto la loro cancellazione, la quale, dunque, qualora ne ricorrano i presupposti, dovrà essere autonomamente azionata (cfr. considerando 68 GDPR, secondo cui l'esercizio del diritto alla portabilità dei dati personali «non dovrebbe segnatamente implicare la cancellazione dei dati personali riguardanti l'interessato forniti da quest'ultimo per l'esecuzione di un contratto, nella misura in cui e fintantoché i dati personali siano necessari all'esecuzione di tale contratto»).

LA TUTELA POST-MORTEM

Il GDPR al considerando 27 afferma che «Il presente regolamento non si applica ai dati personali delle persone decedute», lasciando tuttavia liberi gli Stati membri di «prevedere norme riguardanti il trattamento dei dati personali delle persone decedute». Il legislatore italiano ha rimodulato la disciplina precedente prevedendo, all'art. 2-terdecies cod. privacy, (i) l'esercizio dei diritti sui dati che riguardano il defunto da parte di soggetti diversi dall'interessato, (ii) il potere di autodeterminazione dell'interessato in ordine alla all'esercizio dei diritti sui propri dati per il tempo in cui avrà cessato di vivere, (iii) un raccordo tra l'autodeterminazione informativa dell'interessato e i diritti patrimoniali derivanti dalla morte di quest'ultimo.

In particolare, il primo comma, stabilisce che «i diritti di cui agli articoli da 15 a 22 (accesso, rettifica, cancellazione, portabilità e opposizione) 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».

L'interessato, dunque, oltre a poter incaricare, mediante un contratto di mandato, un determinato soggetto dell'esercizio dei summenzionati diritti, può – «limitatamente all'offerta diretta di servizi della società dell'informazione» – impedire «con dichiarazione scritta presentata al titolare del trattamento o a quest'ultimo comunicata» che uno o più diritti vengano esercitati dai soggetti altrimenti legittimati.

Tale potere, tuttavia, non può escludere «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». Così, a esempio, l'interessato non può vietare agli eredi di accedere al contenuto delle proprie email qualora esso sia indispensabile per accertare la consistenza del patrimonio ereditare e valutare se accettare l'eredità col beneficio d'inventario.

Quanto alla volontà dell'interessato di vietare l'esercizio dei predetti diritti essa – stabilisce il secondo comma dell'art. 2-terdecies cod. privacy – oltre ad essere sempre revocabile e modificabile, «deve risultare in modo non equivoco e deve essere specifica, libera e informata».

Riferimenti bibliografici

Battelli, Ettore, e Guido D'Ippolito 2019. "Il diritto alla portabilità dei dati personali." In *Privacy Digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, a cura di E. Tosi, 185-227. Torino: Giappichelli.

Berti Suman, Adele 2019. "Il diritto alla cancellazione." In *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento (UE) 146 n. 2016/679 (GDPR) e al novellato d.lgs. n. 196/2003 (Codice Privacy)*, a cura di R. Panetta, 199-214. Milano: Franco Angeli.

Bianchi, L. 2019. "Il diritto alla portabilità dei dati." In *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento (UE) 146 n. 2016/679 (GDPR) e al novellato d.lgs. n. 196/2003 (Codice Privacy)*, a cura di R. Panetta, 223-38. Milano: Franco Angeli.

Calisai, F. 2019. "I diritti dell'interessato." In *I dati personali nel diritto europeo*, a cura di V. Cuffaro, R. D'Orazio e V. Ricciuto. Torino: Giappichelli.

Comandé, G. 2021. "Art. 21." In *Codice della privacy e data protection*, a cura di R. D'Orazio, G. Finocchiaro, O. Pollicino e G. Resta. Milano: Giuffrè.

Confortini, V. 2023. *Persona e patrimonio nella successione digitale*. Torino: Giappichelli.

Cristofari, G. 2019. "Il diritto alla limitazione del trattamento." In *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al*

Regolamento (UE) 146 n. 2016/679 (GDPR) e al novellato d.lgs. n. 196/2003 (Codice Privacy), a cura di R. Panetta. Milano: Franco Angeli.
Cuffaro, V. 2019. "Cancellare i dati personali. Dalla damnatio memoriae al diritto all'oblio." In *Persona e mercato dei dati. Riflessioni sul GDPR*, a cura di N. Zorzi Galgano. Milano: Franco Angeli.
Cuffaro, V., V. Ricciuto e V. Zeno-Zencovich 1999. *Il trattamento dei dati personali. II, Profili applicativi*. Torino: Giappichelli.
Davide, Achille 2019. "Art. 12 – Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato." In *Delle persone. Leggi collegate*, vol. II, a cura di A. Barba e S. Pagliantini, 204-217. Milano: Gabrielli.
Di Ciommo, F. 2019. "Diritto alla cancellazione, diritto di limitazione del trattamento e diritto all'oblio." In *I dati personali nel diritto europeo*, a cura di V. Cuffaro, R. D'Orazio e V. Ricciuto. Torino: Giappichelli.
Di Lorenzo, G. 2019. "Spunti di riflessione su taluni «Diritti dell'interessato»." In *Persona e mercato dei dati. Riflessioni sul GDPR*, a cura di N. Zorzi Galgano. Milano: Franco Angeli.
Durante, M. 2019. "Art. 13 – Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato." In *Delle persone. Leggi collegate*, vol. II, a cura di A. Barba e S. Pagliantini, in Comm. c.c. Milano: Gabrielli.
Durante, M. 2019. "Art. 14 – Informazioni da fornire qualora i dati personali non siano stati ottenuti presso l'interessato." In *Delle persone. Leggi collegate*, vol. II, a cura di A. Barba e S. Pagliantini, in Comm. c.c. Milano: Gabrielli.
Durante, M. 2019. "Art. 15 – Diritto d'accesso dell'interessato." In *Delle persone. Leggi collegate*, vol. II, a cura di A. Barba e S. Pagliantini, in Comm. c.c. Milano: Gabrielli.
Falce, V. 2021. "Art. 20." In *Codice della privacy e data protection*, a cura di R. D'Orazio, G. Finocchiaro, O. Pollicino e G. Resta. Milano: Giuffrè.
Finocchiaro, G. 2021. "Art. 17." In *Codice della privacy e data protection*, a cura di R. D'Orazio, G. Finocchiaro, O. Pollicino e G. Resta. Milano: Giuffrè.
Fraioli, M. 2019. "Il diritto di opposizione e la revoca del consenso." In *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento (UE) 146 n. 2016/679 (GDPR) e al novellato d.lgs. n. 196/2003 (Codice Privacy)*, a cura di R. Panetta. Milano: Franco Angeli.
Gambino, A., e M. Siragusa. 2021. "Art. 15." In *Codice della privacy e data protection*, a cura di R. D'Orazio, G. Finocchiaro, O. Pollicino e G. Resta. Milano: Giuffrè.
Genovese, A. 2021. "Art. 12." In *Codice della privacy e data protection*, a cura di R. D'Orazio, G. Finocchiaro, O. Pollicino e G. Resta. Milano: Giuffrè.
Gianello, S. 2021. "Art. 16." In *Codice della privacy e data protection*, a cura di R. D'Orazio, G. Finocchiaro, O. Pollicino e G. Resta. Milano: Giuffrè.
Giannone Codiglione, G. 2021. "Artt. 18-19." In *Codice della privacy e data protection*, a cura di R. D'Orazio, G. Finocchiaro, O. Pollicino e G. Resta. Milano: Giuffrè.
Giorgianni, M. 2019. "Art. 20 – Diritto alla portabilità dei dati." In *Delle persone. Leggi collegate*, vol. II, a cura di A. Barba e S. Pagliantini, in Comm. c.c. Milano: Gabrielli.
Lagioia, F., G. Sartor e A. Simoncini. 2021. "Art. 22." In *Codice della privacy e data protection*, a cura di R. D'Orazio, G. Finocchiaro, O. Pollicino e G. Resta. Milano: Giuffrè.
Liguori, L. 2021. "Artt. 13-14." In *Codice della privacy e data protection*, a cura di R. D'Orazio, G. Finocchiaro, O. Pollicino e G. Resta. Milano: Giuffrè.
Livi, M. A. 2019. "Art. 16 – Diritto di rettifica; Art. 17 – Diritto alla cancellazione («diritto all'oblio»)." In *Delle persone. Leggi collegate*, vol. II, a cura di A. Barba e S. Pagliantini, in Comm. c.c. Milano: Gabrielli.

Montanaro, D. 2019. "Il diritto di accesso ai dati personali e il diritto di rettifica." In *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento (UE) 146 n. 2016/679 (GDPR) e al novellato d.lgs. n. 196/2003 (Codice Privacy)*, a cura di R. Panetta. Milano: Franco Angeli.

Patti, L., e O. Sesso Sarti. 2019. "Art. 22 – Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione." In *Delle persone. Leggi collegate*, vol. II, a cura di A. Barba e S. Pagliantini, in Comm. c.c. Milano: Gabrielli.

Pelino, E. 2016. "I diritti dell'interessato." In *Il Regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*. Milano: Giuffrè.

Piraino, F. 2019. "I "diritti dell'interessato", nel Regolamento generale sulla protezione dei dati personali." *Giur. it.*

Rende, F. 2019. "Art. 18 – Diritto di limitazione di trattamento." In *Delle persone. Leggi collegate*, vol. II, a cura di A. Barba e S. Pagliantini, in Comm. c.c. Milano: Gabrielli.

Rende, F. 2019. "Art. 21 – Diritto di opposizione." In *Delle persone. Leggi collegate*, vol. II, a cura di A. Barba e S. Pagliantini, in Comm. c.c. Milano: Gabrielli.

Renna, M. 2019. "Art. 19 – Obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento." In *Delle persone. Leggi collegate*, vol. II, a cura di A. Barba e S. Pagliantini, in Comm. c.c. Milano: Gabrielli.

Ricci, A. 2017. "I diritti dell'interessato." In *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, a cura di G. Finocchiaro. Bologna: Il Mulino.

Riccio, G. M., e F. Pezza. 2019. "Portabilità dei dati personali e interoperabilità." In *I dati personali nel diritto europeo*, a cura di V. Cuffaro, R. D'Orazio e V. Ricciuto. Torino: Giappichelli.

Sammarco, P. 2019. "Privacy digitale, motori di ricerca e social network: dal diritto di accesso e rettifica al diritto all'oblio condizionato." In *Privacy Digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, a cura di E. Tosi. Torino: Giappichelli.

Simoncini, A. 2021. "Art. 22." In *Codice della privacy e data protection*, a cura di R. D'Orazio, G. Finocchiaro, O. Pollicino e G. Resta. Milano: Giuffrè.

Siragusa, M., e A. M. Gambino. 2021. "Art. 15." In *Codice della privacy e data protection*, a cura di R. D'Orazio, G. Finocchiaro, O. Pollicino e G. Resta. Milano: Giuffrè.

Troiano, S. 2019. "Il diritto alla portabilità dei dati." In *Persona e mercato dei dati. Riflessioni sul GDPR*, a cura di N. Zorzi Galgano. Milano: Franco Angeli.

Tuccari, E. 2022. "I diritti dell'interessato." In *Manuale di diritto privato delle nuove tecnologie*, a cura di G. Magri, S. Martinelli e S. Thobani. Torino: Giappichelli.

Le intersezioni fra disciplina in materia di dati personali e diritto dei consumatori

Chiara Angiolini

Abstract: The interplay between data and consumer protection arises from several law provisions. First, the EU directive 2019/770 on digital content and services contracts is analysed because of the reference to the economic exploitation of consumer data. Then, the chapter addresses the interplay between data and protection and consumer law rules concerning unfair commercial practices and unfair clauses. The last paragraph concerns rules on consumer collective redress for GDPR infringements.

Keywords: Commodification of consumer data, digital content and service contracts, unfair terms, unfair commercial practices, class actions

1. Diritto dei consumatori e trattamento dei dati. Le intersezioni

È cosa nota la continua crescita delle attività economiche che hanno come fulcro la raccolta e il successivo trattamento dei dati personali, spesso attraverso ambienti digitali (es. i *social network*). Tale trattamento non di rado è volto ad acquisire conoscenze sugli interessati che servono a influenzarne le scelte, comprese quelle di natura economica, come sottolineato anche dal Comitato Europeo per la Protezione dei Dati (d'ora in avanti: EDPB) in relazione alla profilazione e il *targeting* (EDPB, *Linee guida 8/2020 sul targeting degli utenti di social media*, 13 aprile 2021).

In questo contesto, come affrontare dal punto di vista giuridico la crescente rilevanza economica del trattamento dei dati personali è una questione cruciale. In tema, in particolare con riguardo al rapporto tra l'interessato e il titolare del trattamento, la dottrina, la giurisprudenza e il legislatore europeo, hanno guardato, alle intersezioni tra il diritto dei consumatori e quello della protezione dei dati, spesso con un approccio volto a valorizzarne la complementarità.

In via preliminare, occorre rilevare che, perché un'intersezione fra diverse discipline ci sia, l'interessato (sulla definizione v. cap. *Le definizioni fondamen-*

Chiara Angiolini, University of Siena, Italy, chiara.angiolini@unisi.it

Referee List (DOI 10.36253/fup_referee_list)
FUP Best Practice in Scholarly Publishing (DOI 10.36253/fup_best_practice)

tali, § 2) deve essere qualificato anche come consumatore, cioè come «la persona fisica che agisce per scopi estranei all'attività imprenditoriale, commerciale, artigianale o professionale eventualmente svolta» (art. 3, co. 1, lett. a), d.lgs. 206/2005, d'ora in avanti: cod. cons.).

A fronte di tale quadro, in questo capitolo si illustreranno alcune delle intersezioni più evidenti fra il diritto dei consumi e la disciplina in materia di trattamento dei dati personali.

2. Fornitura di contenuti e servizi digitali e trattamento dei dati personali dei consumatori

Come si è visto nell'analisi delle basi giuridiche del trattamento (v. *supra* cap. *La disciplina dell'attività di trattamento*, sez. I), quest'ultimo può avere rilevanza nell'ambito dell'esecuzione di un contratto. Invero, se un trattamento dei dati personali è necessario a tale esecuzione, sussiste una condizione che rende lecito tale trattamento (art. 6, par. 1, lett. b), Reg. UE 2016/679 (d'ora in avanti: GDPR). Al di là di questa previsione, già presente nella direttiva 95/46/CE, il legislatore, tanto europeo quanto nazionale, per diverso tempo non ha prestato attenzione ai rapporti che possono intercorrere fra un trattamento di dati personali e una vicenda contrattuale.

L'approccio è cambiato in virtù della crescente presa di coscienza, da un lato, del valore patrimoniali dei dati personali e, dall'altro, della funzione svolta da determinati trattamenti nell'ambito di relazioni economiche.

Il caso più emblematico è rappresentato da quei servizi digitali (ad esempio, servizi di *social networking*, di archiviazione *cloud*) o contenuti digitali (ad esempio, programmi informatici, applicazioni per *smartphone*) che vengono forniti, da un professionista (cioè, un operatore economico), senza la richiesta di un corrispettivo monetario, bensì per ottenere, di solito a fini economici, i dati personali degli utenti.

Il legislatore europeo ha deciso di occuparsi di tale fenomeno all'interno del diritto dei consumatori, scelta che è stata criticata da parte della dottrina in quanto esclude la possibilità di una disciplina unitaria dei rapporti patrimoniali relativi ai dati personali (Angiolini, 2023). Guardando al dettato normativo, l'art. 3 della direttiva 2019/770/UE prevede che si applichino le tutele previste da tale direttiva anche nel caso in cui l'operatore economico fornisce o si impegna a fornire un contenuto digitale o un servizio digitale al consumatore e il consumatore fornisce o si impegna a fornire dati personali all'operatore economico, fatto salvo il caso in cui i dati personali forniti dal consumatore siano trattati esclusivamente dall'operatore economico ai fini della fornitura del contenuto digitale o del servizio digitale a norma della direttiva 2019/770 o per consentire l'assolvimento degli obblighi di legge cui è soggetto l'operatore economico e quest'ultimo non tratti tali dati per scopi diversi da quelli previsti.

Quando si applica la direttiva l'operatore economico sarà obbligato a fornire il contenuto o il servizio digitale promesso, in conformità a quanto previsto dal contratto e, in ogni caso, senza difetti oggettivi che ne impediscano il corretto funzionamento e utilizzo.

Prendendo spunto da quest'intervento, il legislatore europeo ha altresì esteso le norme previste dalla direttiva 2011/83/UE (che stabiliscono, in particolar modo, diversi obblighi informativi precontrattuali a carico del professionista) anche ai contratti di fornitura di contenuti e servizi digitali nei quali il consumatore non paga un prezzo, ma fornisce dati personali (v. art. 4, n. 2), lett. b), direttiva 2019/2161/UE: c.d. direttiva *omnibus*). Infatti, l'art. 3 della direttiva 2011/83, come novellata, prevede che

> La presente direttiva si applica anche se il professionista fornisce o si impegna a fornire un contenuto digitale mediante un supporto non materiale o un servizio digitale al consumatore e il consumatore fornisce o si impegna a fornire dati personali al professionista, tranne i casi in cui i dati personali forniti dal consumatore siano trattati dal professionista esclusivamente ai fini della fornitura del contenuto digitale su supporto non materiale o del servizio digitale a norma della presente direttiva o per consentire l'assolvimento degli obblighi di legge cui il professionista è soggetto, e questi non tratti tali dati per nessun altro scopo.

Il pagamento di un prezzo da parte del consumatore, dunque, non costituisce più un requisito indefettibile per l'applicazione di determinate regole di tutela nei suoi confronti, potendo ormai essere sostituito dalla fornitura di dati personali. Alla base di tali modifiche normative vi è, come si è anticipato, la consapevolezza che il trattamento di dati personali con finalità economiche può rappresentare una fonte remunerativa.

Da una prima lettura dei testi appena richiamati emergono almeno tre questioni rilevanti: i) l'interpretazione del termine «fornisce i dati»; ii) le basi giuridiche del trattamento in presenza delle quali si applica la dir. 2019/770 e la dir. 2011/83; iii) il rapporto fra applicazione della direttiva, trattamento dei dati personali e contratto.

Rispetto al primo profilo, anche alla luce dell'interpretazione data della medesima espressione dall'art. 20 GDPR in materia di diritto alla portabilità, l'espressione «fornisce» deve essere interpretata come relativa anche alle ipotesi in cui i dati sono raccolti dal titolare del trattamento attraverso l'osservazione dell'interessato, ma non include i dati inferiti a partire da quelli raccolti (sul diritto alla portabilità v. cap. *I diritti dell'interessato*).

Venendo alla seconda questione, l'art. 3 delle due direttive non fa riferimento al trattamento dei dati compiuto in virtù di una specifica base giuridica, seppur, se letto congiuntamente con il GDPR, si può escludere dall'ambito di applicazione della direttiva le ipotesi di dati raccolti e trattati secondo le basi giuridiche b) e c) previste dall'art. 6 GDPR, e dunque il caso in cui i dati siano necessari per l'esecuzione di un contratto, e l'ipotesi di adempimento di un obbligo legale (sulle basi giuridiche v. cap. *La disciplina dell'attività di trattamento*, sez. I). Dunque, la direttiva sarà applicabile quando il trattamento dei dati personali, che consiste nella raccolta dei dati «forniti», abbia come base giuridica il consenso dell'interessato e nei casi in cui la base giuridica sia il legittimo interesse ex art. 6, paragrafo 1, lett. f) GDPR. Risulta evidente come le basi giuridiche di cui

all'art. 6, paragrafo 1, lettere d) ed e) GDPR, rispettivamente relative ai trattamenti necessari alla salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica e all'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, siano di difficile applicazione in queste ipotesi.

Rispetto al rapporto fra applicazione della direttiva, trattamento dei dati personali e contratto, occorre sottolineare che la «fornitura» di dati personali o il relativo impegno da parte del consumatore – cui corrisponde un trattamento da parte del professionista, che consiste, almeno, nella raccolta di tali dati –, accanto alla fornitura o all'obbligo di fornitura da parte del professionista di un contenuto digitale (nella dir. 2011/83 mediante un supporto non materiale) o un servizio digitale sono elementi necessari e sufficienti ai fini dell'applicazione delle direttive sopra richiamate indipendentemente dalla sua attrazione o non attrazione nella sfera del contratto nel diritto nazionale.

Le nuove previsioni introdotte dall'UE sono state recepite, nell'ordinamento nazionale, all'interno del codice consumo (v. art. 46, par. 1-*bis* e artt. 135-*octies* e ss., d.lgs. 206/2005). La circostanza che una normativa, come il codice del consumo, diversa dal GDPR e dal codice privacy, prenda in considerazione alcuni aspetti relativi alla rilevanza economica del trattamento di dati personali, rischia di creare delle interferenze fra fonti legislative. In quest'ottica, l'art. 135-*novies*, co. 6, cod. cons. stabilisce che, in caso di conflitto fra le disposizioni consumeristiche e quelle in materia di protezione dei dati personali, la prevalenza va accordata a queste ultime.

L'ordine di preferenza che vede prevalere le norme di protezione dei dati personali può essere giustificato non tanto in ragione della superiorità di grado della fonte (la prevalenza, infatti, vale anche a prescindere da norme costituzionali), quanto in virtù di una gerarchia che può definirsi assiologica (il valore delle norme di protezione dei dati personali è giudicato superiore a quello delle norme di tutela del consumo).

Mentre le antinomie, cioè i contrasti fra norme esistenti, possono risolversi in virtù del criterio sopra richiamato, rimangono dubbi per la presenza di casi non disciplinati da alcuna norma, tanto consumeristica quanto di protezione dei dati personali.

In un contratto come quello di fornitura di contenuti o servizi digitali, che si fonda sul trattamento di dati personali del consumatore, non si chiarisce, ad esempio, quali siano gli effetti sul contratto qualora il consumatore eserciti, nella qualità di interessato, il diritto di revocare il proprio consenso al trattamento (art. 7, par. 3 GDPR). L'unico punto fermo è che la revoca non può rivelarsi pregiudizievole per l'interessato, il quale, altrimenti, sarebbe scoraggiato dall'esercitare un proprio diritto (v. considerando 42, GDPR e EDPB, Linee guida n. 5/2020 sul consenso ai sensi del regolamento (UE) 2016/679). Pertanto, il professionista non può certamente richiedere al consumatore un indennizzo, per la perdita di guadagni causata dall'impossibilità di continuare a trattare i dati personali per fini commerciali.

Sempre nell'ambito dei contratti di fornitura di contenuti o servizi digitali, può accadere che il fornitore violi, durante l'esecuzione del contratto, le re-

gole in materia di protezione dei dati personali (ad esempio, tratta più dati di quelli necessari per il perseguimento delle finalità del trattamento). In tal caso, il consumatore può indubbiamente esercitare i rimedi previsti dal GDPR contro il trattamento illecito dei dati personali, ma, dato il contesto contrattuale, la violazione delle norme di *data protection* può configurarsi, altresì, come un difetto di conformità del contenuto o servizio digitale. Il risultato pratico è che, in una situazione del genere, il consumatore può quindi avvalersi anche dei rimedi contro i difetti di conformità. Vale a dire: può richiedere il ripristino della conformità del contenuto o servizio digitale e, nei casi più gravi, così come nel caso in cui il ripristino fallisca oppure risulti impossibile o sproporzionato, il consumatore può richiedere la risoluzione del contratto di fornitura (v. considerando 48, direttiva 2019/770).

3. Pratiche commerciali scorrette e attività di trattamento

Nello studio delle intersezioni fra disciplina del trattamento dei dati personali e diritto dei consumatori è di particolare interesse l'ambito delle pratiche commerciali scorrette, regolato a livello europeo dalla dir. 2005/29, recepita sul piano nazionale con gli artt. 18 ss. cod. cons.. Tale disciplina è rilevante anche perché non è limitata all'ambito contrattuale, come risulta evidente *in primis* dall'articolo 3, par. 1, della dir. 2005/29/CE, secondo cui: «La presente direttiva si applica alle pratiche commerciali sleali tra imprese e consumatori [...] poste in essere prima, durante e dopo un'operazione commerciale relativa a un prodotto».

Rispetto agli intrecci fra le regole in materia di dati personali e quelle del codice del consumo, è utile chiedersi se e in quali casi il trattamento dei dati possa essere qualificato come pratica commerciale, e poi interrogarsi sulla possibile configurazione di ipotesi di scorrettezza.

Con riguardo al rapporto fra trattamento dei dati e pratiche commerciali, si può partire dalla definizione data dall'art. 18 cod. cons., secondo cui si definisce come pratica commerciale fra professionisti e consumatori: «qualsiasi azione, omissione, condotta o dichiarazione, comunicazione commerciale ivi compresa la pubblicità e la commercializzazione del prodotto, posta in essere da un professionista, in relazione alla promozione, vendita o fornitura di un prodotto ai consumatori».

Guardando alla giurisprudenza, il Consiglio di Stato ha affermato che per pratiche commerciali

> si intendono tutti i comportamenti tenuti da professionisti che siano oggettivamente «correlati» alla «promozione, vendita o fornitura» di beni o servizi a consumatori, e posti in essere anteriormente, contestualmente o anche posteriormente all'instaurazione dei rapporti contrattuali». (Cons. Stato, 29 marzo 2021, n. 2630)

Anche alla luce di quanto detto, occorre affrontare due aspetti:

1) le ipotesi in cui la disciplina in materia di pratiche commerciali scorrette risulterà applicabile;

2) i profili legati alla valutazione della scorrettezza della pratica.

Con riguardo al primo profilo, bisogna domandarsi se le condotte consistenti nel trattamento dei dati relativi ai consumatori possano essere qualificate in alcune ipotesi come «pratica commerciale» ai sensi del codice del consumo.

A tale interrogativo occorre dare risposta positiva, quando il trattamento dei dati da parte dei professionisti sia posto in essere in relazione alla promozione, vendita o fornitura di un prodotto ai consumatori.

Per individuare le ipotesi concrete, è di interesse la Comunicazione «Orientamenti sull'interpretazione e sull'applicazione della direttiva 2005/29/CE» del 29 dicembre 2021, dove la Commissione Europea evidenzia il valore economico derivante da alcuni trattamenti dei dati personali e afferma che la violazione della disciplina in materia di protezione dei dati personali non porta con sé necessariamente l'esistenza di una pratica commerciale scorretta, ma che tale violazione deve essere tenuta in considerazione nella valutazione della scorrettezza di una pratica, in particolare nel caso in cui il trattamento avvenga «a fini di invio di materiale pubblicitario o per qualsiasi altra finalità commerciale, come la profilazione, i prezzi personalizzati o le applicazioni relative ai megadati» (Commissione Europea, *Orientamenti sull'interpretazione e sull'applicazione della direttiva 2005/29/CE*, 29 dicembre 2021, p. 19).

In ambito nazionale il tema è stato affrontato da varie decisioni dell'Autorità Garante per la Concorrenza e del Mercato (d'ora in avanti: AGCM) in cui l'Autorità esamina le condotte dei titolari del trattamento alla luce della disciplina sulle pratiche commerciali scorrette (AGCM, 25 gennaio 2017, n. 10207; dec. 29 novembre 2018, n. 27432, e 11 maggio 2017, n. 26597). In particolare, si possono richiamare due decisioni, del 29 novembre 2018, n. 27432 e dell'11 maggio 2017, n. 26597 in cui l'AGCM ha affermato che tali norme vanno applicate laddove i dati personali relativi agli utenti, nell'un caso di Facebook e nell'altro di Whatsapp, acquisiscano valore economico perché trattati a fini commerciali, anche in assenza di un prezzo pagato per l'utilizzo commerciale di tali dati.

Rispetto all'applicabilità della disciplina, l'AGCM afferma che:

> il patrimonio informativo costituito dai dati degli utenti di FB, utilizzato per la profilazione degli utenti medesimi a uso commerciale e per finalità di marketing, acquista, proprio in ragione di tale uso, un valore economico idoneo a configurare l'esistenza di un rapporto di consumo tra il Professionista e l'utente che utilizza i servizi di FB. (AGCM, dec. 29 novembre 2018, n. 27432)

Tale indirizzo è stato poi confermato da successivi provvedimenti dell'Autorità (ad. es.: AGCM, 9 novembre 2021, n. 29888). A tal riguardo il Tribunale Amministrativo Regionale per il Lazio, nelle sentenze del 10 gennaio 2020, nn. 260 e 261 e il Consiglio di Stato (Consiglio di Stato, sentenze del 29 marzo 2021 nn. 2631 e 2630) hanno confermato l'applicabilità della disciplina in materia di pratiche commerciali scorrette in relazione a condotte relative all'informazione dell'interessato.

Venendo al profilo della scorrettezza della pratica, una pratica commerciale è scorretta, secondo quanto dispone l'art. 20 cod. cons.:

> se è contraria alla diligenza professionale, ed è falsa o idonea a falsare in misura apprezzabile il comportamento economico, in relazione al prodotto, del consumatore medio che essa raggiunge o al quale è diretta o del membro medio di un gruppo qualora la pratica commerciale sia diretta a un determinato gruppo di consumatori.

Il codice del consumo individua poi le pratiche scorrette che si definiscono come «ingannevoli» e «aggressive». In proposito, senza poter illustrare la disciplina nel dettaglio, si può qui semplicemente richiamare l'art. 21 cod. cons., rubricato «azioni ingannevoli» e l'art. 24 cod. cons. relativo alle pratiche aggressive.

L'analisi casistica, da svolgere anche sulla base delle decisioni dell'AGCM e della giurisprudenza in materia, è particolarmente utile per comprendere in concreto le intersezioni fra la disciplina in materia di protezione dei dati personali e le regole relative alle pratiche commerciali scorrette.

Si possono individuare i seguenti gruppi di ipotesi:

1) Casi relativi alla carenza di informazioni all'interessato circa le finalità commerciali del trattamento.

In proposito, nella decisione del 29 novembre 2018, n. 27432 l'AGCM ha valutato la pratica alla luce della disciplina in materia di pratiche commerciali ingannevoli. In particolare, l'AGCM ha qualificato come pratica commerciale ingannevole la mancanza, durante la prima fase di registrazione dell'utente a un noto *social network*, di un'informativa chiara, completa e immediata circa la propria attività di raccolta e utilizzo, a fini commerciali, dei dati relativi ai propri utenti. L'AGCM ha ritenuto che l'informativa fornita dal *social network* fosse generica e incompleta e che non distinguesse adeguatamente tra l'utilizzo dei dati per realizzare campagne pubblicitarie mirate dalle altre finalità del trattamento, relative alla «socializzazione» fra gli utenti. La pratica è considerata ingannevole in quanto:

> nella schermata di registrazione a FB, sia nella versione on line fino al 15 aprile 2018 che nella versione attualmente accessibile (tramite sito e app), il Professionista omette informazioni rilevanti di cui il consumatore necessita al fine di assumere una decisione consapevole di natura commerciale quale è quella di registrarsi nella Piattaforma Facebook per usufruire dell'omonimo servizio di social network.

Tale interpretazione è stata confermata sia dal TAR Lazio nelle sentenze del 10 gennaio 2020, nn. 260 e 261, che dal Consiglio di Stato con le due sentenze del 29 marzo 2021, nn. 2630 e 2631.

2) Casi relativi al consenso al trattamento «preimpostato».

Il Tribunale Amministrativo Regionale per il Lazio, nella decisione del 18 novembre 2022 n. 15326, ha qualificato come pratica aggressiva la «preimpostazione, da parte di Google, del consenso alla cessione dei dati personali relativi alla navigazione in internet», in quanto in questo caso il meccanismo di accettazione prevedeva che nella fase di creazione dell'account il consumatore trovasse preselezionata, in via generalizzata e preventiva, la casella dell'accettazione del trasferimento e/o utilizzo dei propri dati per fini commerciali.

3) Casi relativi al consenso «condizionato»

Un altro tipo di condotte concerne la previsione di un consenso al trattamento cui è condizionato il conseguimento di un vantaggio da parte del consumatore, particolarmente rilevante anche, come noto, sotto il profilo della protezione dei dati personali (sul consenso al trattamento, v. cap. *La disciplina dell'attività di trattamento*, § 2). In proposito, fra le varie decisioni si può richiamare la del 10 febbraio 2017, n. 10207, in cui l'AGCM ha affermato l'aggressività della pratica commerciale secondo cui, dopo l'acquisto di un prodotto, al fine di accedere a dei premi/vantaggi, è richiesto al consumatore di esprimere il consenso al trattamento dei dati personali. Secondo l'AGCM questa pratica configura un indebito condizionamento tale da indurre il consumatore ad assumere una decisione di natura commerciale che non avrebbe altrimenti preso. Il Consiglio di Stato ha seguito l'impostazione dell'AGCM, qualificando la pratica come aggressiva *ex* art. 24 cod. cons. in quanto

> idonea a condizionare indebitamente il consumatore, che si determina ad acquistare il prodotto in promozione allettato dalla possibilità di conseguire il premio/vantaggio promesso, senza essere stato preventivamente edotto della necessità, a tal fine, di fornire i propri dati personali e di rilasciare il consenso al loro trattamento. (Cons. Stato, 27 febbraio 2020, n. 1425)

4) La valutazione del trattamento dei dati in quanto attività.

Occorre sottolineare che nei casi che si sono ripercorsi non emerge la questione della valutazione del trattamento dei dati, in quanto attività, come pratica commerciale scorretta. Ciononostante, questo profilo non è da trascurare. Ad esempio, si immagini che un professionista tratti i dati personali del consumatore per la finalità di comunicare informazioni pubblicitarie personalizzate, violando il principio di compatibilità delle finalità, posto dall'art. 5, par. 1, lett. b) GDPR (v. cap. *La disciplina dell'attività di trattamento*, § 2). In proposito, è opportuno considerare che il trattamento dei dati personali – specie se di grandi quantità di dati personali, e con tecniche avanzate – crea uno squilibrio di potere conoscitivo fra l'interessato e chi tratta i dati, e che in alcuni casi tale potere diviene una vera e propria capacità di indirizzare le scelte, anche commerciali, dell'interessato, come ha riconosciuto anche il Comitato Europeo per la Protezione dei Dati con riguardo al *targeting* degli utenti dei social media (EDPB, *Linee guida 8/2020 sul targeting degli utenti di social media* del 13 aprile 2021, p. 7). In tale contesto, a fronte di un trattamento operato oltre quanto lecito ai sensi della disciplina, non è da escludersi che potrebbe ritenersi, in ragione del caso concreto, che vi sia un indebito condizionamento del consumatore capace di rendere applicabile la disciplina delle pratiche aggressive di cui agli artt. 24 ss. cod. cons. Se non fosse questo il caso, si potrebbe valutare la possibilità della scorrettezza della pratica *ex* art. 20 cod. cons., e dunque giudicare se questa sia contraria alla diligenza professionale – contrarietà che si potrebbe affermare di fronte all'illiceità del trattamento ai sensi del GDPR – e se sia falsa o idonea a falsare in misura apprezzabile il comportamento economico, in relazione al prodotto, del consumatore medio che essa raggiunge o al quale è diretta o del

membro medio di un gruppo qualora la pratica commerciale sia diretta a un determinato gruppo di consumatori.

Infine, in alcune ipotesi è possibile qualificare il trattamento dei dati personali in quanto tale come pratica commerciale. Tale interrogativo potrebbe risultare utile nelle ipotesi in cui il trattamento illecito, pur svolto per finalità commerciali – ad esempio la profilazione a fini di *marketing* – sia svolto da un'impresa, e la strategia pubblicitaria da una diversa azienda.

4. Clausole vessatorie

La disciplina in materia di clausole vessatorie è dettata dalla dir. 1993/13/CEE e recepita nell'ordinamento italiano agli artt. 33 ss. cod. cons. Senza poter qui dar conto della complessità della disciplina, si può partire dalla definizione di clausole vessatorie e dal rimedio della nullità previsto in caso di vessatorietà, per poi guardare alle intersezioni fra questa disciplina e le regole in materia di trattamento dei dati personali.

In particolare, l'art. 33 cod. cons. prevede che: «Nel contratto concluso tra il consumatore ed il professionista si considerano vessatorie le clausole che, malgrado la buona fede, determinano a carico del consumatore un significativo squilibrio dei diritti e degli obblighi derivanti dal contratto».

Sono poi elencate alcune clausole che sono da considerare vessatorie, divise in una lista nera di clausole sempre vietate (art. 36 cod. cons.) e clausole vietate che si presumono vessatorie fino a prova contraria (art. 33 cod. cons.).

La conseguenza della vessatorietà della clausola è stabilita *in primis* dall'art. 36 cod. cons., secondo cui: «Le clausole considerate vessatorie ai sensi degli articoli 33 e 34 sono nulle mentre il contratto rimane valido per il resto».

Nel valutare le intersezioni fra regole in materia di clausole vessatorie e disciplina in materia di dati personali occorre valutare diversi aspetti (Angiolini, 2024), fra cui alcuni particolarmente rilevanti sono:

1) i rapporti fra il contratto e il trattamento dei dati personali o la sua pianificazione, in quanto gli artt. 33 ss. cod. cons. si applicano soltanto ai contratti conclusi fra professionisti e consumatori;

2) La declinazione del giudizio di vessatorietà nei casi relativi al trattamento dei dati personali.

4.1. Trattamento dei dati personali e contratto

Spesso il contratto ha uno spazio significativo nelle dinamiche di circolazione dei dati, in quanto è utilizzato per procurare i dati ad una delle parti, anche attraverso la costruzione della possibilità concreta di raccoglierli in virtù di una relazione con l'interessato, sia per il tramite di un titolare del trattamento che li condivida o trasferisca. Tale ruolo del contratto è dovuto anche ad una peculiarità della disciplina in materia di dati personali attualmente in vigore, che regola il trattamento e non i mezzi e le regole in base a cui il soggetto che intenda trattare tali dati può accedervi. Infatti, il GDPR pone i limiti

entro cui il trattamento può essere posto in essere e pianificato, anche in base a scelte discrezionali di chi tratta i dati. Se si oltrepassano tali limiti, il trattamento è illecito. Le disposizioni in materia di dati non disciplinano però in modo organico il diritto di accedere ai dati da parte di chi intenda trattarli, se non parzialmente con il recente regolamento sulla *governance* dei dati, il Reg. 2022/868 (d'ora in avanti *Data Governance Act*) e il Reg. 2023/2854 (d'ora in avanti: *Data Act*).

A fronte di questo quadro, il contratto e il trattamento dei dati possono intersecarsi in modi diversi oppure in alcuni casi essere indipendenti. Qui non si può esaminare a fondo la mappa delle diverse ipotesi, ma citare alcuni esempi.

Per cominciare, un caso in cui il trattamento dei dati personali a fini profittevoli è indipendente dal contratto è quella in cui il trattamento è compiuto da un'impresa in virtù della base giuridica del legittimo interesse di cui all'art. 6, lett. f) GDPR e consiste nella raccolta di dati personali di chi circola su un determinato percorso stradale, con la finalità di migliorare il sistema di consegne a domicilio dell'impresa stessa. In questa ipotesi, il trattamento dei dati personali ha una sicura rilevanza economica e non sarà applicabile la disciplina in materia di clausole vessatorie.

Con riguardo alle intersezioni fra trattamento dei dati personali (o sua pianificazione) e il contratto, assumono rilevanza le ipotesi in cui il contratto crea le condizioni pratiche che consentono la raccolta dei dati personali. In tali casi, il contratto è elemento necessario perché si crei la possibilità concreta di raccolta dei dati e dunque di un loro trattamento. Un esempio particolarmente significativo è quello dei contratti che regolano l'accesso e l'uso dei *social network* da parte degli utenti. Lo schema è il seguente: un professionista offre un servizio digitale e ottiene la possibilità di raccogliere dati personali all'interno dell'ambiente digitale, il cui uso è regolato in via contrattuale dai «termini e le condizioni». In tali contratti, una parte si assicura la possibilità di raccogliere i dati personali. La prestazione contrattuale dell'interessato-parte contraente si identifica nell'esercizio del diritto alla protezione dei dati personali e alla riservatezza, in una maniera che permette all'altro contraente di raccogliere i dati personali, nel quadro di quanto reso possibile dal mezzo tecnologico. Tale prestazione assume carattere patrimoniale *ex* art. 1174 c.c., in quanto, oltre a essere valutata come dotata di valore economico dalle parti, la sua patrimonialità trova riscontro anche nel sistema.

In questo caso il contratto deve essere interpretato restrittivamente, e deve permettere di comprendere le «modalità di interferenza» dell'accordo con la sfera della personalità, e che dunque debba esserne determinato in modo chiaro l'oggetto (l'espressione è di Giorgio Resta, che la usa in relazione agli accordi relativi in Resta 2005, 287). A tal fine, un ponte fra la disciplina in materia di dati personali e il contratto può essere costruito attraverso l'informativa sul trattamento da fornire ai sensi dell'art. 13 GDPR (v. cap. *I diritti dell'interessato*). Dunque, si deve ritenere che ove il contratto crei le condizioni per la raccolta lecita dei dati personali, l'informativa relativa al trattamento acquisti carattere contrattuale, indipendentemente dalla base giuridica del trattamento utilizzata.

Allora, si applicherà ad essa la dir. CE 1993/13 e le norme che l'hanno recepita, e dunque gli artt. 33 ss. cod. cons.

Gli esempi fatti mostrano che per applicare le regole in materia di clausole vessatorie in casi relativi al trattamento dei dati personali è necessario interrogarsi sull'esistenza di una clausola contrattuale relativa ai dati personali, e dunque a monte di un contratto rilevante rispetto al trattamento, e che la risposta a tale interrogativo non è scontata e richiede al contrario analisi articolate.

4.2. La declinazione del giudizio di vessatorietà nei casi relativi al trattamento dei dati personali

Nella valutazione della vessatorietà della clausola si possono distinguere due scenari in cui opera il controllo di vessatorietà; il primo riguarda i casi dove la clausola è giudicata sfavorevolmente dall'ordinamento (anche) in base alle regole del codice civile, il secondo dove tale giudizio sfavorevole non sussiste.

1) La clausola è giudicata sfavorevolmente dall'ordinamento (anche) in base alle regole poste dal Codice civile.

In tali ipotesi, ci si può interrogare sui casi in cui la clausola determina un oggetto o una causa del contratto illeciti *ex* art. 1418 c.c., e l'illiceità è posta a tutela di una delle parti contrattuali, pur potendo tutelare anche interessi generali. Potrà essere questo il caso del contratto fra un interessato-consumatore e un titolare-professionista che prevede il diritto del professionista di effettuare un trattamento illecito – ad esempio la raccolta dei dati – per mancanza di una base giuridica del trattamento ai sensi dell'art. 6, par. 1 GDPR. Qui si potrà valutare la pattuizione sia sotto il profilo della vessatorietà che sotto quello della illiceità dell'oggetto o della causa del contratto, e la clausola che determina l'illiceità dell'oggetto o della causa del contratto deve essere ritenuta anche vessatoria, in quanto un assetto di interessi talmente impari da essere considerato illecito nei rapporti governati dal diritto comune non può che essere considerato anche vessatorio ai sensi dell'art. 33 cod. cons.

Una variazione sul tema appena tracciato si coglie rispetto a quelle clausole che incidono negativamente sulla libertà del consenso al trattamento: si immagini ad esempio la pattuizione con cui l'interessato-consumatore si obbliga a prestare il consenso al trattamento. In questo caso il consenso, ove prestato, non sarà libero e rispondente al GDPR in quanto oggetto di un obbligo cui l'interessato si è vincolato attraverso un contratto, e dunque manifestando un consenso, quello contrattuale, regolato da norme di minor tutela rispetto a quelle previste dalla disciplina in materia di dati personali. Tornando alla disciplina consumeristica, la clausola è da ritenersi illecita e vessatoria, in quanto dalla norma sulla libertà del consenso si può dedurre che è vietato creare per la via del contratto un obbligo di prestare il consenso al trattamento.

2) La clausola non è giudicata sfavorevolmente dall'ordinamento (anche) in base alle regole del Codice civile.

Per quanto riguarda il controllo di vessatorietà ove la clausola non porti con sé illiceità ai sensi del Codice civile, occorre distinguere fra la situazione in cui

la clausola rientra in una delle ipotesi elencate specificamente dal codice del consumo nelle liste di pratiche vietate e quella in cui è da valutare alla luce della definizione generale di cui all'art. 33, comma 1, cod. cons.

Rispetto al primo gruppo, si può fare un esempio relativo alla fattispecie prevista dall'art. 33, comma 2, lett. g) cod. cons, secondo cui si presumono vessatorie fino a prova contraria le clausole che hanno per oggetto, o per effetto, di riconoscere al solo professionista e non anche al consumatore la facoltà di recedere dal contratto, nonché di consentire al professionista di trattenere anche solo in parte la somma versata dal consumatore a titolo di corrispettivo per prestazioni non ancora adempiute, quando sia il professionista a recedere dal contratto. Con riguardo all'applicazione di tale norma, l'AGCM nel provvedimento, dell'11 maggio 2017, n. 26596 ha qualificato come vessatoria la clausola secondo cui, a fronte della possibilità di liberarsi dal vincolo contrattuale da parte del professionista, a seguito dello scioglimento del contratto per volontà dell'utente «WhatsApp si riserva [...] il diritto di trasferire le informazioni dell'utente alle proprie affiliate, agli aventi causa o a un nuovo proprietario» (AGCM, 17 maggio 2017, n. 26596, § 80).

L'AGCM ritiene che la clausola riconosca al solo professionista e non anche al consumatore la facoltà di recedere dal contratto in quanto la previsione della possibilità per il professionista di trasferire le informazioni dell'utente a terzi è incompatibile con il recesso – l'Autorità fa riferimento in modo atecnico all'istituto della risoluzione – «che si applica, invece, a tutti gli effetti nei confronti del consumatore, in quanto viene cessata la fornitura del servizio». L'ACGM nella sua valutazione considera un argomento *ad adiuvandum* «la rilevanza economica dei dati degli utenti di WhatsApp» (AGCM, 17 maggio 2017, n. 26596, § 81).

Si deve poi riflettere sull'applicazione della norma di carattere generale prevista dall'art. 33, comma 1, cod. cons., e che si è richiamata in apertura di questo paragrafo. La disposizione è stata oggetto dell'attività interpretativa della Corte di Giustizia dell'UE che ha ricostruito alcuni criteri, qualificati dalla stessa Corte non tassativi, né cumulativi né alternativi (CGUE, 8 dicembre 2022, C-600/21, §35). In particolare, la Corte ha affermato che:

i) il diritto dispositivo che si applicherebbe in assenza della clausola costituisce parametro di riferimento per l'accertamento della vessatorietà (CGUE, 14 marzo 2013, C-415/11);

ii) bisogna considerare «se il professionista, qualora avesse trattato in modo leale ed equo con il consumatore, avrebbe potuto ragionevolmente aspettarsi che quest'ultimo aderisse ad una clausola del genere nell'ambito di un negoziato individuale» (CGUE, 26 gennaio 2017, C-421/14, § 60);

iii) si deve tener conto della natura dei beni o dei servizi oggetto del contratto;

iv) occorre valutare le conseguenze della clausola in ragione del diritto contrattuale applicabile (CGUE 24 marzo 2022, C-82/20, § 39; 13 ottobre 2022, C-405/21, §28) e

v) occorre valutare le conseguenze della mancanza di trasparenza della clausola, che però non vale da sola a fondare la vessatorietà della clausola (CGUE, 17 novembre 2021, C-79/21, § 33).

Anche alla luce di tali criteri, l'applicazione del controllo di vessatorietà rispetto alle clausole relative al trattamento dei dati personali conduce a evidenziare la difficoltà di trovare il criterio per valutare la vessatorietà delle clausole che descrivono e delimitano il trattamento.

Tale difficoltà ben si coglie con un esempio: in un contratto fra titolare-professionista e interessato-consumatore, si potrà valutare come vessatoria una clausola che, a fronte della fornitura di servizi di scarso pregio per un tempo limitato, preveda la raccolta di dati personali sulla base di un legittimo interesse per finalità che richiedono un tempo di conservazione e di trattamento dei dati più lungo rispetto a quello della fornitura del servizio? Risulta qui difficoltoso applicare uno dei criteri più importanti individuati dalla Corte di Giustizia per valutare la vessatorietà della clausola, che consiste nell'uso, come parametro di riferimento, del diritto dispositivo che si applicherebbe in assenza della clausola. Rispetto alle clausole di cui ci si sta occupando le norme di riferimento non si trovano tanto nel diritto dei contratti, quanto nella disciplina in materia di trattamento dei dati personali, e in particolare nel GDPR. Tale regolamento non può però essere utilmente usato per valutare la vessatorietà di una clausola con cui le parti esercitino una scelta discrezionale entro i limiti posti dal medesimo regolamento. Questo perché, appunto, se la clausola non è in contrasto con il regolamento, la scelta operata dalle parti è in linea con gli assetti di interessi protetti dal GDPR.

5. Interessi collettivi dei consumatori e azioni a tutela dei dati personali

Nel diritto dei consumatori, un'area tradizionalmente rilevante riguarda la tutela degli interessi collettivi. Spesso, infatti, l'illecito di un professionista non lede solo l'interesse di un singolo consumatore, ma colpisce contemporaneamente gli interessi di un gruppo di consumatori.

Per far fronte a questo tipo di illeciti, che possono procurare pregiudizi di entità non particolarmente significativa per la singola persona fisica, ma che assumono una rilevanza ben diversa se considerati nel complesso dei loro effetti lesivi, il legislatore europeo concede, ad alcuni enti legittimati (ad esempio, le associazioni di consumatori), la possibilità di esercitare azioni rappresentative a tutela degli interessi collettivi (v. direttiva 2020/1828/UE che abroga la precedente direttiva 2009/22/CE). Per quel che rileva ai nostri fini, occorre segnalare che, tra gli illeciti che giustificano l'esercizio di tali azioni, si menzionano anche le violazioni delle disposizioni contenute nel GDPR e nella direttiva 2002/58/CE, (d'ora in avanti: direttiva e-privacy) (v. art. 2, par. 1 e allegato I, nn. 10) e 56), dir. 2020/1828).

L'art. 2, ppar. 1, dir. 2020/1828 ne delinea in modo piuttosto complesso l'ambito di applicazione, prevedendo che la direttiva si applichi alle azioni rappresentative intentate nei confronti di professionisti per violazioni delle disposizioni del diritto dell'Unione di cui all'allegato I, che ledono o possono ledere gli interessi collettivi dei consumatori. Il secondo paragrafo dispone che la direttiva non pregiudica le disposizioni del diritto dell'Unione di cui all'allegato I. In detto allegato, per quel che qui interessa, sono inclusi sia il Reg UE 2016/679 sia la direttiva

2002/58/CE del 12 luglio 2002, relativa alla vita privata e alle comunicazioni elettroniche. Il considerando 16 della direttiva prevede che qualora i provvedimenti contenuti nell'allegato I contengano disposizioni che non attengono alla protezione dei consumatori, tale allegato dovrebbe fare riferimento alle disposizioni specifiche che tutelano gli interessi dei consumatori, e che tuttavia «siffatti riferimenti non sono sempre possibili a causa della struttura di determinati atti giuridici, in particolare nel settore dei servizi finanziari». Sul punto, per quanto riguarda la direttiva 2002/58 l'allegato I richiama gli artt. da 4 a 8 e l'articolo 13 in materia di comunicazioni indesiderate, includendo quindi l'art. 5, particolarmente rilevante in materia di protezione dei dati personali perché relativo ai c.d. cookies, e l'art. 6 relativo ai dati sul traffico (v. sui cookies il cap. *La disciplina dell'attività di trattamento*, sez. I). Il regolamento UE 2016/679 è incluso nell'allegato I, ma non sono indicate specifiche norme. Quindi, un nodo interpretativo chiave riguarda l'individuazione delle ipotesi in cui la Dir. 2020/1828 risulterà applicabile di fronte ad una violazione delle norme del GDPR. In questo caso, la definizione dei confini del diritto dei consumatori rispetto alla protezione dei dati personali si gioca sull'interpretazione della nozione di «interessi collettivi dei consumatori». In proposito, l'art. 3 della direttiva, che dà una definizione di tale nozione, non è di grande aiuto, in quanto definisce gli interessi collettivi dei consumatori come «gli interessi generali dei consumatori e, in particolare ai fini dei provvedimenti risarcitori, gli interessi di un gruppo di consumatori». La definizione di cui al nuovo art. 140-*ter*, comma 1, lett. c) cod. cons., adottata in sede di recepimento non introduce elementi di innovazione rispetto al testo adottato in sede europea. Tirando le somme rispetto alla questione interpretativa oggetto di analisi, alla luce della rilevanza del trattamento a fini profittevoli nell'economia contemporanea, una strada interpretativa è quella di considerare che, di fronte a un trattamento funzionale allo svolgimento di un'attività economica che ha uno sbocco su un mercato cui accedono i consumatori, le violazioni del GDPR possono ledere gli interessi collettivi di questi ultimi.

La dir. 2020/1828 è stata recepita nell'ordinamento nazionale con l'introduzione, nel codice del consumo, degli artt. 140-*ter* ss. In particolare, è l'allegato II-*septies* del codice, cui rinvia l'art. 140-*ter*, a indicare le discipline la cui violazione potrebbe danneggiare gli interessi collettivi dei consumatori. Stranamente, tra le discipline indicate nel suddetto allegato non è menzionato direttamente il GDPR, ma soltanto il d.lgs. n. 101/2018, come disciplina di attuazione dello stesso, oltre che il d.lgs. n. 196/2003, in attuazione della direttiva e-privacy. Nonostante tale anomalia, frutto presumibilmente di un poco accorto recepimento legislativo, la dottrina non dubita che gli interessi collettivi dei consumatori possano essere danneggiati dalla violazione di una disposizione contenuta nel GDPR, che costituisce la fonte primaria in materia di protezione dei dati personali (Angiolini 2023).

Si pensi, per ipotesi, a una piattaforma digitale che, nel fornire i propri servizi, tratti illecitamente i dati personali degli utenti contraenti: in virtù delle norme sopra richiamate, un'associazione consumeristica può richiedere all'autorità

giudiziaria di emettere un ordine con cui vieti alla piattaforma digitale di proseguire nel comportamento antigiuridico e, laddove un gruppo di consumatori abbia subito pregiudizi a causa di tale comportamento, può avviare un'azione risarcitoria o un'altra azione che vi presti rimedio (ad esempio, un'azione di risoluzione del contratto).

Come già si è visto a proposito della direttiva 2019/770, anche le previsioni della direttiva 2020/1828 possono creare delle interferenze con il GDPR.

A dire il vero, quest'ultima normativa, a differenza della disciplina consumeristica, non contiene specifiche disposizioni in merito alla tutela degli interessi collettivi degli interessati al trattamento. Tuttavia, l'art. 80, par. 1 GDPR, disciplinando la «rappresentanza degli interessati», prevede che ciascuno di essi ha il diritto di dare mandato a un ente collettivo, debitamente costituito e attivo nel settore della protezione dei dati, per proporre un reclamo all'autorità di controllo o un ricorso all'autorità giurisdizionale, anche al fine di un risarcimento dei danni eventuali subiti dall'interessato. Tale previsione è completata dalla facoltà lasciata agli Stati membri di consentire agli enti collettivi, qualora ritengano che i diritti di un interessato siano stati violati, di prendere un'iniziativa processuale anche «indipendentemente dal mandato conferito dagli interessati», purché tale iniziativa non consista in un'azione risarcitoria, la quale richiede necessariamente il conferimento di un mandato (v. art. 80, par. 2 GDPR).

Alla luce di queste previsioni contenute nell'GDPR, l'interferenza con la disciplina a tutela dei consumatori può presentarsi nella misura in cui gli enti collettivi possano agire in giudizio sulla base di condizioni diverse rispetto a quelle indicate dall'art. 80, par. 1.

In realtà, la Corte di giustizia dell'UE è già intervenuta chiarendo che «la violazione di una norma relativa alla protezione dei dati personali può simultaneamente comportare la violazione di norme relative alla tutela dei consumatori o alle pratiche commerciali sleali» (CGUE, 28 aprile 2022, C-319/20, § 78).

Pertanto, vista la discrezionalità lasciata agli Stati membri dal par. 2 dell'art. 80, questi possono consentire a un'associazione a tutela dei consumatori di agire in giudizio,

> in assenza di un mandato che le sia stato conferito a tale scopo e indipendentemente dalla violazione di specifici diritti degli interessati, contro il presunto autore di un atto pregiudizievole per la protezione dei dati personali, facendo valere la violazione del divieto di pratiche commerciali sleali, la violazione di una legge in materia di tutela dei consumatori o la violazione del divieto di utilizzazione di condizioni generali di contratto nulle, qualora il trattamento di dati in questione sia idoneo a pregiudicare i diritti riconosciuti da tale regolamento a persone fisiche identificate o identificabili. (CGUE, 28 aprile 2022, C-319/20, § 83)

Nel caso in esame, si discuteva della compatibilità con il GDPR di una disciplina nazionale relativa alla tutela collettiva dei consumatori, tramite l'esercizio di azioni inibitorie, contro eventuali violazioni di regole in materia di protezione dei dati personali. Come si è visto, in virtù dell'art. 80, par. 2 GDPR, la Corte si è espressa in senso favorevole.

In futuro, però, potrebbe riproporsi il problema in merito alla compatibilità con il GDPR di discipline nazionali che consentano alle associazioni consumeristiche di intentare, in assenza di un *preventivo* mandato degli interessati, non solo azioni inibitorie, ma anche azioni risarcitorie (è il caso, ad esempio, del nostro art. 140-*septies*, co. 1 cod. cons.) contro eventuali violazioni di regole in materia di protezione dei dati personali. Il problema sarebbe più complesso perché, ai sensi dell'art. 80, par. 1 GDPR, gli Stati membri hanno meno margini di autonomia nel regolare le condizioni di esercizio di un'azione risarcitoria da parte di un ente collettivo.

Ciò dimostra, ancora una volta, come le possibili sovrapposizioni tra il diritto dei consumatori e la disciplina di protezione dei dati rischino di creare problemi interpretativi che non sempre risultano di facile soluzione.

Riferimenti bibliografici

AA.VV. 2024. *Collective Redress. Country Reports, Digital Freedom Fund*, accessibile all'indirizzo: https://digitalfreedomfund.org/wp-content/uploads/2024/11/CRB_V4.pdf

Angiolini, Chiara. 2023. "Una riflessione critica sulla complementarità fra norme sulla protezione dei dati personali e il diritto dei consumatori nella disciplina dei profili patrimoniali del rapporto fra interessato e titolare del trattamento." In Chiara Angiolini e Daniela Santarpia (a cura di), *La fattispecie «liquida»: quattro casi sintomatici*, 28 ss. Napoli: Edizioni Scientifiche Italiane.

Angiolini, Chiara. 2024. "Clausole abusive e circolazione dei dati personali." In Stefano Pagliantini (a cura di), *Le clausole abusive nei contratti dei consumatori. Trent'anni di direttiva 93/13 – Il foro italiano. Gli Speciali,* fascicolo speciale n. 1/2024 della rivista Il Foro Italiano, Milano.

Bachelet, Vittorio. 2023. *Il consenso oltre il consenso*. Pisa: Pacini.

Magri, Geo, Thobani, Shaira (a cura di). 2022. *Manuale di diritto privato delle nuove tecnologie*. Torino: Giappichelli.

Pagliantini, Stefano. 2022. "L'attuazione minimalista della dir. 2019/770/UE: riflessioni sugli artt. 135 *octies* – 135 *vicies* ter c.cons. La nuova disciplina dei contratti b-to-c per la fornitura di contenuti e servizi digitali." *Le nuove leggi civili commentate* 45, 6: 1499-522.

Resta, Giorgio. 2005. *Autonomia privata e diritti della personalità. Il problema dello sfruttamento economico degli attributi della persona in prospettiva comparatistica*. Napoli: Jovene.

Rott, Peter. 2017. "Data protection law as consumer law. How consumer organisations can contribute to the enforcement of data protection law." In *J. Eur: Consumer and Market L.*

Versaci, Giuseppe. 2020. *La contrattualizzazione dei dati personali dei consumatori*. Napoli: Edizioni Scientifiche Italiane.

Versaci, Giuseppe. 2023. "Trattamenti illeciti dei dati personali e tutele collettive dei consumatori". In Alessandro Palmieri e Francesca Altamura (a cura di), *Class action e meccanismi di tutela collettiva*. Torino: Giappichelli.

Zuiderveen Borgesius, Frederik, Helberger, Natali, Reyna, Agustin. 2017. "The perfect match? A closer look at the relationship between eu consumer law and data protection law." In *Common Market Law Review.*

La disciplina dei diversi rapporti che riguardano i dati personali

Chiara Angiolini, Elia Cremona[1]

Abstract: This chapter highlights the variety of relationships involving personal data. The first paragraphs focus on relations between parties other than data subjects, such as contractual relationships between data controllers and between data controller and data processor. The following paragraphs deal with the relationships between public bodies and private actors with regard to the use of data, and between data intermediaries and actors who seek access to data. Finally, in the last paragraph, Data Act rules are analysed specifically in relation to the new access rights on IoT data.

Keywords: Data protection agreements, data transfer agreements, open data, data altruism, data intermediation services, access rights on IoT data

1. La varietà dei rapporti che riguardano i dati personali

Nei precedenti capitoli si è detto dei diversi ruoli esistenti in relazione al trattamento, in particolare quelli di titolare del trattamento e di responsabile del trattamento (v. cap. *Le definizioni fondamentali*).

In questo capitolo si prendono in esame le regole relative ai rapporti fra tali soggetti, guardando sia agli atti che devono essere adottati ai sensi del Reg. UE 2016/679 (d'ora in avanti: GDPR), anche con riguardo ai trasferimenti verso paesi terzi e organizzazioni internazionali, sia al ruolo del contratto rispetto ai trattamenti che consistono nella comunicazione e nella ricezione dei dati personali fra titolari del trattamento.

[1] Chiara Angiolini ha scritto i paragraafi 1, 2, 3, 4, 5, 7.2 e 8; Elia Cremona ha scritto i paragrafi 6, 7 e 7.1.

Chiara Angiolini, University of Siena, Italy, chiara.angiolini@unisi.it
Elia Cremona, University of Siena, Italy, elia.cremona@unisi.it, 0000-0001-9336-218X

Referee List (DOI 10.36253/fup_referee_list)
FUP Best Practice in Scholarly Publishing (DOI 10.36253/fup_best_practice)

Inoltre, occorre evidenziare come, negli ultimi tempi, i dati personali siano divenuti oggetto di una regolamentazione di rapporti soggettivi che trovano disciplina al di fuori del GDPR. Con l'intento di far circolare maggiormente i dati detenuti da soggetti pubblici e privati, la direttiva UE 2019/1024 (d'ora in avanti: Direttiva *Open Data*), il regolamento UE 2022/868 (d'ora in avanti: *Data Governance Act*) e il regolamento UE 2023/2854 (d'ora in avanti: *Data Act*) hanno messo i dati, personali e non, al centro di una serie di relazioni disciplinate attraverso varie qualificazioni soggettive e complesse regole volte anche alla valorizzazione dei dati nei più ampi contesti sociali.

In questo capitolo, si prendono dunque in esame anche le regole relative a questi ulteriori rapporti riguardanti i dati personali.

2. I contratti fra contitolari del trattamento

In ogni caso di contitolarità del trattamento, ai sensi dell'art. 26 GDPR i contitolari devono determinare in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal GDPR, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14 GDPR (sull'informazione all'interessato, v. cap. *I diritti dell'interessato*), salvo il caso in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti.

L'accordo può designare un punto di contatto per gli interessati e deve riflettere adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati. Il contenuto essenziale dell'accordo deve essere messo a disposizione dell'interessato.

L'art. 26 GDPR dispone anche che, indipendentemente da quanto prevede l'accordo fra contitolari, l'interessato possa esercitare i propri diritti ai sensi del GDPR nei confronti di e contro ciascun titolare del trattamento.

Rispetto a tale accordo, come già detto nel capitolo 3, è di particolare importanza la sentenza della Corte di Giustizia dell'UE del 4 maggio 2023 C- 60/22, secondo cui non si è di fronte ad un trattamento illecito quando vi è la violazione delle regole in merito agli accordi di contitolarità, poste dall'art. 26 GDPR. La Corte poggia tale conclusione su vari argomenti, fra cui quello secondo cui

> l'assenza di un accordo che determini la contitolarità, ai sensi dell'articolo 26 del RGPD […] non è sufficiente a dimostrare, di per sé, l'esistenza di una lesione del diritto fondamentale alla protezione dei dati personali. In particolare, se è vero che […] la chiara ripartizione delle responsabilità tra i contitolari del trattamento e il registro delle attività di trattamento costituiscono mezzi per garantire il rispetto, da parte di tali contitolari, delle garanzie previste da detto regolamento per la tutela dei diritti e delle libertà degli interessati, resta nondimeno il fatto che l'assenza di un siffatto registro o di un siffatto accordo non dimostra, di per sé, che tali diritti e tali libertà siano stati violati. (*Ibidem*, § 65)

3. L'atto fra il titolare e il responsabile del trattamento

L'art. 28 GDPR, rubricato «Responsabile del trattamento» prevede che i trattamenti da parte di un responsabile del trattamento siano disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri.

Tale atto deve vincolare il responsabile del trattamento al titolare del trattamento e deve regolare la materia che ne è l'oggetto e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento.

In particolare, il contratto o altro atto giuridico deve prevedere che il responsabile del trattamento:

a) tratti i dati personali soltanto su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento; in tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;

b) garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;

c) adotti tutte le misure richieste ai sensi dell'articolo 32 GDPR;

d) tenendo conto della natura del trattamento, assista il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III GDPR;

e) assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 GDPR in materia di sicurezza del trattamento, violazione dei dati personali (*data breach*), valutazione di impatto, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;

f) su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati;

g) metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui all'art. 28 GDPR e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato. Il responsabile del trattamento deve informare immediatamente il titolare del trattamento qualora, a suo parere, un'istruzione violi il GDPR o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati.

Inoltre, nell'atto di cui all'art. 28 GDPR si deve prevedere che siano rispettate le regole poste dal medesimo articolo relative alla nomina dei c.d. sub-responsabili del trattamento, che si illustrano di seguito.

In primo luogo, l'art. 28 GDPR prevede che il responsabile del trattamento non ricorra a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento deve informare il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche.

Inoltre, quando un responsabile del trattamento ricorre a un altro responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento, su tale altro responsabile del trattamento sono imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra il titolare del trattamento e il responsabile del trattamento, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR. Infine, qualora l'altro responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il responsabile iniziale conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro responsabile.

L'art. 28 GDPR prevede anche che il contratto o altro atto giuridico di nomina del responsabile possano basarsi su clausole tipo stabilite dalla Commissione Europea. La Commissione Europea ha adottato tali clausole con la Decisione di Esecuzione (UE) 2021/915 della Commissione del 4 giugno 2021 relativa alle clausole contrattuali tipo tra titolari del trattamento e responsabili del trattamento a norma dell'articolo 28, paragrafo 7, GDPR e dell'articolo 29, paragrafo 7, del Regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio.

4. I contratti fra titolari del trattamento per la comunicazione dei dati personali, nella prospettiva del diritto privato

Ad di là di atti e accordi che siano obbligatori ai sensi del GDPR, di cui si è detto nei precedenti paragrafi, è utile dare un quadro delle questioni che concernono i contratti relativi la comunicazione di dati personali fra titolari del trattamento dal punto di vista del diritto privato.

L'inquadramento di tali contratti non è semplice.

Si può cominciare richiamando la nozione di titolare del trattamento, secondo cui si diventa titolari del trattamento quando si determinano le finalità e i mezzi del trattamento (v. cap. *Le definizioni fondamentali*, § 3.5). Proprio in ragione di tale definizione basata sul ruolo di un soggetto rispetto al trattamento, non è possibile trasferire la qualifica di titolare del trattamento.

Dunque, non è corretto discorrere di trasferimento della posizione di titolare del trattamento, ed è invece utile concentrarsi sulla facoltà di una parte di comunicare o diffondere i dati personali, e di quella dell'altro contraente di riceverli, e dunque di raccoglierli.

Entrambe le attività sono da considerare come trattamenti di dati personali, sottoposti al requisito della liceità (sulla liceità del trattamento, v. cap. *La disciplina dell'attività di trattamento*).

Allora, quando il titolare abbia la facoltà di comunicare i dati a un terzo, e questi possa raccoglierli in ragione di una base giuridica del trattamento (v. cap. *La disciplina dell'attività di trattamento*), le parti possono regolare tale comunicazione tramite un contratto, anche verso un corrispettivo. In questi casi il contratto rende possibile l'accesso ai dati personali da parte di un nuovo titolare del trattamento, obbligando il titolare originario a comunicarglieli, ma non trasferisce una situazione giuridica soggettiva fra le due parti, in quanto il nuovo titolare del trattamento potrà trattare i dati in ragione delle basi giuridiche che può far valere e che ha scelto e di cui ha informato l'interessato (sull'informazione dell'interessato v. cap. *I diritti dell'interessato*).

Occorre ora considerare l'ipotesi in cui la comunicazione dei dati da parte del primo titolare sia illecita ai sensi del GDPR e quella in cui lo sia la raccolta da parte del titolare destinatario dei dati (Angiolini, 2020).

Quando la comunicazione non sia lecita da parte del primo titolare del trattamento, il contratto deve essere considerato nullo per illiceità dell'oggetto *ex* art 1418, secondo comma c.c. Infatti, in questo caso è la prestazione stessa ad essere illecita, e dunque l'oggetto del contratto sarà da considerarsi carente del requisito della liceità, posto dall'art. 1346 c.c.

Ove invece la comunicazione dei dati personali da parte del primo titolare è lecita, e ad essere illecita è la raccolta da parte del destinatario della comunicazione, il contratto sarà da ritenersi nullo *ex* art 1418, 2 comma, c.c., in quanto ne sarà illecita la causa, in relazione alla funzione concreta che questo realizza di permettere al secondo titolare di avere accesso ai dati personali – e dunque *in primis* di raccoglierli.

Nelle due ipotesi che si sono viste in cui il contratto è nullo, l'interessato potrà far valere la nullità del contratto. Questo in quanto nell'applicare l'art. 1421 c.c. in tema di legittimazione a far valere la nullità, è da considerare che l'interessato è titolare di diritti sui dati personali che sono oggetto di comunicazione, e dunque parte che può dirsi senz'altro essere pregiudicata da un trattamento illecito. Tale ipotesi è comunque al momento più che altro di scuola, considerando l'elevato grado di opacità di tali rapporti contrattuali.

5. I flussi transfrontalieri di dati personali

Il capo V del GDPR è dedicato ai trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali e prevede una disciplina articolata, che è stata oggetto di vari interventi della Corte di Giustizia dell'UE.

L'art. 44 GDPR, rubricato «principio generale per il trasferimento» è di particolare importanza e recita:

> Qualunque trasferimento di dati personali oggetto di un trattamento o destinati a essere oggetto di un trattamento dopo il trasferimento verso un paese terzo o un'organizzazione internazionale, compresi trasferimenti successivi di dati

> personali da un paese terzo o un'organizzazione internazionale verso un altro paese terzo o un'altra organizzazione internazionale, ha luogo soltanto se il titolare del trattamento e il responsabile del trattamento rispettano le condizioni di cui al presente capo, fatte salve le altre disposizioni del presente regolamento. Tutte le disposizioni del presente capo sono applicate al fine di assicurare che il livello di protezione delle persone fisiche garantito dal presente regolamento non sia pregiudicato.

Gli articoli successivi del GDPR prevedono diversi strumenti relativi al trasferimento dei dati personali verso paesi terzi o organizzazioni internazionali, che sono i seguenti:

i) Trasferimento sulla base di una decisione di adeguatezza (art. 45);
ii) Trasferimento soggetto a garanzie adeguate (artt. 46-47);
iii) Deroghe in specifiche situazioni (art. 49).

5.1. Il trasferimento sulla base di una decisione di adeguatezza

In base a quanto dispone l'art 45 GDPR la Commissione Europea può decidere che un paese terzo, un territorio o uno o più settori specifici all'interno del paese terzo, o un'organizzazione internazionale garantiscono un livello di protezione adeguato. In tal caso il trasferimento può essere compiuto, naturalmente nel rispetto del GDPR e della disciplina applicabile.

L'art. 45 GDPR individua gli elementi che la Commissione deve prendere in considerazione, in particolare, per valutare l'adeguatezza del livello di protezione, che sono i seguenti:

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 la possibilità di 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.

Dal punto di vista procedurale, la Commissione decide mediante atti di esecuzione. L'atto di esecuzione deve prevedere un meccanismo di riesame periodico, almeno ogni quattro anni, che tenga conto di tutti gli sviluppi pertinenti nel paese terzo o nell'organizzazione internazionale.

Inoltre, la Commissione deve controllare su base continuativa gli sviluppi nei paesi terzi e nelle organizzazioni internazionali che potrebbero incidere sul funzionamento delle decisioni di adeguatezza adottate.

Se risulta dalle informazioni disponibili, in particolare in seguito al riesame periodico di cui si è appena detto, che un paese terzo, un territorio o uno o più settori specifici all'interno di un paese terzo, o un'organizzazione internazionale non garantiscono più un livello di protezione adeguato, la Commissione revoca, modifica o sospende nella misura necessaria la decisione di adeguatezza, mediante atti di esecuzione senza effetto retroattivo.

La Commissione pubblica nella Gazzetta ufficiale dell'Unione europea e sul suo sito web l'elenco dei paesi terzi, dei territori e settori specifici all'interno di un paese terzo, e delle organizzazioni internazionali per i quali ha deciso che è o non è più garantito un livello di protezione adeguato. Nel momento in cui si scrive, giugno 2025, la Commissione ha adottato decisioni di adeguatezza relative a vari paesi, fra cui l'Argentina, il Regno Unito, Stati Uniti, Svizzera, Giappone.

Rispetto alla valutazione di adeguatezza è di particolare interesse la sentenza della Corte di Giustizia 16 luglio 2020 C-311/18, in cui la Corte ha giudicato invalida la decisione di adeguatezza relativa ai trasferimenti verso gli Stati Uniti (decisione di esecuzione UE 2016/1250 della Commissione, del 12 luglio 2016, sull'adeguatezza della protezione offerta dal regime dello scudo UE-USA per la privacy). La pronuncia è di particolare rilevanza perché affronta alcuni aspetti importanti relativi all'interpretazione dell'art. 45 GDPR.

In particolare, la Corte, interpretando la disciplina del GDPR alla luce della Carta dei Diritti Fondamentali dell'UE ha statuito che:

i) l'adozione, da parte della Commissione, di una decisione di adeguatezza ai sensi dell'art. 45 GDPR richiede la constatazione, debitamente motivata, da parte di tale istituzione, che il paese terzo di cui trattasi garantisce effettivamente, in considerazione della sua legislazione nazionale o dei suoi impegni internazionali, un livello di protezione dei diritti fondamentali sostanzialmente equivalente a quello garantito nell' ordinamento giuridico dell'Unione, interpretato alla luce dei diritti fondamentali protetti dalla Carta dei Diritti Fondamentali dell'UE, e in particolare gli artt. 7 (Rispetto della vita privata e della vita familiare, su cui si veda il cap. *Le fonti della disciplina in materia di dati personali*), 8 (Diritto alla protezione dei dati personali, su cui si veda il cap. *Le fonti della disciplina in materia di dati personali*) e 47 CDFUE (diritto a un ricorso effettivo e a un giudice imparziale);

ii) nel valutare l'adeguatezza del livello di protezione garantito da un paese terzo, la Commissione deve prendere in considerazione in particolare i mezzi di «ricorso effettivo in sede amministrativa e giudiziaria per gli interessati i cui dati personali sono oggetto di trasferimento», anche alla luce dell'art. 47 CDFUE, che sancisce il diritto a un ricorso effettivo e a un giudice imparziale.

5.2. *Segue*. Il trasferimento soggetto a garanzie adeguate

Secondo quanto prevede l'art. 46 GDPR, In mancanza di una decisione di adeguatezza *ex* art. 45 GDPR, di cui si è appena detto, il titolare del trattamento o il responsabile del trattamento può trasferire dati personali verso un paese terzo o un'organizzazione internazionale solo se:

i) ha fornito garanzie adeguate e

ii) a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi.

Con riguardo alle garanzie adeguate, occorre distinguere le ipotesi che necessitano di un'autorizzazione specifica da parte dell'autorità di controllo e quelle che non la necessitano.

Fatta salva l'autorizzazione dell'autorità di controllo competente, possono costituire garanzie adeguate:

a) le 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; o

b) le disposizioni da inserire in accordi amministrativi tra autorità pubbliche o organismi pubblici che comprendono diritti effettivi e azionabili per gli interessati. L'autorità di controllo in questi casi applica il meccanismo di coerenza di cui all'articolo 63 (v. cap. *La regolamentazione e la tutela amministrativa*).

Inoltre, possono costituire garanzie adeguate, senza necessitare di autorizzazioni specifiche da parte di un'autorità di controllo:

a) uno strumento giuridicamente vincolante e avente efficacia esecutiva tra autorità pubbliche o organismi pubblici;

b) le norme vincolanti d'impresa in conformità dell'articolo 47 GDPR;

c) le clausole tipo di protezione dei dati adottate dalla Commissione;

d) le clausole tipo di protezione dei dati adottate da un'autorità di controllo e approvate dalla Commissione;

e) un codice di condotta approvato a norma dell'articolo 40 GDPR, unitamente all'impegno vincolante ed esecutivo da parte del titolare del trattamento o del responsabile del trattamento nel paese terzo ad applicare le garanzie adeguate, anche per quanto riguarda i diritti degli interessati;

f) un meccanismo di certificazione approvato a norma dell'articolo 42 GDPR, unitamente all'impegno vincolante ed esigibile da parte del titolare del trattamento o del responsabile del trattamento nel paese terzo ad applicare le garanzie adeguate, anche per quanto riguarda i diritti degli interessati.

Con riguardo alle clausole tipo di protezione dei dati adottate dalla Commissione, queste sono state adottate dalla Commissione con la decisione di esecuzione (UE) 2021/914 del 4 giugno 2021.

Per quanto riguarda le norme vincolanti per l'impresa, la procedura per la loro approvazione è prevista dall'art. 47 GDPR. In particolare, l'autorità di controllo competente approva le norme vincolanti d'impresa in conformità del meccanismo di coerenza di cui all'articolo 63 GDPR (v. cap. *La regolamentazione e la tutela amministrativa*), a condizione che queste a norma dell'art. 47 GDPR:

1) siano giuridicamente vincolanti e si applichino a tutti i membri interessati del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune, compresi i loro dipendenti;

2) conferiscano espressamente agli interessati diritti azionabili in relazione al trattamento dei loro dati personali;

3) specifichino almeno:

a) la struttura e le coordinate di contatto del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune e di ciascuno dei suoi membri;

b) i trasferimenti o il complesso di trasferimenti di dati, in particolare le categorie di dati personali, il tipo di trattamento e relative finalità, il tipo di interessati cui si riferiscono i dati e l'identificazione del paese terzo o dei paesi terzi in questione;

c) la loro natura giuridicamente vincolante, a livello sia interno che esterno;

d) l'applicazione dei principi generali di protezione dei dati, in particolare in relazione alla limitazione della finalità, alla minimizzazione dei dati, alla limitazione del periodo di conservazione, alla qualità dei dati, alla protezione fin dalla progettazione e alla protezione per impostazione predefinita, alla base giuridica del trattamento e al trattamento di categorie particolari di dati personali, le misure a garanzia della sicurezza dei dati e i requisiti per i trasferimenti successivi ad organismi che non sono vincolati dalle norme vincolanti d'impresa;

e) i diritti dell'interessato in relazione al trattamento e i mezzi per esercitarli, compresi il diritto di non essere sottoposto a decisioni basate unicamente sul trattamento automatizzato, compresa la profilazione ai sensi dell'articolo 22 GDPR, il diritto di proporre reclamo all'autorità di controllo competente e di ricorrere alle autorità giurisdizionali competenti degli Stati membri conformemente all'articolo 79 GDPR, e il diritto di ottenere riparazione e, se del caso, il risarcimento per violazione delle norme vincolanti d'impresa;

f) il fatto che il titolare del trattamento o il responsabile del trattamento stabilito nel territorio di uno Stato membro si assume la responsabilità per qualunque violazione delle norme vincolanti d'impresa commesse da un membro interessato non stabilito nell'Unione; il titolare del trattamento o il responsabile del trattamento può essere esonerato in tutto o in parte da tale responsabilità solo se dimostra che l'evento dannoso non è imputabile al membro in questione;

g) le modalità in base alle quali sono fornite all'interessato le informazioni sulle norme vincolanti d'impresa, in particolare sulle disposizioni di cui alle lettere d), e) e f), in aggiunta alle informazioni di cui agli articoli 13 e 14 GDPR (su tali informazioni v. cap. *I diritti dell'interessato*);

h) i compiti del responsabile della protezione dei dati (v. cap. *Le definizioni fondamentali*) o di ogni altra persona o entità incaricata del controllo del rispetto delle norme vincolanti d'impresa all'interno del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune e il controllo della formazione e della gestione dei reclami;

i) le procedure di reclamo;

j) meccanismi all'interno del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune per garantire la verifica della conformità alle norme vincolanti d'impresa. Tali meccanismi comprendono verifiche sulla protezione dei dati e metodi per assicurare provvedimenti correttivi intesi a proteggere i diritti dell'interessato. I risultati di tale verifica dovrebbero essere comunicati alla persona o entità di cui alla lettera h) e all'organo amministrativo dell'impresa controllante del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune e dovrebbero essere disponibili su richiesta all'autorità di controllo competente;

k) i meccanismi per riferire e registrare le modifiche delle norme e comunicarle all'autorità di controllo;

l) il meccanismo di cooperazione con l'autorità di controllo per garantire la conformità da parte di ogni membro del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune, in particolare la messa a disposizione dell'autorità di controllo dei risultati delle verifiche delle misure di cui alla lettera j);

m) i meccanismi per segnalare all'autorità di controllo competente ogni requisito di legge cui è soggetto un membro del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune in un paese terzo che potrebbe avere effetti negativi sostanziali sulle garanzie fornite dalle norme vincolanti d'impresa;

n) l'appropriata formazione in materia di protezione dei dati al personale che ha accesso permanente o regolare ai dati personali.

La Commissione può specificare il formato e le procedure per lo scambio di informazioni tra titolari del trattamento, responsabili del trattamento e autorità di controllo in merito alle norme vincolanti d'impresa.

Ancora con riguardo alle norme vincolanti per l'impresa, si possono poi citare, e assumono particolare rilevanza anche dal punto di vista operativo, le Raccomandazioni 1/2022 dell'EDPB sulla domanda di approvazione e sugli elementi e sui principi che devono figurare nelle norme vincolanti d'impresa del titolare del trattamento (articolo 47 del GDPR), adottate il 20 giugno 2023.

Rispetto ai trasferimenti soggetti a garanzie adeguate, l'intervento della Corte di Giustizia dell'UE è stato molto significativo. Infatti, nella decisione del 16 luglio 2020, C-311/18, la Corte ha interpretato congiuntamente l'art. 46 GDPR e l'art. 44 GDPR, affermando che l'art. 46 GDPR

> è contenuto nel capo V del [RGPD] e deve essere pertanto letto alla luce dell'articolo 44 di detto regolamento, rubricato «Principio generale per il trasferimento», il quale dispone che «[t]utte le disposizioni [di detto capo] sono applicate al fine di assicurare che il livello di protezione delle persone fisiche garantito dal [medesimo] regolamento non sia pregiudicato». Tale livello di protezione deve, di conseguenza, essere garantito indipendentemente da quale sia la disposizione di detto capo sul cui fondamento viene effettuato un trasferimento di dati personali verso un paese terzo. (CGUE, 16 luglio 2020, C-311/18, § 92)

La Corte continua affermando che le:

> garanzie adeguate devono essere idonee a garantire che le persone i cui dati personali sono trasferiti verso un paese terzo sulla base di clausole tipo di protezione dei dati godano, come nell'ambito di un trasferimento fondato su una decisione di adeguatezza, di un livello di protezione sostanzialmente equivalente a quello garantito all'interno dell'Unione. (CGUE, 16 luglio 2020, C-311/18, § 96)

Poi, la Corte afferma che quando il trasferimento sia basato sulle clausole tipo adottate dalla Commissione *ex* art. 46, par. 2, lett. c) GDPR, le garanzie adeguate, i diritti azionabili e i mezzi di ricorso effettivi richiesti dall'art. 46 GDPR:

> devono garantire che i diritti delle persone i cui dati personali sono trasferiti verso un paese terzo sul fondamento di clausole tipo di protezione dei dati godano di un livello di protezione sostanzialmente equivalente a quello garantito all'interno dell'Unione da tale regolamento, letto alla luce della Carta. A tal fine, la valutazione del livello di protezione garantito nel contesto di un trasferimento siffatto deve, in particolare, prendere in considerazione tanto le clausole contrattuali convenute tra il titolare del trattamento o il responsabile del trattamento stabiliti nell'Unione e il destinatario del trasferimento stabilito nel paese terzo interessato quanto, per quel che riguarda un eventuale accesso delle autorità pubbliche di tale paese terzo ai dati personali così trasferiti, gli elementi rilevanti del sistema giuridico di quest' ultimo, in particolare quelli enunciati all' articolo 45, paragrafo 2 (RGPD).

L'art. 45, par. 2 GDPR, come si è detto, individua gli elementi che la Commissione Europea deve considerare nel valutare l'adeguatezza del livello di protezione.

Dunque, l'uso degli strumenti previsti dall'art. 46, par. 2 GDPR non garantisce di per sé che i trasferimenti siano conformi al GDPR. Infatti, nella sentenza appena richiamata, (CGUE, 16 luglio 2020, C-311/18) la Corte ha anche affermato che l'adozione di clausole tipo non esclude che, al fine di garantire un livello di protezione sostanzialmente equivalente a quello garantito all'interno dell'Unione da tale regolamento, letto alla luce della Carta, possa essere necessaria «in funzione della situazione esistente nell'uno o nell'altro paese terzo, l'adozione di misure supplementari da parte del titolare del trattamento» (§ 133).

5.3. Le deroghe in specifiche situazioni

In mancanza di una decisione di adeguatezza *ex* art. 45 GDPR, o di garanzie adeguate *ex* art. 46 GDPR, comprese le norme vincolanti d'impresa, è ammesso il trasferimento o un complesso di trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale soltanto se si verifica una delle seguenti condizioni:

a) l'interessato abbia esplicitamente acconsentito al trasferimento proposto, dopo essere stato informato dei possibili rischi di siffatti trasferimenti per l'in-

teressato, dovuti alla mancanza di una decisione di adeguatezza e di garanzie adeguate; tale condizione non si applica alle attività svolte dalle autorità pubbliche nell'esercizio dei pubblici poteri;

b) il trasferimento sia necessario all'esecuzione di un contratto concluso tra l'interessato e il titolare del trattamento ovvero all'esecuzione di misure precontrattuali adottate su istanza dell'interessato; tale condizione non si applica alle attività svolte dalle autorità pubbliche nell'esercizio dei pubblici poteri;

c) il trasferimento sia necessario per la conclusione o l'esecuzione di un contratto stipulato tra il titolare del trattamento e un'altra persona fisica o giuridica a favore dell'interessato; tale condizione non si applica alle attività svolte dalle autorità pubbliche nell'esercizio dei pubblici poteri;

d) il trasferimento sia necessario per importanti motivi di interesse pubblico. In questo caso, l'interesse pubblico è riconosciuto dal diritto dell'Unione o dal diritto dello Stato membro cui è soggetto il titolare del trattamento;

e) il trasferimento sia necessario per accertare, esercitare o difendere un diritto in sede giudiziaria;

f) il trasferimento sia necessario per tutelare gli interessi vitali dell'interessato o di altre persone, qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;

g) il trasferimento sia effettuato a partire da un registro che, a norma del diritto dell'Unione o degli Stati membri, mira a fornire informazioni al pubblico e può esser consultato tanto dal pubblico in generale quanto da chiunque sia in grado di dimostrare un legittimo interesse, solo a condizione che sussistano i requisiti per la consultazione previsti dal diritto dell'Unione o degli Stati membri. Il trasferimento non può riguardare la totalità dei dati personali o intere categorie di dati personali contenute nel registro. Se il registro è destinato a essere consultato da persone aventi un legittimo interesse, il trasferimento è ammesso soltanto su richiesta di tali persone o qualora tali persone ne siano i destinatari.

Inoltre, se non è possibile basare il trasferimento su una decisione di adeguatezza o sull'esistenza di garanzie adeguate, e nessuna delle deroghe appena viste è applicabile, il trasferimento verso un paese terzo o un'organizzazione internazionale è ammesso soltanto se non è ripetitivo, riguarda un numero limitato di interessati, è necessario per il perseguimento degli interessi legittimi cogenti del titolare del trattamento, su cui non prevalgano gli interessi o i diritti e le libertà dell'interessato, e qualora il titolare e del trattamento abbia valutato tutte le circostanze relative al trasferimento e sulla base di tale valutazione abbia fornito garanzie adeguate relativamente alla protezione dei dati personali. In questo caso, il titolare del trattamento informa del trasferimento l'autorità di controllo. In aggiunta alla fornitura di informazioni di cui agli articoli 13 e 14 GDPR (v. cap. *I diritti dell'interessato*), il titolare del trattamento informa l'interessato del trasferimento e degli interessi legittimi cogenti perseguiti. Ques'ultima possibilità di trasferimento non si applica alle attività svolte dalle autorità pubbliche nell'esercizio dei pubblici poteri.

Infine, in mancanza di una decisione di adeguatezza, il diritto dell'Unione o degli Stati membri può, per importanti motivi di interesse pubblico, fissare

espressamente limiti al trasferimento di categorie specifiche di dati verso un paese terzo o un'organizzazione internazionale. Gli Stati membri devono notificare tali disposizioni alla Commissione.

6. La riutilizzazione di dati personali detenuti da enti pubblici

La presa di consapevolezza sulle potenzialità derivanti dalla condivisione dei dati ha come primo punto di emersione la previsione di una disciplina di apertura dei dati e riuso delle informazioni del settore *pubblico*. Questo, come vedremo, si spiega secondo una logica molto semplice: mentre i dati del settore privato costituiscono generalmente un *asset* patrimoniale strumentale all'esercizio dell'attività d'impresa, secondo le logiche della concorrenza e della rivalità, viceversa i dati nella disponibilità dei soggetti pubblici non soggiacciono – di norma – a logiche di mercato. In altre parole, se la condivisione e il riuso dei dati nel settore privato si scontrano con le dinamiche dei vantaggi e degli svantaggi competitivi, nel settore pubblico la stessa operazione di «messa a disposizione» dei dati a soggetti terzi (pubblici o anche privati) assume i contorni di una esternalità positiva, ovvero di una azione non specificamente remunerata che produce di per sé effetti positivi sull'economia o sull'attività di altri soggetti.

6.1. La Direttiva *Open Data*

Esattamente a questa logica è ispirata la Direttiva *Open Data* 2019/1024 (recepita in Italia dal d.lgs. n. 200/2021 che ha emendato il d.lgs. 36/2006) che ha stabilito le regole per l'accesso e l'utilizzo dei dati pubblici da parte delle organizzazioni pubbliche e private all'interno dell'UE. La direttiva muove da alcune considerazioni che è qui utile riproporre:

> il *settore pubblico* degli Stati membri *raccoglie, produce, riproduce e diffonde un'ampia gamma di informazioni* in molti settori di attività, per esempio informazioni di tipo sociale, politico, economico, giuridico, geografico, ambientale, meteorologico, sismico, turistico, informazioni in materia di affari, di brevetti e di istruzione. […] La *fornitura di tali informazioni* […] consente ai cittadini e alle persone giuridiche di *individuare nuovi modi di utilizzarle* e di *creare prodotti e servizi nuovi e innovativi.* (Considerando 8)

E ancora più chiaramente:

> l'*informazione del settore pubblico* rappresenta una fonte straordinaria di dati *in grado di contribuire a migliorare il mercato interno* e lo *sviluppo di nuove applicazioni per i consumatori e le persone giuridiche*. L'utilizzo intelligente dei dati, ivi compreso il loro trattamento attraverso applicazioni di intelligenza artificiale, può *trasformare tutti i settori dell'economia.* (Considerando 9)

Per conseguenza, la direttiva fissa un *principio generale* (art. 3) per il quale i 'documenti' in possesso di enti pubblici e imprese pubbliche siano riutilizzabili «a fini commerciali o non commerciali», siano messi a disposizione in un

«lasso di tempo ragionevole» (art. 4) a titolo, di regola, gratuito (art. 6), sempre salvo il rispetto della normativa in materia di protezione dei dati personali, di diritto d'autore e di proprietà industriale.

6.2. Il profilo pubblicistico del *Data Governance Act*

Con il *Data Governance Act*, definitivamente applicabile nell'Unione europea dal 24 settembre 2023, la logica del riutilizzo dei dati pubblici viene ulteriormente sviluppata, anche muovendo dalla constatazione degli scarsi risultati prodotti su questo piano dalla Direttiva *Open Data*:

> talune categorie di dati conservati in basi di dati pubbliche, quali dati commerciali riservati, dati soggetti a segreto statistico e dati protetti da diritti di proprietà intellettuale di terzi, compresi segreti commerciali e dati personali, *spesso non sono messe a disposizione*, nemmeno per attività di ricerca o di innovazione nel pubblico interesse, *nonostante tale disponibilità sia possibile in conformità del diritto dell'Unione applicabile*. (Considerando 6)

Il Regolamento perciò mira, nella sua parte dedicata al settore pubblico, a sbloccare quelle particolari categorie di dati soggetti a regimi speciali che ne impedivano la riutilizzazione, incoraggiando l'adozione di tecniche di anonimizzazione, aggregazione *et al.* dei dati protetti in maniera tale da assicurare il pieno rispetto dei diritti di terzi.

Il *Data Governance Act*, come accennato, fornisce per la prima volta alcune importanti definizioni, relative ai concetti di 'dato' (ovvero «qualsiasi rappresentazione digitale di atti, fatti o informazioni e qualsiasi raccolta di tali atti, fatti o informazioni, anche sotto forma di registrazione sonora, visiva o audiovisiva»), di 'riutilizzo' del dato pubblico (ovvero il riuso «a fini commerciali o non commerciali»), di 'titolare dei dati' (ovvero chi «ha il diritto di concedere l'accesso a determinati dati personali o dati non personali o di condividerli»), di 'utente dei dati' (ovvero chi ha accesso ai dati e ha diritto di «utilizzare tali dati a fini commerciali o non commerciali») e di 'condivisione dei dati' (ovvero la fornitura di dati da un interessato o un titolare dei dati a un utente dei dati ai fini dell'utilizzo congiunto o individuale di tali dati, dietro compenso o a titolo gratuito sulle qualificazioni soggettive all'interno del Data Governance Act, anche in relazione al GDPR v. cap. *Le definizioni fondamentali*).

Per quanto concerne il profilo pubblicistico, il Regolamento disciplina (art. 5) le condizioni per il riutilizzo di una o più delle categorie di dati protetti *ex* art. 3, par. 1 (cioè coperti da riservatezza commerciale, statistica, protezione dei diritti di proprietà intellettuale di terzi o protezione dei dati personali), detenuti da enti pubblici, prescrivendo che esse siano pubbliche, non discriminatorie, trasparenti, proporzionate e oggettivamente giustificate in relazione alle categorie di dati e alle finalità del riutilizzo e alla natura dei dati per i quali è consentito il riutilizzo.

In ogni caso, tali condizioni non debbono «limitare la concorrenza». Il Regolamento prevede (art. 6) che gli enti pubblici che consentono il riutilizzo delle

categorie di dati protetti di cui sopra possano imporre tariffe non discriminatorie, proporzionate, oggettivamente giustificate (in particolare, per l'eventuale trattamento applicato al fine di garantire i diritti dei terzi; *e.g.* anonimizzazione, aggregazione *etc.*) e che non limitino il gioco concorrenziale. La gestione è affidata ad un sistema di sportelli unici (art. 8), con articolazione settoriale, regionale o locale.

Ad ogni modo, è opportuno chiarire che il *Data Governance Act* non fissa alcun obbligo per gli enti pubblici di acconsentire al riutilizzo dei dati, ma stabilisce una serie di regole comuni che debbono applicarsi qualora l'ente, sia pure dietro compenso, decida di consentirne l'utilizzo.

L'ente pubblico può inoltre svolgere attività di fornitura di «servizi di intermediazione dei dati», nei termini di cui si dirà *infra*, e rivestire altresì il ruolo di 'titolare dei dati' ai sensi del Regolamento in esame, ovvero di quel soggetto a cui l'interessato può richiedere di mettere i propri dati, siano essi personali o non personali, a disposizione di un soggetto terzo, 'utente dei dati', che ha diritto di utilizzarli per finalità commerciali o non commerciali.

7. La condivisione e l'accesso ai dati del settore privato

Si è detto che la recente regolazione europea mira a liberare enormi quantità di dati a beneficio del mercato e dunque a favorire quanto più possibile la loro circolazione e condivisione nel rispetto dei diritti dei soggetti interessati e dei terzi a vario titolo coinvolti. Con molta più prudenza rispetto a quanto osservato per il settore pubblico, la disciplina di favore per la condivisione e l'accesso ai dati coinvolge anche il settore privato. In particolare, come si vedrà in appresso, l'Unione europea ha varato per lo più norme incentivanti la condivisione volontaria dei dati e solo in rare ed eccezionali occasioni ha previsto formule cogenti di accesso ai dati da parte dei soggetti pubblici o di soggetti terzi del mercato.

Proseguendo la nostra disamina, muoviamo verso il lato privatistico del *Data Governance Act*. In particolare, le fattispecie rilevanti sono quelle dei «servizi di intermediazione dei dati» e dell'«altruismo dei dati».

In entrambi i casi, il cuore della proposta è la condivisione dei dati secondo la logica della non rivalità e secondo il metodo della volontarietà: il Regolamento non introduce, come accennato già per il settore pubblico, alcun obbligo di condivisione, ma promuove e regolamenta le forme attraverso le quali tale condivisione può realizzarsi. In particolare, regole stringenti sono fornite in merito alle *Condizioni per la fornitura di servizi di intermediazione dei dati* (art. 12) e ai *Requisiti generali per la registrazione* in un registro pubblico nazionale delle organizzazioni per l'altruismo dei dati riconosciute (artt. 17 ss.).

7.1. L'altruismo dei dati

L'altruismo dei dati mira a favorire la condivisione volontaria di dati *senza compenso* (salvo il rimborso dei costi sostenuti) per obiettivi di interesse generale (Capo IV del *Data Governance Act*).

L'obiettivo a tendere di questa legislazione di favore per la condivisione è perciò quello della creazione di «spazi comuni europei di dati», ossia «quadri interoperabili specifici o settoriali o intersettoriali di norme e prassi comuni per condividere o trattare congiuntamente i dati, anche ai fini dello sviluppo di nuovi prodotti e servizi, della ricerca scientifica o di iniziative della società civile» (considerando 27). L'art. 2, par. 1, n. 16), del *Data Governance Act* descrive l'altruismo dei dati come la «condivisione volontaria di dati sulla base del consenso accordato dagli interessati» o «sulle autorizzazioni di altri titolari dei dati», senza la richiesta o la ricezione di un compenso, salva la compensazione dei costi sostenuti.

Tale condivisione avviene, appunto, per fini altruistici, cioè per obiettivi di interesse generale, stabiliti nel diritto nazionale, quali l'assistenza sanitaria, la lotta ai cambiamenti climatici, il miglioramento della mobilità, l'agevolazione dell'elaborazione, della produzione e della divulgazione di statistiche ufficiali, il miglioramento della fornitura dei servizi pubblici, l'elaborazione delle politiche pubbliche o la ricerca scientifica nell'interesse generale.

Per poter concretamente realizzare tale possibilità di condivisione di dati personali e non personali, gli Stati membri saranno chiamati nei prossimi anni ad accreditare le «organizzazioni per l'altruismo dei dati» attraverso l'iscrizione in un registro pubblico nazionale. Ai sensi dell'art. 17 del *Data Governance Act*, tali organizzazioni non potranno perseguire scopi di lucro e dovranno, ai sensi degli artt. 20 e 21, assicurare un elevato livello di trasparenza in merito al trattamento di dati personali e all'utilizzo di dati non personali nonché assolvere a specifici obblighi di tutela assicurando che i dati siano sempre trattati per lo specifico fine altruistico per il quale sono stati condivisi.

7.2. I servizi di intermediazione dei dati

Come si è visto, il *Data Governance Act* favorisce la condivisione dei dati, personali e non, nella convinzione che più dati vengono condivisi fra enti pubblici e soggetti privati e fra gli stessi privati, maggiori sono le opportunità di sviluppo per l'economia europea.

In questo quadro, il legislatore eurounitario ha regolamentato una nuova tipologia di servizi, che cercano di affermarsi nella prassi: i servizi di intermediazione dei dati. Essi mirano a «instaurare, attraverso strumenti tecnici, giuridici o di altro tipo, rapporti commerciali ai fini della condivisione dei dati tra un numero indeterminato di interessati e di titolari dei dati, da un lato, e gli utenti dei dati, dall'altro, anche al fine dell'esercizio dei diritti degli interessati in relazione ai dati personali» (art. 2, n. 11), *Data Governance Act*).

Si tratta, dunque, di servizi che si prefiggono l'obiettivo di mettere in collegamento, da un lato, le persone fisiche cui i dati si riferiscono e i soggetti, diversi dagli interessati, che hanno il diritto di concedere a terzi l'accesso ai dati, anche non personali (i c.d. «titolari dei dati»: art. 2, n. 8, *Data Governance Act,* su cui v. *supra* cap. *Le definizioni fondamentali*, § 8.1) e, dall'altro, coloro che desiderano utilizzare tali dati (i c.d. «utenti dei dati»: art. 2, n. 9, *Data Governance Act,* su

cui v. *supra* cap. *Le definizioni fondamentali*, § 8.1). Il collegamento dev'essere diretto: non possono considerarsi, quindi, servizi di intermediazione dei dati quei servizi in cui il fornitore ottiene dati dai titolari per poi aggregarli, arricchirli o trasformarli, al fine di aggiungervi un valore sostanziale e concedere licenze per il loro utilizzo (art. 2, n. 11, lett. a).

L'intermediazione, inoltre, deve mirare all'instaurazione di un rapporto «commerciale» fra le due parti in questione e deve riguardare «un numero indeterminato di interessati e di titolari dei dati». Di conseguenza, tenendo conto del primo aspetto, tra i servizi in esame non rientrano i servizi di condivisione dei dati offerti da enti pubblici che agiscono per scopi diversi (art. 2, n. 11, lett. d)) e i servizi che si limitano alla messa a disposizione di strumenti tecnici per gli interessati o per i titolari dei dati per la condivisione di dati con altri (ad esempio, servizi di archiviazione sul *cloud*, di *web browser*, di posta elettronica), senza mirare né a instaurare un rapporto commerciale, né a consentire al fornitore di acquisire informazioni in merito all'eventuale instaurazione del rapporto commerciale (v. considerando 28, *Data Governance Act*). Valorizzando il secondo aspetto, occorre escludere dai servizi di intermediazione in esame quelli utilizzati da un titolare dei dati, o comunque all'interno di un gruppo chiuso di soggetti, al fine di garantire la funzionalità di oggetti o dispositivi connessi all'Internet delle cose (art. 2, n. 11, lett. c)). Infine, un'ulteriore esclusione si basa sull'oggetto dei servizi: se questo è rappresentato da «contenuti protetti da diritto d'autore», l'intermediazione non ricade nella definizione data dal legislatore europeo (art. 2, n. 11, lett. b)).

In concreto, tra gli esempi di servizi di intermediazione dei dati, il *Data Governace Act* cita: i mercati dei dati su cui le imprese possono mettere dati a disposizione di terzi, gli orchestratori di ecosistemi di condivisione dei dati aperti a tutte le parti interessate, nonché i *pool* di dati creati congiuntamente da più persone fisiche o giuridiche con l'intento di concedere licenze per il loro uso a tutte le parti interessate in modo che tutti i partecipanti che contribuiscono al *pool* siano ricompensati per il loro contributo (considerando 28).

Nell'ambito di tali servizi, meritano una menzione speciale i fornitori che hanno come obiettivo principale quello di aiutare gli interessati nell'esercizio dei loro diritti, riconosciuti dal GDPR, in relazione ai dati personali oggetto di trattamento da parte di terzi. Tali fornitori prendono il nome di «cooperative di dati» (v. art. 2, n. 15, *Data Governance Act*) nella misura in cui la struttura organizzativa sia costituita proprio da interessati, nei cui confronti – in quanto membri dell'organizzazione – la cooperativa interverrà in aiuto. Peraltro, tali cooperative di dati possono avere come membri anche piccole e medie imprese (PMI), che, laddove siano esercitate da enti collettivi (ad esempio, società commerciali), quindi soggetti diversi da persone fisiche, non sono certamente qualificabili come interessati al trattamento ai sensi del GDPR. Ciononostante, anche le PMI possono aver bisogno di un'organizzazione che le aiuti nell'esercizio dei loro diritti in relazione a determinati dati non personali.

Considerata l'importanza dei servizi di intermediazione dei dati, anche in ragione dei delicati interessi in gioco, il *Data Governance Act* sottopone la lo-

ro fornitura a una serie di condizioni stringenti tanto sul piano dei divieti (v. art. 12, lett. a), b) e, indirettamente, e)), quanto sul piano degli obblighi (v. art. 12, lett. c), d), f), g), h), i), j), k), l), m), n) ed o)), tra cui spicca l'obbligo di far sì che la procedura di accesso al servizio sia equa, trasparente e non discriminatoria sia per gli interessati e i titolari dei dati, sia per gli utenti dei dati, anche per quanto riguarda i prezzi e le condizioni di servizio. Inoltre, il fornitore di servizi di intermediazione dei dati può avviare la fornitura solo dopo aver presentato una notifica all'autorità competente, per i cui compiti, a livello nazionale, è designata come responsabile l'Agenzia per l'Italia Digitale (AGID) (art. 2, d.lgs. n. 144/2024).

8. I rapporti fra titolari, utenti e destinatari dei dati generati da «prodotti connessi» o «servizi correlati»

Il *Data Act* costituisce un'ulteriore disciplina che interviene nell'ambito della circolazione dei dati, ma, a differenza del *Data Governance Act*, non si limita a favorirne la condivisione attraverso pratiche volontarie, posto che impone, in determinati rapporti fra privati, specifici obblighi di accesso ai dati.

Inoltre, rispetto ad altre normative, il *Data Act* si distingue per il fatto di prendere in esame soltanto una peculiare tipologia di dati, ossia quelli generati dall'uso di un prodotto connesso a Internet (ad esempio, un dispositivo domotico o una macchina agricola intelligente) o di un servizio a esso correlato. Tali dati possono essere sia di natura *personale*, se forniscono informazioni ricollegabili a una persona fisica, sia di carattere *non personale*, se forniscono informazioni che non sono in grado di riguardare una persona fisica identificata o identificabile (ad esempio, le informazioni sui componenti di un suolo agricolo o sulla temperatura rilevata in una determinata area).

La generazione dei dati in esame è il risultato delle azioni di almeno due soggetti: il progettista o il fabbricante di un prodotto connesso, che in molti casi può essere anche un fornitore di servizi correlati, e l'utente del prodotto connesso o del servizio correlato (v. considerando 6 *Data Act*). Nonostante l'attività dell'utente sia fondamentale, nella prassi attuale è frequente che quest'ultimo, a causa del modo in cui i prodotti connessi sono progettati o delle misure di protezione adottate successivamente, non abbia accesso ai dati generati dall'uso di tali prodotti o servizi correlati, a meno che questi dati non siano dati personali cui poter accedere esercitando il diritto di cui all'art. 15 GDPR.

Per superare gli ostacoli della realtà appena descritta, il *Data Act* prevede che i dati in questione debbano essere resi accessibili all'utente (art. 3); qualora quest'ultimo non possa farlo direttamente a partire dal prodotto connesso o dal servizio correlato, il «titolare dei dati» deve mettere prontamente a disposizione dell'utente i dati, nonché i pertinenti metadati necessari per interpretare e utilizzare tali dati, senza indebito ritardo, con la stessa qualità di cui egli stesso dispone, in modo facile, sicuro e gratuito, in un formato completo, strutturato, di uso comune e leggibile da dispositivo automatico e, ove

pertinente e tecnicamente possibile, in modo continuo e in tempo reale (art. 4, par. 1, *Data Act*).

Il «titolare dei dati», in quest'ambito, è definito come la persona fisica o giuridica che ha il diritto o l'obbligo, in base all'ordinamento europeo o nazionale, di utilizzare e mettere a disposizione dati, «compresi, se concordato contrattualmente, dati del prodotto o di un servizio correlato che ha reperito o generato nel corso della fornitura di un servizio correlato» (art. 2, n. 13), *Data Act*) (per un confronto di tale definizione con quella contenuta nel *Data Governance Act*, v. *supra* cap. *Le definizioni fondamentali*, § 8.1).

In casi particolari, il titolare dei dati può rifiutare una richiesta di accesso ai dati pervenuta dall'utente. Ciò può accadere quando: a) l'accesso ai dati possa compromettere i requisiti di sicurezza del prodotto connesso e comportare gravi effetti negativi per la salute, la sicurezza o la protezione di persone fisiche (art. 4, par. 2, *Data Act*); b) i dati in questione siano in grado di rivelare segreti commerciali del titolare e quest'ultimo possa dimostrare, sulla base di elementi oggettivi, che, a causa della divulgazione di tali segreti, subirebbe molto probabilmente gravi danni economici, anche se l'utente adottasse tutte le misure necessarie per tutelarne la riservatezza (art. 4, par. 8, *Data Act*).

Al di fuori di tali ipotesi, il titolare dei dati non solo deve concedere l'accesso all'utente, ma deve anche, se questi lo richiede, mettere a disposizione di terzi i dati che ottiene o può ottenere legittimamente dal prodotto connesso o dal servizio correlato, senza che ciò implichi uno sforzo sproporzionato che vada al di là di una semplice operazione (art. 5, par. 1, *Data Act*). I terzi in questione (ad esempio, imprese interessate a trattare i dati generati dai prodotti connessi per sviluppare servizi digitali innovativi), denominati «destinatari dei dati», devono di regola corrispondere al titolare dei dati un compenso, che verrà concordato con quest'ultimo insieme alle modalità di messa a disposizione dei dati.

Per entrambi i casi, le relative condizioni contrattuali devono essere eque, ragionevoli e non discriminatorie (v. artt. 8-9 *Data Act*). Invero, se una clausola contrattuale viene imposta unilateralmente dal titolare dei dati e si rivela essere abusiva, ossia di natura tale che il suo utilizzo si discosta considerevolmente dalle buone prassi commerciali in materia di accesso ai dati e relativo utilizzo, in contrasto con il principio di buona fede e correttezza, tale clausola non vincola (v. art. 13, parr. 1 e 3, *Data Act*). La novità di tale previsione è che essa consente di accertare l'abusività di una clausola – e dichiararne la conseguente nullità, secondo il diritto italiano – anche nei contratti tra imprese, e non solo nei contratti dei consumatori, per i quali già si applicano le norme in tema di clausole vessatorie contenute negli artt. 33 ss. cod. cons.

I diritti riconosciuti dal *Data Act* agli utenti integrano i diritti di accesso e alla portabilità dei dati di cui agli artt. 15 e 20 GDPR. Ad ogni modo, nell'eventualità di un conflitto tra il *Data Act* e il diritto dell'Unione in materia di protezione dei dati personali o la legislazione nazionale adottata conformemente a tale diritto dell'Unione, la prevalenza va accordata a queste ultime discipline (art. 1, par. 5, *Data Act*).

Riferimenti bibliografici

Angiolini, Chiara. 2020. *Lo statuto dei dati personali. Uno studio a partire dalla nozione di bene*. Torino: Giappichelli.

Bachelet, Vittorio, Gianluigi Marino e Antonio Racano (a cura di). 2025. *Data Act. Accesso equo ai dati e loro utilizzo: profili sistematici e applicativi nell'orizzonte del diritto privato*. Wolters Kluwer.

Batlle, Sergi, van Waeyenberge, Arnaud. 2024. "EU-US Data Privacy Framework: A First Legal Assessment." *European Journal of Risk Regulation* 1.

Bravo, Fabio. 2021. "Intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act." In *Contratto impresa e Europa* 1: 199-256.

Cuffaro, Vincenzo, D'Orazio, Roberto, Ricciuto, Vincenzo (a cura di). 2019. *I dati personali nel diritto europeo*. Torino: Giappichelli.

Proietti, Giuseppe. 2023. "Il trasferimento dei dati personali all'estero: proporzionalità, poteri delle agenzie di intelligence ed effetto Bruxelles." *Il diritto dell'Informazione e dell'informatica* 6.

Ricciuto, Vincenzo. 2022. *L'equivoco della privacy. Persona vs dato personale*. Napoli: Edizioni Scientifiche Italiane.

La regolamentazione e la tutela amministrativa

Elia Cremona

Abstract: This chapter analyses the public bodies entrusted with regulating, monitoring and enforcing data protection and data governance rules. In particular, it illustrates the sanctioning and non-sanctioning measures that can be taken by the supervisory authority.

Keywords: Data protection bodies, data governance bodies, penalties, administrative actions

1. Il ruolo dell'autorità garante nazionale

Il Garante per la protezione dei dati personali, anche noto come Garante privacy, è un'autorità amministrativa indipendente. L'autorità è stata istituita con la l. n. 675/96, la quale recepiva la direttiva 95/46/CE, ed è oggi «Autorità di controllo» incaricata di controllare la corretta applicazione del Regolamento in materia di protezione dei dati personali ai sensi dell'art. 51 GDPR e dell'art. 153 del d.lgs. 196/2003 (d'ora in avanti: cod. privacy).

L'istituzione del Garante per la Privacy nasce dall'esigenza di proteggere le persone fisiche riguardo al trattamento dei loro dati personali, garantendo che tale trattamento avvenga nel rispetto dei diritti e delle libertà fondamentali, senza che – allo stesso tempo – sia pregiudicata la libera circolazione dei dati personali all'interno dell'Unione.

Il Garante, dunque, si configura oggi come una autorità amministrativa con una *mission* supplementare rispetto ad altre autorità: non è chiamato a svolgere una attività meramente tecnica di regolazione del mercato in un'ottica di efficienza economica, ma ha il compito di presidiare la tutela di diritti e libertà fondamentali.

Per questa ragione, è particolarmente importante che sia assicurata l'indipendenza dei suoi componenti nell'adempimento dei propri compiti e nell'esercizio dei propri poteri, ai sensi dell'art. 52 GDPR. I componenti del collegio, infatti, debbono astenersi da qualunque attività incompatibile con le loro funzioni per tutta la durata del mandato.

Elia Cremona, University of Siena, Italy, elia.cremona@unisi.it, 0000-0001-9336-218X

Referee List (DOI 10.36253/fup_referee_list)
FUP Best Practice in Scholarly Publishing (DOI 10.36253/fup_best_practice)

Ai sensi dell'art. 153 cod. privacy, il collegio è composto da quattro componenti, eletti due dalla Camera dei deputati e due dal Senato della Repubblica con voto limitato (i parlamentari possono cioè esprimere un numero di preferenze inferiore rispetto al totale dei candidati, in modo da assicurare l'elezione di almeno un candidato espresso dai gruppi di minoranza).

Dal 2018 si prevede poi che i componenti siano eletti tra coloro che presentano la propria candidatura nell'ambito di una procedura di selezione il cui avviso deve essere pubblicato nei siti internet della Camera, del Senato e del Garante. Le candidature possono essere avanzate da persone che assicurino, come accennato, indipendenza e che risultino di comprovata esperienza nel settore della protezione dei dati personali, con particolare riferimento alle discipline giuridiche o dell'informatica.

I componenti eleggono tra loro un presidente, il cui voto prevale in caso di parità, e un vicepresidente, che assume le funzioni del presidente in caso di sua assenza o impedimento. L'incarico di presidente e quello di componente hanno durata settennale e non sono rinnovabili.

L'autorità opera in piena autonomia, sia amministrativa che finanziaria, e le sue decisioni possono essere impugnate solo davanti al giudice ordinario.

Il ruolo del Garante è variegato e comprende diversi «compiti» (*ex* art. 57 GDPR e 154 cod. privacy) e «poteri» (*ex* art. 58 GDPR e 154-*bis* cod. privacy).

Tra i «compiti» vi è naturalmente quello di assicurare e sorvegliare l'applicazione del GDPR da parte di soggetti pubblici e privati, controllando altresì l'applicazione delle norme nazionali in materia di protezione dei dati. Questo include, ad esempio, la verifica che i dati siano raccolti e trattati solo per finalità legittime, che il trattamento sia proporzionato e trasparente, o che siano adottate tutte le misure necessarie per garantire la sicurezza dei dati, evitando accessi non autorizzati, perdite o distruzioni accidentali.

A questa competenza principale si affiancano ulteriori compiti di carattere informativo, finalizzati alla promozione della consapevolezza pubblica su questi temi, e l'attività consultiva, principalmente rivolta nei confronti del Parlamento, del Governo e di altri organismi istituzionali. Il Garante è altresì titolare di specifiche competenze regolatorie di integrazione contrattuale consistenti ad esempio nella adozione di «clausole contrattuali tipo» o nella approvazione delle «norme vincolanti d'impresa», v. cap. Le fonti della disciplina in materia di dati personali).

Per quanto riguarda invece i «poteri», si distinguono i) i poteri di indagine, ii) i poteri correttivi e sanzionatori e iii) i poteri autorizzativi e consultivi.

Quanto ai primi, essi consentono all'autorità di condurre accertamenti e raccogliere informazioni. Ad esempio, può richiedere informazioni al titolare del trattamento e al responsabile del trattamento, può effettuare ispezioni e audit dei trattamenti di dati, può accedere a qualsiasi locale in cui sono trattati i dati.

Quanto ai poteri correttivi e sanzionatori, essi includono il potere di emettere ammonimenti o avvertimenti al titolare o al responsabile del trattamento, di imporre limiti o divieti sul trattamento dei dati, di disporre la rettifica o la

cancellazione di dati personali o la limitazione del trattamento e, infine, come si vedrà, di comminare sanzioni amministrative, comprese le multe.

Infine, per quanto attiene ai poteri autorizzativi e consultivi, essi consentono all'autorità di controllo di intervenire in alcune situazioni su richiesta di soggetti pubblici e privati, potendo rilasciare pareri – quando richiesto – in materia di trattamenti o autorizzare clausole contrattuali standard o meccanismi di trasferimento di dati verso paesi terzi. Il Garante ha anche il potere di esprimere pareri su atti normativi e regolamenti che possono influire sulla protezione dei dati personali, assicurando che ogni nuova normativa rispetti i principi fondamentali della materia. Inoltre, gestisce i reclami presentati dai cittadini riguardanti presunte violazioni dei loro diritti relativi alla privacy.

Oltre alle sue attività a livello nazionale, il Garante per la Privacy collabora strettamente con altre autorità nazionali per la protezione dei dati all'interno dell'Unione Europea e a livello internazionale. Questo lavoro di collaborazione è fondamentale per affrontare le sfide globali legate alla protezione dei dati, come l'armonizzazione delle normative tra diversi paesi e la gestione delle problematiche legate ai trasferimenti internazionali di dati personali.

2. Il ruolo dell'European Data Protection Board e il meccanismo di coerenza

L'European Data Protection Board (EDPB) è un organismo indipendente dell'UE istituito dal GDPR, con il compito di garantire un'applicazione coerente del regolamento in tutta l'Unione Europea. Esso è composto dai rappresentanti delle autorità di controllo di ciascun Stato membro e dal Garante europeo per la protezione dei dati. Il Board raccoglie l'eredità del Working Party 29, gruppo di lavoro istituito ai sensi dell'art. 29 della previgente direttiva 95/46/CE che aveva avviato un'importante opera di interpretazione e indirizzo volta ad armonizzare l'applicazione del diritto europeo in materia di protezione dei dati personali.

Le funzioni dell'EDPB sono disciplinate dagli articoli 68-76 del GDPR e si caratterizzano per una doppia natura, in parte consultiva e in parte decisoria. In particolare, come previsto dall'art. 70 GDPR, il Board ha il compito di monitorare l'attuazione del Regolamento e di assicurare la corretta applicazione del regolamento attraverso la pubblicazione di linee guida, raccomandazioni e buone prassi.

Il Board fornisce inoltre pareri e consulenze alla Commissione, relativamente agli adempimenti connessi all'applicazione del GDPR, e alle autorità di controllo nazionali. In particolare, coordina e supervisiona il funzionamento del «meccanismo di coerenza», uno degli strumenti fondamentali per garantire l'uniformità nell'applicazione del GDPR (*ex* artt. 63-66 del Regolamento).

Ai sensi dell'art. 64 GDPR, infatti, viene richiesto da parte delle autorità nazionali il parere dell'EDPB quando queste redigono una lista dei tipi di trattamenti che richiedono una valutazione di impatto (DPIA), o quando approvano clausole contrattuali standard per il trasferimento di dati verso paesi terzi o organizzazioni internazionali, o ancora codici di condotta che riguardano il trattamento di dati personali transfrontaliero o internazionale.

In tutti questi casi, l'EDPB è tenuto ad intervenire secondo una procedura dettagliata, che prevede: 1) *Richiesta di parere*: l'autorità di controllo che intende adottare una misura, che può avere un impatto su trattamenti transfrontalieri o può richiedere un'armonizzazione a livello europeo, invia una richiesta formale di parere all'EDPB; 2) *Termine per il parere dell'EDPB*: l'EDPB deve emettere il suo parere entro un termine massimo di otto settimane dalla ricezione della richiesta. Tale termine può essere prorogato di altre sei settimane per questioni particolarmente complesse. L'autorità di controllo che ha richiesto il parere deve necessariamente attendere la decisione dell'EDPB prima di adottare la propria misura; 3) *Efficacia del parere*: Sebbene i pareri dell'EDPB non siano sempre vincolanti, l'autorità di controllo, ricevuta la notifica, è tenuta a dare seguito a essi e a giustificare ogni eventuale decisione contraria.

In casi di disaccordo, può essere attivato il «meccanismo di composizione delle controversie» dell'art. 65. Il meccanismo si applica in situazioni in cui, ad esempio, vi sia disaccordo tra un'autorità di controllo competente e l'EDPB o tra l'autorità di controllo capofila e le altre autorità interessate in un trattamento transfrontaliero.

La procedura inizia con la richiesta di una delle autorità coinvolte all'EDPB di intervenire per risolvere la controversia. Il Board emette quindi una decisione vincolante entro un mese (prorogabile di altre due settimane per casi particolarmente complessi). Questa decisione può confermare il parere dell'autorità principale, accogliere i punti sollevati dalle altre autorità o risolvere questioni specifiche di disaccordo. Una volta adottata, la decisione vincolante viene notificata a tutte le autorità coinvolte, le quali devono poi applicarla nei rispettivi ordinamenti nazionali.

L'articolo 65 si collega strettamente al meccanismo dello sportello unico (c.d. *one-stop-shop*) previsto dall'art. 60 GDPR. In caso di trattamenti transfrontalieri, infatti, l'autorità capofila adotta la decisione notificandola presso lo stabilimento principale del titolare o responsabile del trattamento, ma il meccanismo di risoluzione delle controversie garantisce che, anche in caso di disaccordi tra le autorità, vi sia un intervento dell'EDPB volto ad assicurare coerenza.

3. Il ruolo dell'European Data Protection Supervisor

L'European Data Protection Supervisor (EDPS), o Garante europeo per la protezione dei dati, è un organismo dell'Unione istituito per garantire che le istituzioni e gli organismi dell'Unione Europea rispettino le norme sulla protezione dei dati personali. Il suo mandato è disciplinato dal Regolamento UE 2018/1725, che stabilisce le regole per il trattamento dei dati personali da parte delle istituzioni europee, riflettendo principi simili a quelli del GDPR.

Il Parlamento europeo e il Consiglio nominano di comune accordo il Garante europeo della protezione dei dati, per un periodo di cinque anni, in base a un elenco predisposto dalla Commissione dopo un invito pubblico a presentare candidature. L'elenco di candidati deve essere composto da personalità che offrano ogni garanzia di indipendenza e che possiedano una conoscenza specialistica in materia di protezione dei dati.

A differenza delle autorità di controllo nazionali, che vigilano sull'applicazione del GDPR nei singoli Stati membri, l'EDPS ha la responsabilità esclusiva di monitorare il rispetto delle norme in materia di protezione dei dati personali da parte del Parlamento Europeo, della Commissione Europea e del Consiglio dell'Unione Europea. Nell'ambito dell'assetto istituzionale dell'Unione, riveste un duplice ruolo: da un lato, assicura la conformità del trattamento dei dati delle istituzioni europee, dall'altro fornisce pareri consultivi in materia di protezione dei dati, in particolare quando nuove normative o politiche UE impattano sui diritti dei cittadini.

Tra i poteri dell'EDPS rientrano quelli di condurre indagini e prendere misure correttive in caso di violazioni delle norme sulla protezione dei dati. Può altresì emettere ammonimenti, ordini di rettifica o cancellazione dei dati trattati in modo illegittimo, e imporre limitazioni o divieti sul trattamento. Come accennato, si tratta di poteri che riflettono quelli delle autorità di controllo nazionali, ma sono focalizzati esclusivamente sulle istituzioni dell'UE.

Un altro aspetto rilevante del mandato dell'EDPS è la sua partecipazione in seno all'European Data Protection Board (EDPB), nell'ambito del quale collabora, ad esempio, nella risoluzione di eventuali questioni transfrontaliere riguardanti il trattamento di dati personali da parte delle istituzioni UE.

L'EDPS gioca anche un ruolo di primo piano nella promozione della consapevolezza sui diritti alla protezione dei dati. Secondo l'art. 57(1)(b) del Regolamento 2018/1725, il Garante ha il compito di informare e sensibilizzare il pubblico e le istituzioni dell'UE sui rischi, le norme e i diritti relativi alla protezione dei dati personali.

4. Le autorità per i servizi di intermediazione dei dati e per l'altruismo dei dati

Come si è visto nel Capitolo precedente, il fenomeno della circolazione dei dati è regolato da norme ulteriori e complementari rispetto al GDPR, che si limita a disciplinare le forme e i modi del trattamento dei dati personali. Tra queste, il *Data Governance Act* (Regolamento UE 2022/868), delinea le responsabilità di ulteriori autorità con l'obiettivo di promuovere un utilizzo responsabile e sicuro dei dati sia a livello commerciale sia a fini altruistici.

In particolare, gli Stati membri sono obbligati a designare le «autorità competenti per i servizi di intermediazione dei dati» e quelle «per la registrazione delle organizzazioni per l'altruismo dei dati».

Con riferimento alle prime, ai sensi dell'art. 13 del *Data Governance Act*, la designazione di una o più autorità competenti è funzionale a gestire la procedura di notifica e monitoraggio dei fornitori di servizi di intermediazione dei dati. Queste autorità sono cioè incaricate di verificare la conformità dei fornitori ai requisiti stabiliti dal Regolamento, nonché di intervenire in caso di violazioni. Tra i loro poteri, figurano la richiesta di informazioni necessarie per il controllo e la possibilità di imporre sanzioni o di sospendere i servizi in caso di mancato rispetto delle norme.

Queste autorità devono cooperare strettamente con altre entità nazionali, come le autorità per la protezione dei dati, le autorità di concorrenza e quelle

responsabili della sicurezza informatica, per garantire una regolamentazione armonizzata e coerente a livello nazionale e sovranazionale.

Le autorità competenti per la registrazione delle organizzazioni per l'altruismo dei dati hanno invece il compito, ai sensi dell'art. 23 del Data Governance Act, di mantenere un registro pubblico delle organizzazioni riconosciute che operano a fini di altruismo dei dati. Queste organizzazioni, che raccolgono dati messi a disposizione volontariamente dai cittadini per finalità di interesse generale, devono rispettare criteri rigorosi di trasparenza e sicurezza. Le autorità competenti monitorano il rispetto di tali criteri e collaborano con altre entità per garantire, anche in questo caso, la corretta gestione dei dati, in particolare quando tali dati comprendono informazioni personali.

Ogni Stato membro deve notificare alla Commissione Europea le autorità competenti individuate e tali registrazioni sono rese pubbliche per garantire trasparenza e fiducia nel sistema.

Infine, sia le autorità di intermediazione dei dati che quelle per l'altruismo dei dati debbono essere giuridicamente indipendenti e garantire l'imparzialità delle loro decisioni, al fine di promuovere un ambiente di scambio dei dati sicuro e trasparente per cittadini e aziende.

5. Il Comitato europeo per l'innovazione in materia di dati

Il Comitato europeo per l'innovazione in materia di dati, istituito dalla Commissione Europea, è un gruppo di esperti volto a promuovere una governance efficace dei dati nell'Unione Europea. Questo comitato è composto da rappresentanti delle autorità competenti per i servizi di intermediazione dei dati, per la registrazione delle organizzazioni per l'altruismo dei dati, del Comitato europeo per la protezione dei dati, del Garante europeo della protezione dei dati, dell'European Union Agency for Cybersecurity (ENISA), della Commissione e da altri rappresentanti rilevanti, inclusi quelli per le PMI e altri settori specifici.

Secondo l'articolo 29 del *Data Governance Act*, il Comitato ha – tra gli altri – il compito di consigliare e assistere la Commissione nello sviluppo di una prassi coerente per il riutilizzo dei dati e per l'altruismo dei dati nell'Unione. Il Comitato opera anche attraverso la costituzione di sottogruppi che si occupano di specifici temi, come le questioni tecniche legate alla portabilità e interoperabilità dei dati, oltre che al coinvolgimento dei portatori di interessi, incluse le imprese e la società civile.

6. Le sanzioni amministrative e gli altri provvedimenti dell'autorità

Il rispetto del Regolamento è garantito attraverso un complesso sistema sanzionatorio, di natura amministrativa e penale, a seconda della gravità dell'infrazione commessa. In particolare, l'articolo 83 GDPR stabilisce un sistema di sanzioni amministrative pecuniarie. Per espressa previsione della norma, tali sanzioni devono essere «effettive, proporzionate e dissuasive», e il loro ammontare varia a seconda della gravità della violazione e delle circostanze del

caso specifico. Le sanzioni pecuniarie possono arrivare fino a 20 milioni di euro o al 4% del fatturato mondiale annuo dell'impresa, a seconda di quale delle due sia la cifra maggiore.

Il GDPR distingue due livelli di gravità delle violazioni, con sanzioni differenti. Il primo livello, disciplinato dal paragrafo 4 dell'articolo 83, prevede multe fino a 10 milioni di euro o al 2% del fatturato annuo globale, per violazioni legate agli obblighi di natura tecnica e organizzativa. Ad esempio, rientrano in questa categoria le violazioni degli articoli 8 (condizioni applicabili al consenso dei minori), 11 (trattamento che non richiede identificazione), e 25-39, che riguardano i principi di «privacy by design» e «privacy by default», la nomina e i compiti del responsabile della protezione dei dati (DPO), e altre misure tecniche e organizzative atte a garantire la sicurezza dei dati personali.

Il secondo livello di gravità, disciplinato dai paragrafi 5 e 6 dell'articolo 83, prevede sanzioni più severe, fino a 20 milioni di euro o al 4% del fatturato mondiale annuo, per violazioni dei principi fondamentali del GDPR. In questa categoria rientrano le violazioni degli articoli 5, 6, 7 e 9, che trattano i principi di base per il trattamento dei dati, le condizioni di liceità del trattamento, le condizioni per il consenso e il trattamento di categorie particolari di dati personali, come quelli relativi alla salute o all'orientamento sessuale. Anche le violazioni riguardanti i diritti degli interessati, previsti negli articoli 12-22, come il diritto di accesso, rettifica, cancellazione (diritto all'oblio), portabilità e opposizione, sono soggette a tale trattamento sanzionatorio.

Le autorità di controllo, che hanno il compito di monitorare la conformità al GDPR, sono i soggetti deputati alla irrogazione delle sanzioni in caso di violazione. Nel decidere se infliggere una sanzione amministrativa pecuniaria e nel determinare il suo importo, l'autorità di controllo deve tenere in considerazione una serie di fattori elencati nel paragrafo 2 dell'articolo 83, che include undici criteri specifici. Tra questi figurano: la natura, la gravità e la durata della violazione, avuto riguardo al tipo di trattamento e al numero di soggetti coinvolti; il carattere doloso o colposo della violazione; le misure adottate per attenuare i danni subiti dagli interessati; il grado di responsabilità del titolare o del responsabile del trattamento, considerando le misure tecniche e organizzative adottate in conformità con gli articoli 25 e 32; le eventuali precedenti violazioni pertinenti; il grado di cooperazione con l'autorità di controllo; le categorie di dati personali interessate dalla violazione, come dati particolari ai sensi dell'articolo 9; le modalità con cui l'autorità di controllo ha preso conoscenza della violazione, ad esempio, se la violazione è stata notificata dal titolare come previsto dall'articolo 33; l'adesione a codici di condotta o meccanismi di certificazione.

Tutti questi criteri devono essere contemporaneamente presi in considerazione dall'autorità di controllo nella commisurazione della sanzione da infliggere, che deve quindi essere sempre proporzionalmente gradata.

Inoltre, il paragrafo 3 dell'articolo 83 stabilisce che se un titolare del trattamento o un responsabile viola con dolo o colpa più disposizioni del GDPR in relazione allo stesso trattamento o a trattamenti collegati, l'importo totale della sanzione non deve superare quello previsto per la violazione più grave. Questo al

fine di evitare un cumulo di sanzioni sproporzionato e di garantire che la multa sia ragionevole in base alla gravità complessiva della condotta.

Oltre alla funzione correttiva, le sanzioni del GDPR perseguono un importante scopo dissuasivo. La severità del trattamento sanzionatorio mira a scoraggiare le imprese dal violare le norme, promuovendo al contempo una cultura di *compliance* alla disciplina in materia di protezione dei dati personali. Per esempio, l'articolo 58, paragrafo 2, conferisce alle autorità di controllo ampi poteri correttivi, tra cui l'emissione di ammonimenti, ordini di limitazione o sospensione del trattamento.

In Italia, come si è detto in apertura di questo Capitolo, il Garante per la protezione dei dati personali è l'autorità di controllo designata per l'applicazione delle sanzioni del GDPR. Il d.lgs. 196/2003 ha modificato il Codice Privacy (d.lgs. 196/2003) per allinearlo al GDPR. Tra le modifiche più significative, vi è stata proprio l'introduzione di sanzioni amministrative per le violazioni del Codice italiano che corrispondono a quelle previste dal GDPR. Il Garante ha il potere di avviare procedimenti sanzionatori sia su segnalazione degli interessati sia d'ufficio, e può imporre provvedimenti correttivi in caso di violazioni accertate.

7. Le azioni nei confronti dell'autorità di controllo

Contro i provvedimenti del Garante per la protezione dei dati personali può essere presentato ricorso innanzi al giudice ordinario in virtù del combinato disposto degli artt. 78 GDPR, 152 cod. privacy, e 10 del d.lgs. 150/2011 recante la disciplina dei procedimenti civili semplificati. In particolare, l'art. 78 GDPR garantisce agli interessati il diritto a un ricorso giurisdizionale effettivo contro le decisioni dell'autorità di controllo, mentre l'art. 152 cod. privacy disciplina le modalità di impugnazione dei provvedimenti del Garante, rinviando per quanto attiene ai profili processuali al d.lgs. 150/2011.

Quest'ultimo, all'art. 10, stabilisce che i provvedimenti del Garante possono essere impugnati dinanzi al giudice ordinario, che il ricorso deve essere presentato entro 30 giorni dalla notifica del provvedimento o entro 60 giorni se il ricorrente è residente all'estero. Il ricorrente può altresì dare mandato a un ente del terzo settore che sia attivo nel settore della tutela dei diritti e delle libertà degli interessati con riguardo alla protezione dei dati personali, che può esercitare l'azione in sua vece.

Durante il procedimento, il ricorrente può chiedere la modifica, la sospensione o l'annullamento del provvedimento del Garante, come nei casi di sanzioni amministrative ritenute sproporzionate o di presunte violazioni procedurali. Il giudice esamina la legittimità del provvedimento e il rispetto delle regole relative al procedimento che ne ha condotto all'adozione: un vizio di legittimità nell'attività procedimentale (ad esempio, l'eccessiva durata della fase istruttoria) può infatti determinare l'annullabilità del provvedimento finale, ancorché sostanzialmente corretto.

La sentenza che definisce il giudizio non è appellabile e può prescrivere tutte le misure ritenute necessarie dal giudice, anche in difformità da quanto previsto dal provvedimento impugnato, oltre a provvedere – quando richiesto – in merito al risarcimento del danno.

Riferimenti bibliografici

Belisario, E., G. M. Riccio e G. Scorza. 2023. *GDPR e normativa privacy*. Alphen aan den Rijn: Wolters Kluwer, pp. 729 ss.

Bolognini, L., E. Pellino e C. Bistolfi (a cura di). 2016. *Il Regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*. Milano: Giuffrè.

European Data Protection Board (EDPB). 2022. *Linee guida 4/2022 sul calcolo delle sanzioni amministrative pecuniarie ai sensi del GDPR*. [s.l.]: EDPB.

Grossi, L. 2023. "Sulla decisione della Data Protection Commission irlandese nel caso Meta: il ruolo delle autorità indipendenti nella protezione dei dati personali." In *Rivista della regolazione dei mercati*, fasc. 2/2023, pp. 474 ss.

Guzzardo, G. 2018. "Accountability e pubbliche Amministrazioni nel regolamento europeo in materia di protezione dei dati personali." In *Amministrazione In Cammino*, 1° aprile 2018.

Il risarcimento del danno da illecito trattamento dei dati personali

Gianluca Navone

Abstract: The chapter concerns compensation in the field of personal data protection, analysing the elements necessary for having access to compensation, the sujects liable, and the issue of quantification of damages.

Keywords: Compensation, liability rules in data protection, damages, non material damages, liable subjects

1. Introduzione

Dal 25 maggio 2018 – giorno nel quale è divenuto pienamente applicabile in tutti gli Stati membri dell'Unione europea il Reg. 2016/679 (d'ora in avanti: GDPR) – la materia della responsabilità civile da illecito trattamento dei dati personali è assoggettata al governo di un'unica regola continentale. Quella uniformemente enunziata dall'art. 82 GDPR che, rubricato sotto la dizione «Diritto al risarcimento e responsabilità», nella sua parte essenziale così recita: «Chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento», salvo che questi ultimi non riescano a dimostrare che «l'evento dannoso non gli è in alcun modo imputabile».

In esordio, merita di essere segnalato che l'essenziale novità della disposizione appena riportata non risiede tanto nella sua formulazione letterale, quanto nel fatto di essere posta in via esclusiva da una fonte europea di tipo regolamentare; e quindi, da uno strumento giuridico di uniformazione che – come si sa – è *self-executing*: interamente vincolante e direttamente applicabile in ciascuno dei Paesi dell'Unione, senza alcuna mediazione dei diritti interni d'attuazione.

Siamo dunque al cospetto di una fattispecie d'illecito sovranazionale (essa non appartiene a questo o a quell'ordinamento statale), alla pietra di fondazione di un edificio normativo in larga misura da costruire, quello del *diritto comune europeo della responsabilità civile*.

Gianluca Navone, University of Siena, Italy, gianluca.navone@unisi.it

Referee List (DOI 10.36253/fup_referee_list)
FUP Best Practice in Scholarly Publishing (DOI 10.36253/fup_best_practice)

Gianluca Navone, *Il risarcimento del danno da illecito trattamento dei dati personali,* © Author(s), CC BY-SA 4.0, DOI 10.36253/979-12-215-0796-6.11, in Chiara Angiolini, Antonello Iuliani (edited by), *Manuale sulla protezione e circolazione dei dati personali*, pp. 143-160, 2025, published by Firenze University Press and USiena PRESS, ISBN 979-12-215-0796-6, DOI 10.36253/979-12-215-0796-6

Ora, la circostanza che l'art. 82 GDPR detta una regola di 'vero e proprio' diritto privato europeo, calata dall'alto (a mo' di manto) da una fonte pervasiva qual è il regolamento, induce effetti sistemici degni di nota.

Innanzitutto, si registra un'importante ricaduta sul terreno dell'interpretazione. A tale proposito, infatti, una preziosa indicazione metodologica – una sorta di 'bussola ermeneutica' – si rinviene già nella prima pronuncia della Corte di giustizia sull'art. 82 (CGUE 4 maggio 2023, causa C-300/21). In particolare, là dove essa precisa che «i termini di una disposizione del diritto dell'Unione, la quale non contenga alcun rinvio espresso al diritto degli Stati membri al fine di determinare il suo significato e la sua portata, devono di norma dar luogo, in tutta l'Unione, ad un'interpretazione autonoma e uniforme». Ne consegue, quindi, che l'interprete è tenuto a confrontarsi direttamente con la norma sovranazionale, senza sentirsi vincolato da orientamenti giurisprudenziali e nozioni di diritto interno.

Diversamente opinando, pur muovendo dalla stessa linea di partenza (nella specie: la lettera dell'art. 82), i giudici dei singoli Stati membri verrebbero quasi inevitabilmente a tagliare traguardi differenti. All'unicità della disposizione scritta, finirebbe per corrispondere una pluralità di norme applicate; tante regole operative quante sono i Paesi dell'Unione. Con buona pace, s'intende, dell'uniformazione e delle sue finalità.

Nondimeno, occorre avvertirlo, ciò non significa che le soluzioni interpretative offerte dal diritto europeo non possano mai coincidere con quelle fornite dai singoli ordinamenti nazionali, ma che una verifica in questo senso si può fare soltanto *ex post*, ossia «a valle».

La natura regolamentare della regola di responsabilità sancita dall'art. 82 GDPR incide anche sul modo in cui si deve procedere all'integrazione del suo (lacunoso) dettato normativo.

L'intelligenza della questione ha bisogno di una premessa.

La disposizione in discorso realizza un'uniformazione soltanto parziale e non esaustiva: l'art. 82 tipizza una singola, specifica fattispecie di responsabilità, ma non disciplina l'intero istituto della responsabilità civile. Essa si presenta (passi l'immagine) come campata nel vuoto, è un *testo senza contesto*, giacché non investe tutti i possibili aspetti della responsabilità da illecito trattamento dei dati personali.

Anche qui, allora, si riscontrano i tratti tipici del diritto privato europeo, caratterizzato da incursioni normative puntiformi, il cui sviluppo procede «a spizzichi e bocconi», senza soverchie preoccupazioni d'ordine sistematico. Donde la necessità di rimediare all'endemico difetto di autosufficienza della regola scritta di fonte regolamentare e, quindi, accrescere la «densità» della disciplina continentale, senza remare contro gli obiettivi teleologici sottesi alla scelta di uno strumento giuridico di uniformazione.

Naturale domandarsi: ma come?

Ora, ad avviso di chi scrive, l'unico modo per rimediare al difetto di autosufficienza della fonte regolamentare è quello di sollecitare – per il medio del rinvio pregiudiziale – l'oramai riconosciuta opera *creatrice* ed *integratrice* della Corte di giustizia.

Le decisioni della Corte lussemburghese, per comune consenso munite di «autorità di cosa interpretata» *ultra partes*, sono le fonti di diritto complementare ideale per uno strumento legislativo di uniformazione, le sole idonee a disciplinare i profili trascutati dalla regola scritta (e a infittire la trama complessiva della normativa europea), senza innescare l'effetto «vestito di Arlecchino». In altri termini, i *dicta* resi in sede di rinvio pregiudiziale, vincolanti per tutti i giudici nazionali cui venga sottoposta un'analoga questione, introducono gocce di diritto uniforme che s'insinuano negli spazi lasciati vuoti dalla fonte regolamentare, colmandoli.

In altre parole, sia dai regolamenti sia dalla giurisprudenza della Corte di giustizia origina un diritto d'immediata applicazione, che sta sopra agli Stati membri dell'Unione. Un diritto «multicanale», ma non «multilivello», atteso che tanto le regole di fonte regolamentare quanto le decisioni della Corte di giustizia si collocano su un unico piano, quello del diritto uniforme europeo.

Apparentemente, una questione soltanto tecnica. Apparentemente. Perché in realtà la questione è anzitutto «politica». A ben riflettere, qui si gioca una partita decisiva sulla redistribuzione del potere; più nello specifico, sulla misura della partecipazione degli Stati membri al processo di creazione della normativa continentale; e, ancora più specificamente, sul ruolo dei singoli diritti nazionali quali fonte d'integrazione del diritto europeo uniforme.

Per concludere sul punto, si può dunque ben dire che l'adozione di uno strumento *self-executing*, quale il regolamento, non è affatto neutrale, ma corrisponde a una precisa scelta di accentramento della produzione giuridica. Da essa, infatti, consegue un avanzamento del diritto eurounitario e un arretramento – uguale e contrario – dei diritti nazionali. Le ragioni sono essenzialmente due: la prima è più evidente, la seconda meno. Anzitutto, l'impiego dello strumento regolamentare esclude in radice l'adozione di normative domestiche di recepimento. Ma non solo, l'obiettivo dell'uniformazione riduce al lumicino la rilevanza dei tre formanti (legislativo, giurisprudenziale e dottrinale) squisitamente nazionali.

2. La questione del «se»

Secondo il comune pensiero, alle regole sulla responsabilità civile si chiede di affrontare e risolvere tre questioni cruciali: la questione del «se», la questione del «chi», la questione del «quanto».

Ai fini della nostra particolare indagine, quindi, intorno al «se» il danno originato da un'attività di trattamento dei dati personali debba essere risarcito, al «chi» debba eventualmente risarcirlo e al «quanto» tale risarcimento ammonta, s'intende costruire la trattazione che verrà.

Interrogarsi sul «se» il danno subito da una persona fisica in conseguenza del trattamento di dati che la riguardano debba o no essere risarcito, equivale a chiedersi quale sia il criterio di selezione dei pregiudizi (materiali e/o immateriali) idonei ad attivare il rimedio risarcitorio.

In limine, si può allora rammentare che nell'ottica interna del diritto nazionale italiano tale «problema» viene correttamente affrontato adoperando il fil-

tro dell'ingiustizia del danno, sulla cui efficienza selettiva non può tuttavia fare affidamento l'interprete della disciplina continentale uniforme dettata dall'art. 82 del GDPR; giacché – come già si è osservato – l'applicazione di una regola di responsabilità posta in via diretta ed esclusiva dalla fonte europea di tipo regolamentare non è condizionabile alla ricorrenza dei presupposti di risarcibilità prescritti dall'art. 2043 del codice civile italiano o dalla previsione domestica di un altro Stato dell'Unione.

Tanto premesso, muoviamo dalla formula d'apertura della disposizione in esame per poi registrare le impressioni che subito suscitano le parole di cui si compone: «Chiunque subisca un danno [...] causato dalla violazione del presente regolamento ha il diritto di ottenere il risarcimento».

Balza evidente che il fuoco della previsione legale cade sull'espressione «violazione del presente regolamento». Cosicché, una spedita lettura dell'enunciato normativo induce a ritenere che il danno materiale o immateriale sia risarcibile se è eziologicamente riconducibile a un'attività di trattamento dei dati personali svolta in inosservanza del GDPR. La questione è tuttavia più complessa di quanto non risulti a un primo sguardo. Infatti, una disamina più approfondita di questo frammento di disposizione suscita almeno tre interrogativi interpretativi:

1) se la mera violazione di una prescrizione del GDPR sia (o no) sufficiente ad attribuire alla persona fisica cui i dati si riferiscono il diritto al risarcimento, oppure se sull'interessato grava l'onere di provare di aver subito un danno ulteriore, cioè una perdita di utilità materiali e/o immateriali conseguenti all'attività di trattamento;

2) se qualsiasi violazione del GDPR dà diritto di ottenere il risarcimento del danno conseguente all'attività di trattamento, o se sono idonee ad attivare il rimedio risarcitorio soltanto quelle violazioni che realizzano la lesione del diritto alla protezione dei dati personali dell'interessato;

3) se una «violazione del presente regolamento» rilevante sotto il profilo della responsabilità civile deve essere puntualmente provata, oppure solamente allegata da chi aziona il diritto al risarcimento del danno.

Sul primo dei tre quesiti la Corte di giustizia si è più volte pronunciata (CGUE 4 maggio 2023, C-300/21; 14 dicembre 2023, C-456/22; 25 gennaio 2024, C-687/21; 11 aprile 2024, C-741/21; 20 giugno 2024, C-590/22). L'orientamento, oramai consolidato, è il seguente: «l'articolo 82, paragrafo 1 del GDPR deve essere interpretato nel senso che la mera violazione delle disposizioni di tale regolamento non è sufficiente per conferire un diritto al risarcimento». Ergo, la semplice circostanza di porre in essere un'attività di trattamento in spregio di un precetto del regolamento europeo sulla protezione dei dati non comporta l'insorgere dell'obbligazione risarcitoria in favore dell'interessato ove quest'ultimo, in conseguenza di tale attività, non abbia subito una perdita di utilità.

Volendo adoperare un linguaggio familiare all'operatore del diritto italiano, si può dire che i *dicta* della Corte suonano come una repulsa della categoria del danno evento, consustanziale all'inosservanza delle regole dettate dal GDPR; nell'assunto che anche i pregiudizi extra-patrimoniali (diversi, cioè,

dalla ricchezza perduta e/o preclusa a seguito dell'illecito trattamento dei dati) devono essere specificatamente allegati e provati da chi ne domanda il ristoro. Donde ne discende, a mo' di corollario, che il c.d. «danno conseguenza» è da annoverarsi tra gli elementi costitutivi della fattispecie di responsabilità tipizza dall'art. 82 del GDPR.

Questa conclusione è sostenuta con due linee argomentative convergenti.

La prima di esse fa leva sulla formulazione letterale dell'art. 82 da cui «emerge […] che l'esistenza di un "danno" che sia stato "subito" costituisce una delle condizioni del diritto al risarcimento previsto da detta disposizione». D'altro canto, si aggiunge che la «menzione distinta di un "danno" e di una "violazione" […] sarebbe superflua se il legislatore dell'Unione avesse ritenuto che una violazione delle disposizioni del regolamento in parola possa essere sufficiente, da sola e in ogni caso, a dare fondamento a un diritto al risarcimento».

La seconda linea argomentativa ruota attorno alla diversità funzionale tra la tutela risarcitoria *ex* art. 82 e quella amministrativa *ex* artt. 83 e 84. Le due forme di tutela, rispettivamente di *private* e *public enforcement*, costituiscono un «incentivo a rispettare il GDPR [e] a scoraggiare la reiterazione di comportamenti illeciti». Tuttavia, mentre funzione eminente del risarcimento è quella di ristorare la vittima che abbia subito una perdita di utilità patrimoniali e/o extra-patrimoniali, la funzione essenziale delle sanzioni pecuniarie amministrative comminate dalle autorità di controllo nazionali (in Italia, il Garante per la protezione dei dati personali) è invece punitiva. Soltanto queste ultime, quindi, «non sono subordinate all'esistenza di un danno individuale».

Va semmai aggiunto che i giudici di Lussemburgo tendono a considerare assolto l'onere di provare l'esistenza del danno immateriale con una certa generosità. Come quando, in riferimento a un caso di diffusione non autorizzata di dati personali a seguito di un attacco hacker (c.d. *data breach*), hanno considerato sufficiente, a tal fine, la dimostrazione del mero «timore di un potenziale utilizzo abusivo dei dati da parte di terzi» (CGUE, 14 dicembre 2023, C-340/21); e, in un caso ancor più recentemente, quando hanno dichiarato che «il timore nutrito da una persona che i suoi dati personali […] siano stati divulgati a terzi, senza che si possa dimostrare che ciò sia effettivamente avvenuto, è sufficiente a dare fondamento a un diritto al risarcimento purché tale timore, con le sue conseguenze negative, sia debitamente provato» (CGUE, 20 giugno 2024, C-590/22).

Ciò posto, un ulteriore passo verso la negazione de facto della separazione fra violazione e danno è stato compiuto con la sentenza CGUE 4 ottobre 2024, C-200/23. In questa occasione, la Corte di giustizia si è spinta ad affermare che la perdita di controllo, anche temporanea, sui dati personali a seguito della loro indebita pubblicazione online (nello specifico, sull'equivalente bulgaro del nostro registro delle imprese) «può essere sufficiente a cagionare un "danno immateriale" […] senza che tale nozione di danno […] richieda la dimostrazione che sussistono ulteriori conseguenze negative tangibili». In altre parole, e a dispetto delle rassicuranti proclamazioni di fedeltà al principio di separazione tra violazione e danno, siamo qui al cospetto di una soluzione che strizza l'occhio (pur

senza maio nominarla) alla controversa categoria del danno in *re ipsa*. Infatti, affermare che la perdita di controllo dei dati costituisce, in sé e per sé, un danno immateriale significa abbracciare – forse senza troppa consapevolezza teorica – un modello di responsabilità civile in cui il danno non s'identifica più con la perdita di utilità, bensì con la lesione di una particolare situazione soggettiva: il diritto all'autodeterminazione informativa (da intendersi, a sua volta, come una particolare declinazione del più ampio diritto alla protezione dei dati personali).

Il secondo e il terzo degli interrogativi interpretativi sopra riportati, per la loro importanza, meriterebbero di formare oggetto di future domande di pronuncia pregiudiziale. Per entrambi, ad avviso di chi scrive, la *ratio legis* e l'interpretazione sistematica cospirano in senso antagonista rispetto a una lettura rigidamente letterale della disposizione.

Riguardo al secondo quesito (ossia se è vero o no che la violazione di una qualsiasi prescrizione del «presente regolamento» può far sorgere il diritto al risarcimento), infatti, è di tutta evidenza che l'art. 82 proclama risarcibile il danno conseguente a un'attività di trattamento svolta in spregio alle regole del GDPR, senza fare alcun riferimento testuale alla necessaria lesione di una situazione giuridica soggettiva, qual è – per l'appunto – il diritto alla protezione dei dati personali. Tanto da indurre a pensare, *prima facie*, di trovarsi al cospetto di una fattispecie di responsabilità civile senza filtri, in 'presa diretta' cioè con la trasgressione di una prescrizione (quale che sia) del regolamento europeo. A rifletterci, tuttavia, è ragionevole dubitare che la benché minima imprecisione, la più piccola irregolarità formale o procedurale possa essere davvero sufficiente a giustificare la pretesa risarcitoria dell'interessato.

A tale proposito, si può anzitutto osservare che nel sistema europeo l'intera disciplina è edificata a presidio di una particolare situazione giuridica soggettiva. Il GDPR, si legge eloquentemente nell'intitolazione, è il «Regolamento […] relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali».

Ancora oltre, sempre nella stessa direzione, sospinge la constatazione che nel GDPR esistono regole organizzative o meramente procedurali la cui inosservanza non è idonea a ledere alcuna situazione soggettiva dell'interessato. Si pensi, per limitarci a qualche esempio, alla mancata designazione del responsabile della protezione dei dati nei casi in cui essa è obbligatoria (art. 37); all'omessa o incompleta tenuta del registro delle attività di trattamento (art. 30); all'assenza di un accordo interno tra contitolari del trattamento (art. 26). Tutte infrazioni atte a giustificare l'irrogazione di una sanzione pecuniaria amministrativa, ma non sufficienti a rendere illeciti – di per sé solo – ogni trattamento eseguito dal titolare che abbia commesso tali violazioni.

Per concludere sul punto, l'art. 82, par. 1, del GDPR deve allora essere interpretato nel senso che sono idonee ad attivare il rimedio risarcitorio soltanto quelle violazioni che realizzano la lesione del diritto alla protezione dei dati personali.

Come già anticipato, il terzo e ultimo dei nostri interrogativi può essere sintetizzato nella domanda se l'esistenza di una violazione del regolamento europeo (rilevante ai fini della responsabilità civile) debba o non debba essere provata da chi aspira al risarcimento del danno materiale e/o immateriale.

Orbene, la considerazione isolata della disposizione in esame instrada verso una piana risposta affermativa. A tutta prima, l'antigiuridicità – identificabile nel contrasto tra il fatto causativo del danno (trattamento dei dati) e i dettami «del presente regolamento» – appare come un elemento che integra in positivo la fattispecie di responsabilità tipizzata dall'art. 82 del GDPR. In quanto elemento costitutivo, quindi, l'antigiuridicità dovrebbe essere provata dall'interessato che avanza la pretesa risarcitoria. Senonché, la lettura congiunta degli artt. 82 e 24 orienta verso una diversa conclusione.

Valga, in proposito, rilevare che la pietra d'angolo su cui poggia tutta la disciplina eurounitaria è costituita dal principio di *accountability* il quale – *inter alia* – onera il titolare a «dimostrare che il trattamento è effettuato conformemente al presente regolamento».

In limpida coerenza con il principio di *accountability*, è allora persuasivo sostenere che non sia l'antigiuridicità elemento costitutivo della fattispecie di responsabilità in parola, ma piuttosto la non antigiuridicità (dovuta, ad esempio, alla presenza di un'idonea «base giuridica» e al rispetto dei «principi» di cui all'art. 5 GDPR) a essere elemento impeditivo dell'insorgere della responsabilità civile in capo al titolare del trattamento.

Donde, l'art. 82, par. 1, del GDPR va interpretato nel senso che una «violazione del presente regolamento» dev'essere solamente allegata – non anche provata – da chi aziona il diritto al risarcimento.

In conclusione: il «chiunque» (persona fisica) che agisce in giudizio per ottenere il ristoro del danno materiale e/o immateriale *ex* art. 82 ha solo l'onere di provare l'esistenza di un'attività di trattamento – riferibile al candidato responsabile – avente a oggetto dati personali che lo riguardano, una perdita di utilità patrimoniali e/o extra-patrimoniali (*id est*: il danno), e il nesso di causalità tra l'attività di trattamento e la perdita di utilità, limitandosi invece alla mera allegazione di una violazione del regolamento europeo idonea a ledere il diritto alla protezione dei dati personali.

3. *Segue*. Il «se» del danno immateriale non è subordinato al raggiungimento di una certa soglia di gravità.

In risposta a una pluralità di domande pregiudiziali, la Corte di giustizia si è pronunciata sul seguente interrogativo: se, ai sensi dell'art. 82 GDPR, l'*an debeatur* del danno immateriale possa essere subordinato al raggiungimento di una soglia minima di gravità (CGUE, 4 maggio 2023, C-300/21; CGUE, 14 dicembre 2023, C-456/22; CGUE, 20 giugno 2024, C-590/22).

Alla vigilia di tali pronunciamenti, l'art. 82 si presentava – passi l'immagine – come una casa semivuota, quasi tutta d'arredare secondo il gusto, se non addirittura l'arbitrio, dei giudici di Lussemburgo. A costoro è stato affidato il compito d'infittire le maglie della disciplina continentale, di accrescerne la «densità», senza poter contare sul conforto di una definizione legale di «danno» (e ancor meno di «danno immateriale»), né sulla guida di una pregressa giurisprudenza a riguardo.

Tanto considerato, il risultato dell'opera creatrice/integratrice della Corte UE è stato il seguente: l'art. 82, par. 1, del GDPR deve essere interpretato nel senso che il risarcimento del danno immateriale non è subordinato «alla condizione che il danno subito dall'interessato abbia raggiunto un certo grado di gravità».

Nessuna franchigia risarcitoria, quindi, è compatibile con l'autonoma categoria eurounitaria del danno immateriale, fermo restando che questa apertura al ristoro di disutilità non patrimoniali minime non significa che «una persona [...] che abbia subito conseguenze negative» a seguito di un illecito trattamento dei propri dati «sia dispensata dal dimostrare che tali conseguenze costituiscono un danno immateriale, ai sensi dell'art. 82»; occorre comunque dimostrare «di aver effettivamente subito tale danno, per quanto minimo».

A tale approdo si giunge adducendo ad argomento *princeps* il rilievo che «l'articolo 82 [...] si limita ad enunciare in modo esplicito che può dare diritto a un risarcimento non solo un "danno materiale", ma anche un "danno immateriale", senza che venga menzionata una qualsivoglia soglia di gravità». Dietro queste parole, è difficile non scorgere l'impiego di una classica tecnica di costruzione di norme inespresse. Più precisamente, della tecnica dell'argomento *a contrario* in funzione costruttiva. Nella specie, infatti, si assume che il legislatore europeo ha detto esattamente ciò che intendeva dire (*ubi lex voluit dixit, ubi tacuit noluit*), sicché ciò che non ha detto, evidentemente, non intendeva dirlo, giacché, se avesse voluto dirlo, l'avrebbe detto.

A puntello di tale ragionamento, la Corte aggiunge un argomento di natura teleologica. L'interpretazione secondo cui «il diritto al risarcimento non è subordinato al fatto che il danno di cui trattasi raggiunga una certa soglia di gravità» è in linea con quanto indicato nel centoquarantaseiesimo «considerando» del GDPR che invita a interpretare il «concetto di danno [...] in senso lato [e] in modo [...] da rispecchiare pienamente gli obiettivi del presente regolamento»; mentre «tale concezione ampia della nozione di "danno", privilegiata dal legislatore dell'Unione, sarebbe contraddetta se detta nozione fosse circoscritta ai danni di una certa gravità», così come «subordinare il risarcimento di un danno immateriale a una certa soglia di gravità rischierebbe di nuocere alla coerenza del regime istituito dal GDPR, poiché la gradazione di siffatta soglia, da cui dipenderebbe la possibilità o meno di ottenere detto risarcimento, potrebbe variare in funzione della valutazione dei giudici aditi».

Ora, al di là della persuasività di queste contorsioni verbali, balza evidente la preoccupazione di accreditare l'opzione interpretativa reputata più idonea ad assicurare l'uniforme applicazione dell'art. 82 all'interno dell'Unione. Ma vi è di più, questo modo di leggere la previsione regolamentare amplia l'operatività delle tecniche di tutela collettiva, poiché consente di coagulare tante piccole pretese risarcitorie omogenee; bagatellari se le si considera singolarmente, ma (non di rado) d'ingente valore economico se si ha riguardo alla loro somma.

In questa sede, tuttavia, quel che più interessa sottolineare è la coesistenza attuale di un duplice statuto normativo del danno extra-patrimoniale: da un lato, quello del *danno immateriale*, disciplinato in via esclusiva dal formante legislativo europeo di fonte regolamentare, così come interpretato/integrato dalla

Corte di giustizia; dall'altro lato, quello domestico del *danno non patrimoniale* al quale – almeno in Italia – continua ad applicarsi il doppio filtro della «gravità della lesione» della situazione giuridica protetta e della «serietà del pregiudizio» patito dalla vittima in conseguenza di tale lesione. Di talché, l'espressione «danno immateriale», sebbene sia il frutto di una traduzione (persino troppo) letterale della locuzione inglese *non-material damage*, si sta comunque rivelando utile. Col senno di poi, possiamo considerarla come il prodotto di una *felix culpa* del traduttore, in quanto vale a rendere d'immediata percezione la matrice squisitamente europea di tale tipologia di danno e a segnalarne l'autonomia.

Segni eloquenti di una crescente consapevolezza della specificità del danno immateriale si rinvengono nelle primissime decisioni dei giudici nazionali in argomento. A cominciare dalla prima pronuncia sull'art. 82 della nostra Corte di Cassazione. Quest'ultima, nel confermare la sentenza di merito (con cui era stato condannato al risarcimento del danno immateriale un Comune il quale – per sole 24 ore – aveva indebitamente pubblicato sul proprio sito istituzionale i dati identificativi di una lavoratrice che aveva subito il pignoramento del quinto dello stipendio), ha significativamente affermato che «il soggetto danneggiato a seguito di un trattamento dei suoi dati in violazione delle norme del GDPR [...] può ottenere il risarcimento di qualunque danno occorsogli, *anche se la lesione sia marginale*» (Cass. ord., 15 maggio 2023, n. 13073).

Analogamente, sempre ai sensi dell'art. 82, un Tribunale tedesco ha recentemente liquidato la cifra simbolica di venticinque euro a chi aveva ricevuto due *mail* pubblicitarie indesiderate (Tribunale regionale di Heidelberg il 16 marzo 2022, LG Heidelberg – 4S 1/21).

Nell'accordare questo modesto risarcimento, il Tribunale ha quindi tenuto conto di alcune piccolissime 'disutilità' extra-patrimoniali consistenti nel tempo sprecato a occuparsi delle *mail* indesiderate, individuare il loro mittente, redigere e inviare una comunicazione scritta per chiedere la cancellazione dei dati, rimuovere i messaggi dalla casella di posta elettronica. Per inciso, una particolare sottolineatura merita la circostanza che la decisione sia stata assunta da un giudice tedesco. Anche in Germania, così come in Austria e Italia, si era infatti consolidata la contrapposta regola giurisprudenziale dell'irrilevanza ai fini risarcitori dei danni non patrimoniali di minima entità.

Tutto ciò detto, rimane da chiedersi se questa convivenza tra differenti statuti normativi (quello squisitamente europeo del danno immateriale da illecito trattamento dei dati personali e quelli nazionali degli altri danni non patrimoniali) sia davvero priva di punti d'attrito e di possibilità di contagio.

Infatti, è lecito dubitare che l'anzidetto passaggio «dal danno non patrimoniale ai danni non patrimoniali» possa passare indenne al vaglio dei giudici delle leggi dei vari Paesi UE. A riguardo, con specifico riferimento alla situazione italiana, si è già utilmente rilevato che un sistema del danno non patrimoniale calibrato su due velocità, con la sottoclasse del danno immateriale *ex* art. 82 GDPR, che fa da sé, giustapposta alla categoria domestica del danno non patrimoniale *ex* art. 2059 c.c. nel quale il superamento di soglia minima di gravità continua invece a essere richiesta, finirà per alimentare le voci propense a denunziare

un'illegittimità costituzionale derivante da una disparità di trattamento patita dagli altri diritti fondamentali di rilevanza costituzionale.

È ben possibile, tuttavia, che le predette questioni d'illegittimità siano prevenute dai giudici nazionali, allineando l'interpretazione delle norme interne ai canoni ermeneutici dettati dalla Corte di Lussemburgo per l'art. 82. E, se così sarà, la specie del danno immateriale produrrà una sorta di *coattail effect*, un effetto di trascinamento di grandissimo rilievo: l'uniformazione europea «dal basso», cioè in via giurisprudenziale, dell'intero genere del danno non patrimoniale.

4. La questione del «chi»

La questione del «chi» si apre sul presupposto che a quella sul «se» sia stata data una risposta affermativa. Quindi, una volta appurato che il danno è risarcibile, occorre procedere all'individuazione del soggetto obbligato al risarcimento. A tale fondamentale funzione provvedono le regole sui criteri di imputazione/attribuzione della responsabilità. A esse, infatti, è commesso il compito d'identificare la ragione per cui il costo di un danno deve essere posto a carico di un soggetto diverso da colui (la vittima) che storicamente lo ha subito.

Con specifico riferimento al tema che ci occupa, è da osservare che, nella fattispecie di responsabilità delineata dall'art. 82, il criterio d'imputazione dell'obbligo risarcitorio è incentrato sulla particolare natura dell'attività esercitata dal presunto responsabile. Nei suoi elementi costitutivi, tale fattispecie ricollega l'attribuzione della responsabilità al fatto oggettivo dello svolgimento di un'attività qualificabile – ai sensi dell'art. 4, n. 2 del GDPR – come «trattamento»: vale a dire, «qualsiasi operazione o insieme di operazioni […] applicate a 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».

Con una precisazione, dal momento che il regolamento europeo «non si applica ai trattamenti di dati personali […] effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico» (art. 2, par. 2, lett. *c* del GDPR), sono esclusi dall'arco di applicazione dell'art. 82 i danni conseguenti a trattamenti eseguiti – volendo riproporre le stesse parole impiegate nel diciottesimo «considerando» – «senza una connessione con un'attività commerciale o professionale».

Ne viene, pertanto, che, nell'economia dell'art. 82, il coinvolgimento in un'operazione di trattamento di dati personali svolta nel quadro di attività *lato sensu* professionali costituisce ragione sufficiente, indipendentemente dalla colpa del candidato responsabile, per l'imputazione della responsabilità.

Siamo qui al cospetto di una fattispecie di responsabilità presunta (più che «di responsabilità per colpa accompagnata da un'inversione dell'onere della prova», come impropriamente sostenuto dalla Corte di giustizia nella sentenza 21 dicembre 2023, causa C-667/21), caratterizzata dalla previa canalizzazione

dell'obbligazione risarcitoria verso soggetti predeterminati, ossia coloro ai quali risulta riferibile l'attività di trattamento dei dati che ha costituito il fattore causale del «danno conseguenza».

Si vuol quindi ripetere che tra i fatti costitutivi, quelli che condizionano il sorgere dell'effetto risarcitorio, la previsione dell'art. 82 non contempla il criterio d'imputazione soggettivo della colpa, ma attribuisce la responsabilità in relazione al fatto oggettivo dello svolgimento di una peculiare attività.

Merita considerare, tuttavia, chi esercita professionalmente un'attività di trattamento dei dati personali non è affatto privo di possibilità di difesa. Infatti, trattandosi di una presunzione relativa di responsabilità, il terzo paragrafo della disposizione in esame stabilisce che «Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità [...] se dimostra che l'evento dannoso non gli è in alcun modo imputabile».

Senonché, né il tenore letterale della formula impiegata dal legislatore europeo, né il «considerando» (il centoquarantaseiesimo) che a essa fa fugacemente riferimento, offrono sufficienti indicazioni riguardo al contenuto della prova liberatoria. Ampio, perciò, è il ventaglio delle soluzioni interpretative possibili.

Così, ad esempio, lo si potrebbe intendere in senso restrittivo, assumendo che la prova dell'*evento dannoso in alcun modo imputabile* coincide con quella del caso fortuito che – nella sua accezione oggettiva – si riferisce a circostanze esterne al (presunto) destinatario dell'imputazione, tali da escludere in radice la rilevanza di qualsiasi giudizio valutativo della condotta dell'agente in chiave di assenza di colpa. Tuttavia, la centralità che il principio di *accountability* riveste nell'architettura normativa complessiva del GDPR e – come si vedrà tra breve – la giurisprudenza della Corte di giustizia non orientano in questa direzione.

Diversamente, a noi sembra più convincente ritenere che il contenuto privilegiato della prova liberatoria concessa al presunto responsabile consista nella dimostrazione dell'insussistenza della violazione del regolamento europeo (idonea a integrare la lesione del diritto alla protezione dei dati personali) allegata – ma non provata – dalla controparte.

In altri termini, è la non antigiuridicità a essere elemento impeditivo dell'insorgere dell'obbligazione risarcitoria in capo al titolare e/o al responsabile del trattamento.

Più in generale, qui vale la pena di ricordare che il trattamento di dati personali altrui è lecito/non antigiuridico se ricorrono due condizioni: 1) l'attività di trattamento deve poggiare su una delle «basi giuridiche» indicate all'articolo 6 cui si aggiunge l'applicazione dell'art. 9 GDPR per le categorie particolari di dati personali (v. cap. *La disciplina dell'attività di trattamento*, sez. I); 2) deve svolgersi, altresì, nel rispetto dei principi sanciti all'art. 5 del GDPR (trasparenza, limitazione delle finalità e dei tempi di conservazione, minimizzazione, integrità, e così via enumerando). Il giudizio sulla liceità del trattamento si configura quindi come una valutazione complessa, scandita da due momenti successivi: è necessario che sussista almeno una base giuridica; e che, ciò appurato, l'operazione di trattamento sia svolta in conformità dei «principi applicabili al trattamento dei dati personali».

La presenza di una valida base giuridica non garantisce, di per sé sola, la liceità del trattamento. Si pensi, in via esemplificativa, al caso di un Comune che, in esecuzione di un preciso obbligo legale (nella specie, quello prescritto dall'art. 15 del d. lgs. n. 33 del 2013), pubblichi nell'apposita sezione del proprio sito istituzionale il *curriculum* del titolare di un incarico di consulenza. Ebbene, tale trattamento, pur poggiando su una solida base giuridica (vd. art. 6, par. 1, lett. *c* del GDPR), sarebbe comunque illecito se il documento diffuso online contenesse informazioni personali eccedenti rispetto alle finalità di trasparenza amministrativa, in spregio del principio di «minimizzazione dei dati» (ai sensi art. 5, par. 1, lett. *c* del GDPR).

Quindi, per restare all'esempio delineato, il consulente che voglia agire per il risarcimento del danno materiale e/o immateriale *ex* art. 82 GDPR avrà l'onere di provare l'avvenuta pubblicazione del proprio *curriculum* nella sezione «Amministrazione trasparente» del sito web dell'ente convenuto, di aver subito una perdita di utilità patrimoniali e/o extrapatrimoniali e il nesso di causalità tra la pubblicazione e la perdita di utilità, mentre dovrà solo allegare la violazione del principio di minimizzazione. Il Comune, invece, per andare esente da responsabilità, dovrà dimostrare che i dati personali divulgati sono «adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati». Mentre, ove non gli riuscisse di fornire siffatta dimostrazione, resterà obbligato al risarcimento in ragione della presunzione *iuris tantum* di responsabilità.

Riguardo al contenuto della prova liberatoria, è da sottolineare che a essa non è estranea una valutazione del comportamento tenuto dal presunto responsabile. Difatti, se la «violazione del presente regolamento» integra gli estremi della colpa specifica in termini d'inosservanza di discipline, la prova della conformità del trattamento alle regole che vi presiedono (*id est*: della «non antigiuridicità») si sostanzia nella dimostrazione dell'assenza di colpa.

L'esattezza di questa conclusione emerge con particolare nitore nelle ipotesi in cui l'interessato lamenta di aver subito un danno a seguito di una violazione di dati personali (c.d. *data breach*), ossia un incidente di sicurezza «che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati» (art. 4, n. 12 GDPR). Ipotesi, queste, in cui la responsabilità civile da illecito trattamento s'intreccia in maniera vistosa con il principio di *accountability*.

Ma procediamo con ordine e cominciamo col dire che tra i «principi» enunciati all'art. 5 GDPR spicca, per importanza, quello di «integrità e riservatezza» che impone di trattare i dati personali «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» (§ 1, lett. *f*) (v. cap. La disciplina dell'attività di trattamento, sez. II). Non solo, in più luoghi del regolamento europeo si aggiunge che l'esercente attività di trattamento deve essere in grado di dimostrare di aver adottato misure di sicurezza adeguate a garantire un elevato livello di protezione dei diritti delle persone fisiche cui i dati si riferiscono,

tenendo conto dello stato dell'arte, dei costi di attuazione delle predette misure, della natura dei dati, delle finalità del trattamento, nonché dei rischi e dei danni potenziali (cfr. artt. 5, par. 2, 24, par. 1, 25 e 32 del GDPR). In essenza, quindi, l'*accountability* (espressione che con molte difficoltà e qualche insoddisfazione è stata tradotta in italiano con il sostantivo «responsabilizzazione») si riduce al duplice obbligo di *adottare misure di sicurezza adeguate* e di *provare di averle adottate*.

Sicché, nell'evenienza di un attacco hacker – incidente di sicurezza per eccellenza – alla persona fisica dell'interessato spetterà dimostrare (ad esempio) che la propria cartella clinica è stata divulgata da pirati informatici e di aver subito un danno in conseguenza di tale divulgazione, mentre dovrà limitarsi ad allegare che il presunto responsabile ha violato il principio di «integrità e riservatezza». Il convenuto, invece, per liberarsi dalla responsabilità, avrà l'onere di provare di aver adottato misure tecniche e organizzative adeguate.

A questo proposito, la Corte di giustizia ha ulteriormente precisato che «una divulgazione non autorizzata di dati personali o un accesso non autorizzato a tali dati da parte di "terzi" […] non sono sufficienti, di per sé, per ritenere che le misure tecniche e organizzative attuate dal titolare del trattamento in questione non fossero "adeguate"», «senza neppure consentire a quest'ultimo di fornire prova contraria»; e che «l'adeguatezza delle misure […] attuate dal titolare del trattamento […] deve essere valutata dai giudici nazionali in concreto, tenendo conto dei rischi connessi al trattamento di cui trattasi e valutando se la natura, il contenuto e l'attuazione di tali misure siano adeguate a tali rischi» (sentenza 14 dicembre 2023, causa C-340/21).

Tanto vale a dire che l'adeguatezza delle misure adottate è da accertarsi mediante una valutazione *ex ante*, riferita al momento precedente all'incidente di sicurezza, anteriore cioè a quello in cui – per usare un'espressione invalsa nel gergo degli informatici – «i buoi sono scappati dalla stalla». Tale valutazione, inoltre, deve essere operata tenendo conto dei diversi criteri di giudizio dettati dall'art. 32 par. 1 GDPR: stato dell'arte della tecnologia, costi di attuazione, natura dei dati, finalità del trattamento ed entità del rischio. Cosicché, sempre nell'ipotesi di divulgazione non autorizzata di documentazione sanitaria a opera di pirati informatici, le stesse misure tecniche e organizzative potrebbero essere considerate adeguate se il titolare del trattamento è un medico di base e, al contempo, inadeguate se a rivestire la qualità giuridica di titolare è una grande azienda ospedaliera.

In ogni caso, anche per la Corte di giustizia, può dirsi acquisito che «nell'ambito di un'azione di risarcimento fondata sull'art. 82 […], al titolare del trattamento di cui trattasi incombe l'onere di dimostrare l'adeguatezza delle misure di sicurezza da esso attuate».

Va semmai soggiunto che il contenuto della prova liberatoria è sensibilmente più ampio per chi, in forza di un titolo formale di designazione (contratto o altro atto giuridico scritto *ex* art. 28, par. 9 GDPR), dimostra di aver agito in qualità di responsabile del trattamento. Infatti, «la persona fisica o giuridica […] che tratta dati per conto del titolare del trattamento» (art. 4, n. 9 GDPR) va esente

da responsabilità se prova che la violazione del regolamento europeo contestatagli dall'interessato si riferisce a un obbligo che incombe esclusivamente sul titolare; come quello, per esempio, di astenersi dall'eseguire un'attività di trattamento in difetto di un'idonea base giuridica.

A nostro avviso, questo è il senso dell'involuta locuzione normativa secondo la quale il «responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto agli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento» (art. 82, par. 2 GDPR).

In chiusa di paragrafo, traendo le fila da quanto sin qui osservato, pare di poter dire che l'art. 82 configura una fattispecie di responsabilità presunta, nella quale l'obbligazione risarcitoria è imputata oggettivamente, in considerazione della peculiare natura dell'attività esercitata dal titolare e/o dal responsabile del trattamento. Diversamente, la prova liberatoria, implicando una valutazione del comportamento assunto dal presunto responsabile (circa l'insussistenza della violazione del regolamento europeo allegata dalla controparte), si risolve nella dimostrazione dell'assenza di colpa. Sicché, facendo tesoro dell'insegnamento della dottrina che più e meglio ha studiato la materia delle responsabilità presunte, la fattispecie in esame si colloca «nell'ambito di un sistema intermedio o di un *tertium genus* fra il sistema della responsabilità soggettiva e quello di responsabilità oggettiva», tenendosi appunto conto che tale fattispecie nel fatto costitutivo prescinde dal criterio d'imputazione della colpa, prevede il fatto impeditivo dell'assenza di colpa come prova liberatoria e attribuisce il rischio della mancata prova del fatto impeditivo al soggetto presunto responsabile (Comporti, 2000).

5. La questione del «quanto»

Tra i nostri giuristi è diffusa la constatazione che, nel momento attuale, il problema più annoso della responsabilità civile sia quello della liquidazione del danno.

Questo vale per il danno per il danno in generale, sia patrimoniale sia non patrimoniale («materiale» e «immateriale» nel lessico eurounitario dell'art. 82 GDPR); ma è vieppiù accentuato per quello non patrimoniale che – tradotto in essenza – si sostanzia nella perdita di utilità areddituali, alle quali, in un determinato momento storico, non è possibile accedere attraverso la mediazione del denaro; o, in altre parole, nell'ammanco di utilità non conseguibili mediante l'acquisto di beni o di servizi offerti sul mercato e che, quindi, molto in sintesi (e con un certo margine d'ineliminabile approssimazione), «non si possono comprare».

Il risarcimento del danno patrimoniale presuppone, per la vittima che lo subisce, una perdita economica; il risarcimento del danno non patrimoniale, invece, vi prescinde completamente.

Da questa semplice constatazione discende che il rimedio risarcitorio svolge per l'uno e per l'altro funzioni necessariamente diverse.

Più in dettaglio, il risarcimento del danno patrimoniale svolge una funzione eminentemente «compensativa»: mira alla reintegrazione della ricchezza per-

duta e/o preclusa a seguito del fatto illecito attraverso l'azzeramento del saldo negativo che si è venuto a creare nel patrimonio della vittima in conseguenza del fatto illecito, ma – si aggiunge – senza «esuberi». Per cui s'insegna, tradizionalmente, che il suo ammontare è uguale al delta tra due termini monetari. Alla differenza aritmetica, cioè, tra il valore che il patrimonio del danneggiato avrebbe avuto qualora l'illecito non si fosse verificato (minuendo) e quello suo effettivo a seguito del verificarsi dell'illecito (sottraendo). E, così facendo, si dà attuazione al principio della *riparazione integrale*: il *quantum* del risarcimento deve corrispondere all'entità della perdita economica subita, nulla di più e nulla di meno.

Diversamente è a dirsi, invece, per il risarcimento del danno non patrimoniale che – si vuol ripetere – prescinde dall'esistenza di un'alterazione *in peius* del patrimonio della vittima; per cui, non venendo qui in questione la reintegrazione di un *damnum emergens* e/o di un *lucrum cessans*, la sua funzione appare ontologicamente incompatibile con quella di compensare ammanchi di ricchezza verificatisi a seguito dell'illecito.

La corresponsione di una somma di denaro a titolo di ristoro del danno non patrimoniale svolge quindi, sempre e di necessità, un'altra prioritaria funzione. Più precisamente, una funzione «satisfattiva». Suo tramite, infatti, si tende a confortare la vittima procurandole utilità economiche sostitutive di utilità areddituali oramai irrimediabilmente perdute, perché non recuperabili sul mercato.

In diverse parole, si «consola» la vittima arricchendola in termini monetari (esito normalmente precluso, come si è già osservato, alle regole che governano il risarcimento del danno patrimoniale), ma senza pretesa di realizzare un'illusoria equivalenza tra le sofferenze patite e le soddisfazioni che il denaro può arrecare. A fronte di «disutilità» non patrimoniali, questo è quello che finora il diritto civile è riuscito a fare: attribuire una somma di denaro che non pretende di cancellare il dolore né di essergli equivalente.

Ne discende come corollario che il risarcimento del danno non patrimoniale (a cui è del tutto estranea la funzione di compensazione di una perdita economica) non può essere governato dal principio della «riparazione integrale».

Tanto acquisito, torniamo al nostro tema, quello della liquidazione dei pregiudizi materiali e/o immateriali conseguenti a un trattamento di dati personali di cui l'interessato allega l'illiceità.

A riguardo, la prima delle decisioni rese dalla Corte di giustizia sull'art. 82 GDPR (4 maggio 2023, C-300/21) si è pronunciata sulla seguente questione pregiudiziale: se la disposizione in parola debba essere interpretata «nel senso che, ai fini della determinazione dell'importo del risarcimento dovuto in base al diritto al risarcimento sancito in tale articolo, i giudici nazionali devono applicare le norme interne di ciascuno Stato membro relative all'entità del risarcimento pecuniario».

Ad avviso di chi scrive, la 'bussola' dell'autonomia del diritto europeo di fonte regolamentare e la considerazione degli obiettivi teleologici sottesi alla scelta di uno strumento giuridico di uniformazione avrebbero dovuto orientare la Corte verso una sicura risposta negativa. Infatti, posto che l'art. 82 non contiene indicazioni riguardo alla stima del danno immateriale, né, su questo

specifico aspetto, rinvia espressamente al diritto degli Stati membri, il conseguente vuoto di disciplina avrebbe dovuto essere colmato attraverso l'innesto creativo/integrativo della Corte di giustizia: i *dicta* resi in sede di rinvio pregiudiziale, vincolanti per tutti i giudici nazionali cui venga sottoposta un'analoga questione, sono i soli idonei a rimediare al difetto di autosufficienza del formante legislativo europeo, senza innescare l'effetto 'vestito di Arlecchino', ossia un esito di frammentazione regolatoria opposto all'obiettivo dell'uniformazione.

Diversamente (e sorprendentemente), i giudici di Lussemburgo hanno risposto al quesito in discorso così: «l'articolo 82 del GDPR deve essere interpretato nel senso che, ai fini della determinazione dell'importo del risarcimento dovuto in base al diritto al risarcimento sancito da tale articolo, i giudici nazionali devono applicare le norme interne di ciascuno Stato membro relative all'entità del risarcimento pecuniario, purché siano rispettati i principi di equivalenza e di effettività del diritto dell'Unione».

Nel tentativo di puntellare questa conclusione, la motivazione chiama a supporto il principio di *autonomia processuale*, secondo il quale «in mancanza di norme dell'Unione in materia, spetta all'ordinamento giuridico interno di ciascuno Stato membro stabilire le modalità procedurali dei ricorsi giurisdizionali». Principio implicitamente richiamato dallo stesso art. 82 che, al sesto e ultimo paragrafo, rinvia al «diritto dello Stato membro» per quanto attiene all'individuazione dell'autorità giurisdizionale competente a conoscere della domanda risarcitoria e, più in generale, riguardo alle regole di carattere processuale.

Senonché, è agevole osservare che il principio di autonomia processuale è qui richiamato dalla Corte UE del tutto a sproposito, poiché nulla c'entra con le regole che presiedono alla quantificazione dell'obbligazione risarcitoria. La liquidazione monetaria del danno è una questione spinosa, scivolosa come una lastra di ghiaccio, sì, ma di diritto sostanziale.

Tra parentesi, se all'errore appena denunciato sarà data acriticamente continuità, l'effetto sarà quello di escludere indebitamente una fase centrale del giudizio di responsabilità, quella che attiene alla determinazione del *quantum debeautur*, dal processo di costruzione del diritto comune europeo della responsabilità civile.

Ad ogni modo, dopo la sentenza 'apripista', altre decisioni hanno riguardato il profilo della commisurazione del danno (CGUE, 21 dicembre 2023 C-667/21; CGUE, 25 gennaio 2024, C-687/21; CGUE, 11 aprile 2024, C-741/21; CGUE, 20 giugno 2024, C-182/22 e C-189/22). Queste sentenze, pur non rinnegando la soluzione sovranistica propugnata dalla *Österreichische Post AG*, si sono comunque sforzate di delineare regole uniformi per la liquidazione. Là dove, in particolare, esse impongono a tutti i giudici dell'Unione di interpretare l'art. 82 GDPR nel senso che «il diritto al risarcimento previsto da tale disposizione svolge una *funzione esclusivamente compensativa*, in quanto il risarcimento pecuniario fondato su detta disposizione deve consentire di *compensare integralmente il danno* concretamente subito [...], e *non una funzione punitiva*». Aggiungendo, in linea di coerenza con questa affermazione di principio, che ai fini della commisurazione dell'entità della prestazione risarcitoria non devono essere presi in consi-

derazione elementi che prescindono dalla dimensione della perdita economica effettivamente determinatasi nella sfera giuridica della persona fisica cui i dati si riferiscono. Quali, invece, sarebbero quelli che attengono al grado di riprovevolezza della condotta assunta dal danneggiante: «il livello di gravità della violazione del regolamento» commessa dal titolare o dal responsabile del trattamento, l'intensità della loro colpa o «l'eventuale carattere doloso della violazione».

Nella medesima lunghezza d'onda si colloca l'ulteriore precisazione dei giudici di Lussemburgo secondo cui «per determinare l'importo dovuto a titolo di risarcimento [...] non si devono applicare *mutatis mutandis* i criteri di fissazione dell'importo delle sanzioni amministrative pecuniarie previsti dall'art. 83» del GDPR. Infatti, per espressa previsione del legislatore europeo, «le sanzioni amministrative *inflitte*» ai sensi della suddetta disposizione devono essere «*dissuasive*», cioè svolgere una funzione punitivo/deterrente. Tant'è che ai fini della fissazione del loro ammontare le autorità nazionali di controllo devono tener conto – tra l'altro – della «gravità [...] della violazione», del «carattere doloso o colposo della violazione», del «grado di responsabilità del titolare del trattamento o del responsabile del trattamento», di «precedenti violazioni», nonché di «eventuali [...] benefici finanziari conseguiti o le perdite evitate, indirettamente o indirettamente, quale conseguenza della violazione».

A nostro avviso il ragionamento svolto dalla Corte di giustizia è parzialmente emendabile, nella misura in cui esso pretende di valere, indistintamente, sia per il danno materiale/patrimoniale sia per quello immateriale/non patrimoniale.

Ora, questo modo di argomentare – che spesso si rinviene anche nelle motivazioni della Cassazione italiana – sconta un'evidente difficoltà culturale, che deriva anzitutto dall'insufficiente comprensione dell'ontologica diversità funzionale tra le due tipologie di danno. Infatti, come già sopra si è detto, al risarcimento del danno extra-patrimoniale è del tutto estranea la funzione di compensazione. Esso, pertanto, non può essere governato dal principio della «riparazione integrale».

Cadono acconce, a riguardo, le parole di una delle voci più autorevoli della nostra dottrina specialistica secondo cui il «principio del risarcimento integrale ha un preciso significato giuridico per il danno patrimoniale, dove [...] esprime [...] la regola per la quale la somma dovuta a titolo di risarcimento va calcolata in modo da corrispondere all'entità della perdita economica subita dalla vittima», ma che «parlare di risarcimento integrale per il danno non patrimoniale [*è*] formulazione priva di significato» e che – di conseguenza – sarebbe «una missione impossibile proporsi di determinare i criteri di quantificazione del danno non patrimoniale attraverso l'applicazione di quel principio» (Salvi 2014).

D'altro canto, la controprova empirica dell'inapplicabilità del principio della «riparazione integrale» al risarcimento dei danni extra-patrimoniali è data dalla circostanza che il suo inappropriato richiamo è insuscettibile di tradursi in regole operative che aiutino il giudice al momento del «dunque». Quando, cioè, questi è concretamente chiamato a determinare la misura dell'arricchimento monetario da accordare a chi ha subito la privazione di un *quid* che non ha valore di scambio.

Riferimenti bibliografici

Buset, Giacomo. 2024. "Ingiustizia del danno e antigiuridicità del fatto nella responsabilità da trattamento dei dati personali." *Rivista di diritto civile* 5: 1008-32.

Camardi, Carmelita. 2023. "Illecito trattamento dei dati e danno non patrimoniale. Verso una dogmatica europea." *La nuova giurisprudenza civile commentata* 5: 1136-45.

Comporti, Marco. 2000. "Le presunzioni di responsabilità." *Rivista di diritto civile* 5 – Parte prima: 615-61.

Episcopo, Francesca. 2024. "UI v. Österreichische Post – A First Brick in the Wall for a European Interpretation of Art. 82 GDPR. 9. Case note on: CJEU, 4/05/23 (C-300/21 UI v. Österreichische Post AG)." *EuCML* 87, 2.

Faccioli, Mirko. 2025. "Criterio di imputazione e risarcimento del danno nella responsabilità civile per illecito trattamento di dati personali." *Accademia* 7: 167-95.

Navone, Gianluca. 2022. "Ieri, oggi e domani della responsabilità civile da illecito trattamento dei dati personali" *Nuove leggi civili commentate* 1: 132-62.

Pagliantini, Stefano. 2023. "Un altro palcoscenico della «guerra» tra le corti: il danno (immateriale) bagatellare dell'art. 82 Gdpr". *Il foro italiano* 6 – Parte quarta: 285-93.

Palmieri, Alessandro, e Roberto Pardolesi. 2023. "*Mai futile il danno non* patrimoniale da violazione della privacy (purché lo si provi)." *Il foro italiano* 6 – Parte quarte: 278-84.

Salanitro, Ugo. 2023. "Illecito trattamento dei dati personali e risarcimento del danno nel prisma della Corte di giustizia." *Rivista di diritto civile* 3: 426-57.

Salvi, Cesare. 2014. "Il risarcimento integrale del danno non patrimoniale, una missione impossibile. Osservazione sui criteri per la liquidazione del danno non patrimoniale." *Europa e diritto privato* 3: 217-31.

Scognamiglio, Claudio. 2023. "Danno e risarcimento nel sistema del Rgpd: un primo nucleo di disciplina eurounitaria della responsabilità civile?" *La Nuova Giurisprudenza Civile Commentata* 5: 1150-59.

STRUMENTI DEL DIPARTIMENTO DI GIURISPRUDENZA DI SIENA

TITOLI PUBBLICATI

1. Mario Perini (a cura di), *Il gioco d'azzardo: una prospettiva multidisciplinare. Atti del convegno tenutosi presso il Dipartimento di Giurisprudenza dell'Università degli Studi di Siena il 1° dicembre 2023*, 2024
2. Gianfranco Orlando, *Beni culturali umani. Reificazioni, risignificazioni, restituzioni*, 2024
3. Mario Perini (a cura di), *La tutela dei diritti nell'era della riproduzione artistica digitale. Atti del Convegno tenutosi presso il Dipartimento di Giurisprudenza dell'Università degli Studi di Siena il 19 aprile 2024*, 2025
4. Chiara Angiolini, Antonello Iuliani (a cura di), *Manuale sulla protezione e circolazione dei dati personali*, 2025

Strumenti del Dipartimento di Giurisprudenza di Siena

MANUALE SULLA PROTEZIONE E CIRCOLAZIONE DEI DATI PERSONALI

Questo manuale è volto a offrire agli studenti, ai professionisti del settore e, più in generale, a chiunque voglia accostarsi alla materia, uno strumento per acquisire una conoscenza sistematica delle nozioni e degli istituti relativi alla protezione e alla circolazione dei dati personali. L'analisi del dettato normativo, non limitata al solo Regolamento Generale sulla Protezione dei Dati Personali (Reg. UE 2016/679) ed estesa anche ad alcuni profili dei più recenti atti normativi, come il *Data Act* (Reg. UE 2023/2854) e il *Data Governance Act* (Reg. UE 2022/868), è arricchita da una disamina della giurisprudenza europea e nazionale più rilevante, indispensabile per comprendere le *rationes* e l'effettiva portata delle regole che compongono il diritto attuale.

CHIARA ANGIOLINI è ricercatrice presso l'Università di Siena e abilitata alle funzioni di professoressa associata in Diritto privato. È autrice di monografie e saggi in tema di protezione dei dati personali, diritto dei consumatori, diritto agrario, diritto dei beni e dei contratti.

ANTONELLO IULIANI è professore ordinario di Diritto privato presso l'Università Pegaso. È autore di monografie e saggi in tema di obbligazioni e contratti, teoria dei beni e responsabilità civile.

ISSN 3035-5656 (print)
ISSN 3035-5842 (online)
ISBN 979-12-215-0795-9 (Print)
ISBN 979-12-215-0796-6 (PDF)
ISBN 979-12-215-0797-3 (ePUB)
ISBN 979-12-215-0798-0 (XML)
DOI 10.36253/979-12-215-0796-6
www.fupress.com