UNIVERSITÀ
DEGLI STUDI
DI PADOVA

Sede Amministrativa: Università degli Studi di Padova
Dipartimento di Scienze Politiche, Giuridiche e Studi Internazionali

CORSO DI DOTTORATO DI RICERCA IN: Diritto internazionale e diritto privato e del lavoro
CICLO: XXXIV

LA RESPONSABILITÀ CIVILE DA ILLECITO TRATTAMENTO DEI DATI PERSONALI

Coordinatore e Supervisore: Ch.ma Prof.ssa Arianna Fusaro

Dottorando: Dr. Giovanni Calabrese

La responsabilità civile da illecito trattamento dei dati personali

La tesi affronta il tema della responsabilità civile da illecito trattamento dei dati personali (art. 82 GDPR).
Il lavoro si pone l'obbiettivo di dimostrare che, mentre il diritto alla privacy è un diritto essenzialmente individualistico, il diritto alla protezione dei dati è, solo parzialmente, un diritto soggettivo. Per poter predisporre strumenti di tutela più efficaci, è necessario abbandonare la concezione prettamente individualista, che comporta un sistema di responsabilità ad azione del singolo. In particolare, quando i trattamenti involgono attività di profilazione e big data, dovrebbero essere garantite anche finalità di sviluppo etico e sociale. Il diritto alla protezione dei dati dovrebbe, dunque, considerare maggiormente i rischi collettivi e il sistema di accountability dovrebbe essere integrato da obblighi di trasparenza maggiori e da un sistema di controlli più penetranti ed incisivi da parte delle autorità di controllo.
La prima parte del lavoro si concentra sull'evoluzione che ha portato all'affermazione del diritto alla protezione dei dati, quale espressione del diritto alla privacy, tenendo in considerazione il contesto tecnologico in cui tale riconoscimento è maturato. L'analisi ripercorre le principali teorie della dottrina e della giurisprudenza statunitensi che hanno contribuito all'affermazione del diritto alla privacy, per dimostrare che esso viene inteso in chiave essenzialmente individualistica.
L'evoluzione storica ripercorre le tappe legislative europee e nazionali sulla disciplina dei dati e culmina con un'analisi dei punti di contatto tra diritto alla protezione dei dati, il diritto alla riservatezza, il diritto all'identità personale, il diritto all'autodeterminazione.
Nel secondo capitolo, si evidenzia che l'evoluzione esponenziale degli strumenti tecnologici dell'epoca moderna mette in crisi la concezione del diritto alla protezione dei dati in chiave essenzialmente individualistica. In particolare, la creazione di internet, le piattaforme informatiche, i social network, lo sviluppo dell'intelligenza artificiale e gli algoritmi predittivi, rischiano di rendere del tutto inefficiente e inadeguato un sistema di tutela basato su una concezione meramente individualistica del diritto alla protezione dei dati. Si analizzano i rischi collettivi/sociali del trattamento dei dati, illustrando le principali teorie della sorveglianza.
Nel terzo capitolo si analizzano le figure soggettive di cui all'art. 82 GDPR e i principi del trattamento. L'analisi evidenzia che il meccanismo di tutela ancora fondato sul consenso determina una forte perdita di effettività del sistema di tutela dei dati. Il GDPR si focalizza maggiormente sulla figura del titolare, su cui gravitano obblighi pregnanti, in particolare quello di accountability. Il titolare è tenuto a svolgere un'attività di ponderazione dei rischi per mettere in atto misure tecniche e organizzative per evitarli o mitigarli. Egli è tenuto a monitorare costantemente i processi della sua attività imprenditoriale che involgono l'utilizzo di dati ed è tenuto a conformare la propria attività nell'osservanza dei principi del GDPR.
L'ultima parte del lavoro di ricerca tratta della natura della responsabilità per illecito trattamento dei dati personali. La tesi approfondisce il modello di gestione del rischio disegnato dal GDPR, secondo cui il titolare deve mantenere un approccio proattivo nel prevenire i rischi, dotandosi di una struttura organizzativa che, a tutti i livelli e in tutte le aree di competenza, adotti le necessarie misure per garantire che i dati personali siano trattati sempre in modo lecito. Da ultimo il lavoro di ricerca approfondisce il problema dei danni risarcibili a seguito di trattamento illecito, con riferimento specifico alla questione dei danni non patrimoniali. Nella dottrina europea vi è un acceso dibattito attorno al problema della risarcibilità, in termini di definizione e quantificazione, dei danni immateriali derivanti da illecito trattamento.

Civil liability for the unlawful processing of personal data

This research thesis addresses the issue of civil liability for unlawful processing of personal data (art. 82 GDPR).

The research aims to demonstrate that, while the right to privacy is an essentially personal right, the right to data protection is, only partially, a subjective right. In order to provide more effective protection tools, it is necessary to abandon the purely individualistic conception, which involves a system of responsibility based on the action of the individual. In particular, when processing involves profiling and big data, ethical and social development purposes should also be guaranteed. The right to data protection should, therefore, take more account of collective risks and the accountability system should be complemented by greater transparency obligations and a system of more penetrating and incisive controls by supervisory authorities.

The first part of the thesis focuses on the evolution that has led to the affirmation of the right to data protection, as an expression of the right to privacy, taking into account the technological context in which this recognition has matured. The analysis retraces the main theories of U.S. doctrine and jurisprudence that have contributed to the affirmation of the right to privacy, to show that it is understood in an essentially personalistic key.

The historical evolution traces the stages of European and national legislation on data regulation and culminates with an analysis that highlights how the right to data protection, the right to privacy, the right to personal identity, the right to self-determination are intertwined.

In the second chapter, we show that the exponential evolution of technological tools of the modern era undermines the conception of the right to data protection in an essentially personalistic key. In particular, the creation of the internet, computer platforms, social networks, the development of artificial intelligence and predictive algorithms, are likely to make completely inefficient and inadequate a system of protection based on a purely personalistic conception of the right to data protection. The collective/social risks of data processing are analyzed, illustrating the main theories of surveillance.

In the third chapter, the subjects referred to in Article 82 GDPR and the principles of processing are analyzed. The analysis shows that the protection mechanism still based on consent determines a strong loss of effectiveness of the data protection system. The GDPR focuses on the figure of the controller, who is burdened by significant obligations, in particular that of accountability. The controller is required to carry out a risk assessment activity in order to implement technical and organizational measures to avoid or mitigate risks. He is required to constantly monitor the processes of his business activity that involve the use of data and is required to comply with the principles of the GDPR.

The last part of the research deals with the nature and discipline of liability for unlawful processing of personal data. The thesis delves into the risk management model designed by the GDPR, according to which the controller must adopt a proactive approach in preventing risks through an organizational structure that, at all levels and in all areas of competence, takes the necessary measures to ensure that personal data are always processed lawfully. Lastly, the research explores the issue of the damages resulting from unlawful processing, with specific reference to the issue of immaterial damages. In the European doctrine there is a heated debate around the problem of compensability, both in terms of definition and quantification, of immaterial damages resulting from unlawful processing.

INDICE

Capitolo III

SOGGETTI E PRINCIPI DEL TRATTAMENTO

Capitolo IV

NATURA E DISCIPLINA DELLA RESPONSABILITÀ

DA ILLECITO TRATTAMENTO DEI DATI

Introduzione

Rodotà ha osservato che il moderno concetto di riservatezza nasce a seguito della scomparsa della società feudale e, in particolare, che si tratta di un sentire sociale che emerge nella società borghese della fine dell'Ottocento, intimamente connesso al parallelo affermarsi dell'individualismo dell'epoca[1]. La *privacy* è, infatti, legata al riconoscimento dell'individuo come soggetto al centro della scena sociale e giuridica.

È vero che tale riconoscimento è formalmente contenuto nella Dichiarazione dei diritti dell'uomo e del cittadino, ma è stato osservato che, nella sostanza, occorre molto tempo perché l'astratto individuo giuridico in essa delineato si trasformi in realtà [2].

È proprio durante il XIX secolo che si accentua e diffonde il sentimento dell'identità personale[3]: con esso, inizia a formarsi l'idea di una sfera di vita privata, da cui l'individuo può escludere sia gli altri consociati, sia lo Stato.

Questa idea di vita privata e personale è catalizzata dalle trasformazioni socio-economiche dell'Ottocento, che incidono, di fatto, anche sulla conformazione e sull'organizzazione della stessa vita cittadina, anche in senso di organizzazione architettonica delle città, consentendo all'uomo borghese di costruirsi spazi fisici e spirituali che prima non erano ipotizzabili.

Si contrappone l'idea di casa, di famiglia, di privato, all'idea di scena pubblica, ed emerge il pensiero e la necessità di un luogo privato, l'abitazione, in cui l'uomo vive la propria intimità escludendo il pubblico. Per la società dell'epoca, "*la vita privata è il rifugio dove gli uomini si riposano dal loro lavoro e dal mondo esterno. Tutto deve essere fatto per rendere questo rifugio piacevole. La casa è il nido, il luogo del tempo sospeso*"[4].

Il diritto alla vita privata che viene sviluppandosi è una facoltà connessa al diffondersi della ricchezza nelle classi borghese e aristocratica, ricchezza che consente all'individuo – borghese – di crearsi uno spazio di intimità personale e di appropriarsene: per questo l'Ottocento è considerata l'"età aurea del privato"[5].

Come oggi ci poniamo il problema della tutela dei dati in relazione allo sviluppo di tecnologie sempre

---

[1] S. RODOTÀ, *Elaboratori elettronici e controllo sociale*, Il Mulino, 1973, ID., *La privacy tra individuo e collettività*, in *Politica e diritto*, 1974, pp. 545 ss.; per un'analisi statunitense, si v. W. FAULKNER*, Privacy. Il sogno americano: che ne è stato?,* traduzione italiana a cura di M. MATERASSI, Adelphi, 2003.

[2] M. PERROT, *Introduzione*, in *La vita privata*, *L'Ottocento* a cura di P. ARIÈS-G. DUBY, vol. 4, Editori Laterza, 1988, p. 5, "*in quanto in quest'epoca tra società civile, privato, intimo e individuale si traccerebbero dei cerchi idealmente concentrici e realmente intersecantesi*".

[3] A. CORBIN, *Il segreto dell'individuo*, in *La vita privata. L'Ottocento*, a cura di M. PERROT, traduzioni di Fausta Cataldi Villani, Maria Garin, Stefano Neri, Francesco Salvatorelli, Laterza, 1988, p. 333.

[4] A. MARTIN-A.FUGIER, *I riti della vita privata nella borghesia*, in *La vita privata*, p. 161.

[5] M. PERROT, *Introduzione*, cit., p. 4.

più evolute, alla fine del diciannovesimo secolo il bisogno di riservatezza si evolve anche in relazione al diffondersi di tre particolari tecnologie[6].

La prima è l'invenzione del telefono, che diviene immediatamente strumento essenziale per tutte le attività umane. La diffusione delle linee telefoniche, tuttavia, rende presto le conversazioni vulnerabili, perché possono essere captate dalle forze di polizia per esercitare controllo, sorveglianza e svolgere indagini, nonché dalle orecchie indiscrete della stampa.

La seconda invenzione fondamentale è il microfono, che consente di ascoltare e registrare conversazioni in luoghi distanti da colui che ascolta e che ben presto diviene uno strumento diffuso nelle indagini di polizia.

L'ultimo progresso tecnologico è la fotografia istantanea[7], accessibile a qualsiasi amatore perché di utilizzo relativamente semplice, nonché di dimensioni contenute, che ne consentono la portabilità.

In particolare, lo sviluppo di quest'ultima tecnologia contribuisce a delineare maggiormente il sentimento dell'identità personale. Si diffonde, infatti, la moda della fotografia di famiglia e dell'esibizione del ritratto di sé. Corbin osserva che "*messo ben in vista, il ritratto è testimonianza del successo*" dell'uomo borghese e, grazie alla fotografia, "*l'uomo* [borghese] *del popolo potrà per la prima volta fissare, possedere e replicare in serie la propria immagine*"[8].

Ben presto, queste tecnologie pongono il problema della riservatezza nel rapporto tra individuo e Stato, nonché nel rapporto tra individui.

Infatti, l'affermazione dell'io individuale va di pari passi con la cd. perdita di "anonimato", che contraddistingueva la popolazione al tempo del feudalesimo. A mano a mano che viene meno l'anonimato del popolo, s'impone alle autorità pubbliche la necessità di operare una forma di controllo, sorvegliare sulle singole persone: "*la folla, che sempre più fitta e silenziosa occupa le strade, perde la propria teatralità, trasformandosi in un aggregato di persone assorte nel pensiero dei propri personali interessi. Si comprende come da quel momento i sistemi d'identificazione divengano più sofisticati e come vada precisandosi il controllo sociale*"[9]. Infatti, le sopracitate tecnologie consentono all'autorità pubblica di svolgere un controllo, una sorveglianza, sulla società.

Sul diverso fronte della riservatezza nel rapporto tra individui, possiamo osservare che il diffondersi della fotografia istantanea è direttamente collegato allo sviluppo della "stampa sensazionalistica", la cui invadenza è una delle ragioni che muovono Warren e Brandeis[10] alla scrittura del famoso saggio[11].

---

[6] A. F. WESTIN, *Privacy and Freedom*, Atheneum New York, 1967, p. 338.
[7] Per un'analisi delle tecnologie emergenti in relazione alla concezione della vita privata nell'Ottocento, *cfr* A. CORBIN, *Il segreto dell'individuo*, in *La vita privata*, cit., p. 335.
[8] *Ibidem*, p. 335.
[9] A. CORBIN, *op. cit*., p. 339.
[10] S. WARREN-L. BRANDEIS, *The right to Privacy*, Vol. 4, No. 5., in *Harvard Law Review*, 1890, p. 193.
[11] S. RODOTÀ, *opp. citt*.; N. LUGARESI, *Internet, Privacy e pubblici poteri negli Stati Uniti*, Giuffrè, 2000.

Infatti, nel 1833 nasce nel Regno Unito il tabloid *Sun*, che riporta notizie di microcriminalità, litigi nelle famiglie borghesi altolocate, scandali pubblici, ossia il cosiddetto gossip: sei mesi dopo la sua fondazione, circolano ogni giorno per Londra oltre 8.000 copie del quotidiano.

Il fenomeno approda anche in America, dove si sviluppa esponenzialmente la cd. stampa sensazionalistica[12], anche detta "giornalismo giallo"[13], ossia una forma di giornalismo che esalta enormemente le notizie, attraverso l'uso dei titoli degli striscioni, la fumettistica colorata e le numerose illustrazioni[14]: se nel 1850 ci sono circa un centinaio di quotidiani pubblicati con 800.000 lettori, alla fine del 1890 i giornali pubblicati sono oltre 900 con più di 8 milioni di lettori.

Le principali testate giornalistiche sono, peraltro, in mano a J. Pulitzer e W. R. Hearst, i quali, per superarsi nella reciproca rivalità, esaltano al massimo il sensazionalismo in ogni articolo pubblicato, così ponendo le basi per una lesione della sfera di vita privata dei consociati.

La fortuna di questi quotidiani si deve, peraltro, ad un'ulteriore invenzione tecnologica, la macchina da stampa a rotativa e la linotipia, che consentono di stampare molte copie ad un minimo costo, includendo immagini e riproduzioni fotografiche all'interno dei quotidiani stessi.

---

[12] S. ROTENBERG SCHWARTZ, *Information privacy law*, Aspen Publishers, 2005, p. 9.

[13] *Cfr* W. L. PROSSER, *Privacy*, in *California Law Review*, vol 48, no. 3, 1960.

[14] Lo sviluppo dei tabloid americani viene descritto da C. DICKENS, nel suo romanzo *The life and adventurers of Martin Chuzzlewit*, 1844.

Capitolo I

LA TUTELA DEI DATI PERSONALI NELLA SOCIETÀ TECNOLOGICA

SOMMARIO: 1. La nascita del diritto alla privacy e il saggio Warren-Brandeis. - 2. La successiva evoluzione nella dottrina statunitense: la teoria di Prosser. - 3. Costituzione americana ed evoluzione nella giurisprudenza della Suprema Corte. - 3.1. *Il caso Olmstead v. United States.* - 3.2. *Il caso Katz v. United States.* - 3.3. *Il caso Whalen v. Roe*. - 4. L'approdo della privacy nella dottrina italiana. - 5. Diritto alla personalità e riservatezza. - 6. Il riconoscimento della privacy nella giurisprudenza italiana. - 7. Il successivo sviluppo tecnologico e le nuove istanze di tutela della privacy. I dati personali. - 8. Gli elaboratori elettronici. - 9. Il diritto alla protezione dati nel contesto europeo. - 10. Prime leggi italiane sulla tutela dei dati personali. - 11. Rapporto tra diritto alla protezione dati e riservatezza. - 12. Rapporto tra diritto alla protezione dati e identità personale (digitale). - 13. Responsabilità per illecito trattamento nel Codice della *privacy* (rinvio). - 14. Il Regolamento europeo per la protezione dei dati. - 15. L'art. 82 GDPR. Cenni. - 16. Natura anche patrimoniale del diritto alla protezione dei dati.

1. La nascita del diritto alla *privacy* e il saggio Warren-Brandeis

La definizione di *privacy* si deve a Cooley[15], che nell'ambito di un trattato in tema di illecito aquiliano, si trovò, quasi per caso, a definire la *privacy* come "*the right to one's person may be said to be a right of complete immunity: to be let alone*".

Come opportunamente osservato, "*to be let alone*" non va tradotto come diritto "*ad esser lasciati soli*" quanto, piuttosto, diritto "*ad esser lasciati tranquilli*"[16], ossia diritto a mantenere una vita privata, all'interno delle mura della propria casa in particolare, con la facoltà di escludere gli altri da questa sfera di intimità.

Per comprendere il contesto in cui scrissero il loro saggio[17], va tenuto in considerazione che i due giovani avvocati Warren e Brandeis vivevano la vita della più altolocata borghesia dell'epoca, i cui componenti sviluppavano il senso e la ricerca della riservatezza.

In particolare, Warren era personalmente interessato al tema della riservatezza, poiché la moglie era

---

[15] T. C. COLLEY, *A treatise on the Law of Torts or the Wrongs which arise indipendent of Contract*, Callaghan & Company, Chicago, 1889.

[16] N. LUGARESI, *Internet, Privacy e pubblici poteri negli Stati Uniti*, Giuffrè, 2000; A. G. PARISI, *Privacy e mercato digitale*, Pacini, 2020; F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali*, I, Giappichelli, 2016, p. 43 ss.; A. MANTELERO, *Il costo della privacy tra valore della persona e ragione d'impresa*, Giuffrè, 2007.

[17] S. WARREN-L. BRANDEIS, *The right to Privacy*, Vol. 4, No. 5., in *Harvard Law Review*, 1890, p. 193.

stata coinvolta dalla stampa in alcuni scandali mondani che ne avevano compromesso la reputazione. Egli si chiedeva, pertanto, se la notorietà dovuta alla sua posizione sociale fosse una ragione che potesse giustificare le intrusioni del pubblico nella propria vita privata.

Brandeis, di religione ebraica, era interessato ai diritti delle minoranze e ai pericoli delle discriminazioni basate sulle raccolte di dati e sull'espressione delle opinioni[18].

Questo evidenzia che già nella prima formulazione di questo diritto si intravedono due anime ben distinte: quella prettamente individualistica (Warren) e quella che risponde ad un interesse più collettivo e sociale o, comunque, di una cerchia determinata di soggetti comunque superiore al mero individuo. Sarà il primo di questi due aspetti quello che verrà maggiormente tenuto in considerazione dalle elaborazioni successive.

Nella premessa del saggio i due Autori spiegano che se l'ordinamento giuridico inizialmente tutelava la proprietà materiale e l'individuo nel suo profilo "fisico", successivamente si è giunti a riconoscere una certa tutela anche dalle aggressioni alla sfera spirituale dell'uomo, dei suoi sentimenti e del suo intelletto[19].

Infatti, il concetto di diritto alla vita si è allargato sino a ricomprendere il concetto a *godere* della vita, così come la proprietà si è estesa sino a comprendere la possibilità di essere proprietari di beni intangibili, non esclusivamente materiali. In particolare, affermano Warren e Brandeis, "*later, there came a recognition of man's spiritual nature, of his feelings and his intellect. Gradually the scope of these legal rights broadened; and now the right to life has come to mean the right to enjoy the life, the right to be let alone; […] and the term "property has grown to compromise every form of possession, intangible, as well as tangible*".

I due autori passano in rassegna, a questo punto, i principali beni "intangibili" dell'individuo che vengono tutelati dall'ordinamento: il ragionamento sarà il presupposto necessario per verificare se il diritto alla *privacy* è, effettivamente, riconosciuto e tutelato dal *common law*.

Osservano che la reputazione dell'individuo, ossia lo stare in mezzo agli altri cittadini, viene preso in considerazione e tutelato dal diritto con le leggi contro la calunnia e la diffamazione[20].

Le relazioni famigliari dell'uomo sono divenute parte della concezione legale della sua vita. Da un punto di vista civilistico, viene riconosciuto anche il danno morale per la lesione dell'onore della famiglia.

Il bisogno di tutela di queste situazioni giuridiche, non direttamente percepibili, viene collegato all'avvento delle nuove tecnologie e all'uso, che i due autori ritengono non lecito, che di esse fa la

---

[18] S. RODOTÀ, *Prefazione*, in M. BOCCHIOLA, *Privacy. Filosofia e politica di un concetto inesistente*, Luiss, 2014, p. 10.
[19] S. WARREN-L. BRANDEIS, *op. cit*., p. 193, "*and now the right to life has come to mean the right to enjoy life, the right to be let alone*".
[20] "*His reputation, the standing among his fellow-men, was considered, and the law of slander and libel arose*".

stampa scandalistica: osservano che fotografie e industrie della carta stampata hanno invaso i sacri limiti della sfera privata e le nuove tecnologie hanno consentito di rendere pubblico tutto ciò che avviene nell'intimità della vita privata[21].

Peraltro, gli autori osservano che la giurisprudenza ha già riconosciuto la tutela inibitoria a difesa dell'immagine personale, menzionando il caso dell'attrice Marion Manola, che era stata fotografata all'improvviso, senza il suo consenso, nel camerino di un teatro di Broadway; il fotografo aveva ottenuto l'accesso agli spazi riservati al personale con la complicità del proprietario del locale. In questo caso, il tribunale aveva ingiunto al fotografo di non utilizzare o diffondere la fotografia[22].

È evidente che, nella prima teorizzazione effettuata in materia, il problema ruota principalmente attorno al rapporto tra diritto alla *privacy* dell'individuo e diritto di cronaca, il quale viene tuttavia utilizzato, secondo W.-B., in modo distorto, "*the press is overstepping in every direction the obvious boungs of property and of decency. Gossip is no longer the resource of the idle and of the vicious, but has become a trade, which is pursued with industry as well as effrontery*".

Analizzate, dunque, le ragioni che imporrebbero di tutelare il diritto alla *privacy*, i due autori verificano se vi sono strumenti già apprestati dall'ordinamento per ottenere detta tutela.

L'argomentazione viene svolta verificando se sia possibile applicare a questa situazione giuridica soggettiva i rimedi previsti dalle leggi sulla diffamazione e sulla proprietà intellettuale.

Osservano, infatti, che il danno per violazione della *privacy* presenta, almeno superficialmente, una somiglianza con i danni conseguenti a calunnie e diffamazioni. Ma la *ratio* di tale disciplina differisce radicalmente, in quanto protegge esclusivamente il sentimento dell'onore e della reputazione. La tutela della diffamazione ha a che fare col danno alla reputazione nella sfera delle relazioni esterne dell'individuo, ovvero colpisce la stima che i consociati nutrono nei suoi confronti.

Ciò che viene pubblicato, a prescindere dalla vastità della sua circolazione e dal pubblico che riesce a raggiungere, per essere sanzionabile deve avere un effetto dannoso sui rapporti con gli altri, deve cioè esporlo al ridicolo dei consociati. La legge sulla diffamazione non tutela direttamente il sentimento dell'io interiore, ossia la "*stima che l'individuo ripone in sé stesso*".

Con riferimento alla legge sulla tutela della proprietà intellettuale, osservano i due autori che tale disciplina tutela beni immateriali, in particolare parole, segni, dipinti, sculture, musica. L'accostamento del diritto alla *privacy* con il diritto alla proprietà intellettuale è passaggio argomentativo volto a evidenziare che l'ordinamento già tutela beni immateriali, sicché anche la sfera spirituale dell'individuo può essere riconosciuta come un bene da tutelare. Evidenziano gli autori che

---

[21] *Instantaneous photographs and newspaper enterprise have invaded te sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall ben proclaimed from the house-tops*.

[22] N.Y. SUPREME COURT, 15.6.1890, Marion Manola v. Stevens & Myers.

la giurisprudenza ha più volte riconosciuto la tutelabilità della sfera intellettiva dell'uomo, delle sue idee. E aggiungono che nessuno può essere obbligato a esprimere e rendere pubbliche le proprie idee e i propri sentimenti (salvo il testimone chiamato a deporre in tribunale).

E anche nel caso in cui l'individuo decida di esprimere ciò che pensa, egli ha comunque il potere di "governare" la diffusione del proprio pensiero, fissandone dei limiti. Uno snodo argomentativo è fondamentale: la legge sulla proprietà intellettuale non ne tutela solo il valore economico e commerciale, perché la *ratio* di questa disciplina non è la proprietà privata. Al contrario, le opere dell'intelletto vengono tutelate perché appartengono al solo individuo e sono tutelate perché è tutelata l'inviolabilità personale del soggetto.

Ma questa tutela è comunque accordata per un fine economico del soggetto. Laddove questo non si configura, la legge sulla proprietà intellettuale non è sufficiente per tutelare l'inviolabilità personale. Qualora l'idea e la sua manifestazione sia del tutto slegata dal concetto di profitto ricavabile, è necessario tutelarla sulla base di principi differenti e la legge sulla proprietà privata non offre un'adeguata tutela.

Il contenuto del diritto alla *privacy* dimostra, dunque, che esso non può essere accostato alla reputazione, tutelata dalla legge sulla diffamazione e calunnia, né ad un'opera del suo autore, tutelata dalla legge sulla proprietà intellettuale.

La tutela del diritto alla *privacy* può essere riconosciuta intendendo in modo più estensivo e più moderno il concetto di proprietà: ogni individuo è "proprietario" della propria identità personale e può escludere le ingerenze degli altri consociati come potrebbe fare per violazioni alla proprietà privata materiale. Il diritto di proprietà, nel suo significato più ampio, include tutti i tipi di possesso, tutti i diritti e i privilegi e, dunque, include anche il diritto all' inviolabilità della persona.

La *privacy* è perciò un diritto *as against the world*. Il principio che protegge gli scritti di una persona e qualsiasi altra produzione dell'intelletto e delle emozioni è il diritto alla *privacy*: la legge non deve porre un nuovo principio per proteggere anche l'aspetto personale/individuale di un soggetto, né per tutelare ciò che egli dice o fa, o le sue relazioni personali o intime.

L' invasione della *privacy* costituisce una lesione dell'identità individuale e gli elementi per esigerne una riparazione sono già presenti nell'ordinamento.

Nel loro saggio, Warren-Brandeis avvertono che, comunque, non si tratta di un diritto in assoluto prevalente, in quanto il diritto di cronaca prevale sulla *privacy* quando la notizia ha ad oggetto materie pubbliche o di interesse generale: il personaggio pubblico non può, pertanto, pretendere che la propria riservatezza prevalga sul diritto di stampa, perché è l'invasione non autorizzata della *privacy individuale* che è da condannare e se possibile da prevenire. Essi teorizzano che i motivi per cui la pubblicazione dovrebbe essere inibita sono quelli che concernono la vita privata, le abitudini, gli atti,

le relazioni di un individuo che non hanno una connessione con la carica pubblica ricoperta dal soggetto, o con la sua capacità di ricoprire incarichi pubblici. Inoltre, il diritto alla *privacy* non proibisce ogni tipo di comunicazione, se essa è fatta in circostanze che la rendono privilegiata, secondo la legge sulla diffamazione e l'ingiuria (come potrebbero essere le comunicazioni che si svolgono nell'aula di tribunale o nell'assemblea legislativa).

Proprio perché l'oggetto del saggio è, in particolare, il bilanciamento tra *privacy* e cronaca, viene affermato che non c'è violazione del diritto alla *privacy* qualora l'individuo abbia prestato il consenso alla pubblicazione della notizia.

Per quanto attiene ai rimedi civili per la lesione del diritto alla *privacy*, i due autori teorizzano che possano essere i medesimi – ma non applicati in via analogica – di quelli previsti contro la diffamazione e a difesa del diritto d'autore e della proprietà intellettuale, ossia: *i*) l'azione extracontrattuale di risarcimento del danno, che può prevedere un risarcimento anche per il solo danno morale; *ii*) l'azione inibitoria.

Dunque, inizialmente la *privacy* si sviluppa in una versione esclusivamente individualistica del diritto, con una visione antropocentrica che vuole tutelare la sfera di intimità delle persone.

Quest'idea verrà a pervadere tutti i successivi studi sulla *privacy*: Faulkner, alcuni anni più tardi, affermerà che la libertà di ciascuno finisce dove inizia la sfera di libertà e intimità degli altri consociati[23].

2. La successiva evoluzione nella dottrina statunitense: la teoria di Prosser

Il saggio di Warren-Brandeis è stato il primo intervento di una lunga serie sul diritto alla *privacy*. A parte alcune eccezioni, la dottrina statunitense si è trovata d'accordo con la costruzione dogmatica operata dai due autori. Peraltro, l'articolo dei due autori ha avuto un immediato effetto sulle decisioni dei Giudici, come vedremo nei paragrafi successivi.

Nel 1960 viene pubblicato sulla California Law Review un articolo di William Prosser[24] che riscuote un successo immediato per la nuova prospettiva di studio.

Tale saggio, che ha rivestito primaria importanza nel dibattito in materia, è, comunque, stato anche molto criticato, perché, come vedremo, scompone il diritto alla *privacy* in tanti interessi quante sarebbero le differenti situazioni giuridiche che ricadono all'interno del concetto di riservatezza: viene, dunque, a mancare l'unitarietà del diritto alla personalità e all'identità personale.

L'analisi è interessante perché, da un certo angolo di prospettiva, la teoria di Prosser presenta

---

[23] W. FAULKNER*, Privacy. Il sogno americano: che ne è stato?,* traduzione italiana a cura di M. MATERASSI, Adelphi, 2003.

[24] W. L. PROSSER, *Privacy*, in *California Law Review*, vol 48, no. 3, 1960, p. 384.

simmetrie con la teoria pluralista dei diritti della personalità, concezione che si sviluppa in Italia negli anni '50-'60.

Prosser analizza lo stato della giurisprudenza americana (verificando quasi quattrocento casi) e schematizza l'esistenza di quattro diverse situazioni giuridiche che ricomprende sotto il diritto alla *privacy*:

- "*intrusion apon the plaintiff's seclusion or solitude, or into his private affairs*";
- "*public disclosure of embarassing private facts about plaintiff*";
- "*publicity which places the plaintiff in a false light in the public eye*";
- "*appropriation, for the defendant's advantage, of the plaintiff's name or likeness*";

La necessità di tale schematizzazione nasce dall'evidenza, secondo Prosser, di una grave disomogeneità nelle decisioni dei tribunali. Egli ritiene che sia necessario portare a comune denominatore le varie fattispecie di *privacy*, individuandone caratteristiche comuni e apprestando forme di tutela differenti per ciascuna di esse: certamente la ricostruzione di Prosser enfatizza la chiave essenzialmente individuale del diritto alla privacy.

La prima fattispecie corrisponde all'interesse del soggetto a non subire "*mental distress*". Costituisce, dunque, un'intrusione nella sfera privata, e si realizza quando sussiste una condotta intrusiva altamente offensiva per una persona ragionevole.

La seconda figura tutela anch'essa l'interesse del soggetto ad essere libero da "*mental distress*", nonché la reputazione dello stesso. È la fattispecie che più si avvicina a quella tratteggiata nel saggio Warren-Brandeis. Anche in questo caso l'azione è ammissibile se vengono provate alcune circostanze, in particolare se la notizia che viene divulgata è altamente offensiva per una persona di comune ragionevolezza e non di interesse per la società. Questo *tort* viene approfondito da Prosser, stante l'ampia applicazione giurisprudenziale dello stesso: egli ne individua i principali limiti. Innanzitutto, non può essere impedita la pubblicazione di quelle informazioni ottenute in modo lecito che sono veritiere e di interesse pubblico. Inoltre, dev'esserci stata un'ampia pubblicità della notizia, come nel caso essa sia stata pubblicata su qualche giornale o, comunque, portata all'attenzione della comunità con una forma di pubblicità. Non viene, dunque, impedita la circolazione di notizie all'interno di cerchie famigliari o, comunque, ristrette. Questa fattispecie viene, come detto, considerata una sorta di estensione del *tort* di diffamazione: ma la caratteristica che le differenzia è la falsità della notizia: si tratta di requisito necessario affinché si realizzi la diffamazione, ininfluente ai fini di riconoscere una lesione alla *privacy*.

Va, tuttavia, precisato, che questa figura ha avuto un'applicazione sempre più restrittiva, a causa dell'ultimo requisito per la sua configurabilità, elaborato dalla successiva giurisprudenza. In particolare, afferma la giurisprudenza statunitense che l'azione è fondata solo se l'attore riesce a

provare l'"*actual malice*" del convenuto, ossia la conoscenza della falsità della notizia ovvero, in ogni caso, una sorta di negligenza nel verificare la fondatezza della stessa. Quest'ultimo requisito rende, di fatto, sempre lecita l'attività della stampa[25].

La terza figura di *privacy* (*tort* di *false light*) tutela specificamente la reputazione dell'individuo. Essa riguarda la diffusione di notizie che possono porre l'individuo sotto una "falsa luce" nella visione della comunità. Anche in questo caso, sono molte le condizioni che limitano l'utilizzabilità di questa azione, tra cui appunto il test relativo alla *actual malice*.

La quarta ipotesi schematizzata, ossia il *tort* di appropriazione del nome o dei tratti distintivi di una persona, tutela la reputazione del soggetto, la sua identità personale e, più nello specifico, tutela la relazione tra il soggetto e i propri tratti umani distintivi.

Si evidenzia che per nessuna delle quattro ipotesi rileva la verità della vicenda pubblicata. La verità non può essere una causa di esclusione della responsabilità né per il caso di ingerenza, né per l'appropriazione del nome o dell'immagine, né per la diffusione di fatti privati.

Sulla scia della previgente dottrina, anche Prosser teorizza che il consenso dell'interessato renda lecita l'intrusione. Afferma che il consenso può essere dato espressamente, oppure attraverso un comportamento inequivoco, ad esempio posando per una foto con la consapevolezza dello scopo per cui sarà usata. Inoltre, il consenso gratuito può essere revocato in ogni momento prima dell'intrusione; tuttavia, se il consenso riguarda un contratto per l'utilizzo dell'immagine, essendo il consenso di norma irrevocabile, non v'è alcuna responsabilità per la pubblicità e l'appropriazione entro i termini contrattualmente pattuiti. In questo caso, se l'intrusione in concreto va oltre il contratto, come per il caso dell'alterazione della foto dell'interessato, o viene fatta una pubblicità differente da quella pattuita, il consenso non sarà sufficiente a scongiurare la responsabilità.

Prosser evidenzia la tendenza della giurisprudenza a richiedere che il consenso sia espresso per iscritto. Anche laddove si ammette la rilevanza del consenso orale, questo è tenuto in considerazione per la riduzione dei danni, non per l'esclusione dell'azione.

Con riferimento ai rimedi per l'intrusione illecita nella vita privata, l'autore afferma la correttezza della soluzione proposta da Warren-Brandeis di riconoscere la tutela risarcitoria e la tutela inibitoria per la difesa della *privacy*.

Vediamo, ancora, che il diritto alla *privacy* è teorizzato solo in chiave di diritto soggettivo. Peraltro, va evidenziato che la teoria di Prosser viene criticata fortemente da una parte della dottrina americana, che ritiene tale teoria eccessivamente riduttiva, in quanto, nella sua scomposizione, non tiene in

[25] N. LUGARESI, *op. cit.*

adeguata considerazione l'aspetto, invece unitario, della dignità umana e dell'identità personale[26]. Infatti, ancorché sia vero che la *privacy* tutela diversi interessi, comunque la sua funzione primaria è quella di tutela della libertà personale di ogni individuo.

3. Costituzione americana ed evoluzione nella giurisprudenza della Suprema Corte

Nella Costituzione americana non è espressamente prevista la tutela del diritto alla *privacy*, trattandosi di concetto che, al momento della sua entrata in vigore (anno 1789), non era teorizzato, né era sentito come un valore che necessitasse di una tutela di rango così elevato. Solo con il successivo sviluppo tecnologico, si fa sentire l'esigenza di tutela della vita privata e si viene a riconoscere tutela costituzionale alla riservatezza.

Nel 1791 viene approvato il *Bill of Rights*, ossia dieci emendamenti che sostanzialmente limitano i poteri d'azione del governo, i quali sono, al contrario, riconosciuti dalla Costituzione. Va precisato, tuttavia, che è solo dal 1868 che ai cittadini vengono effettivamente riconosciuti tutti i diritti del *Bill of Rights*, quando viene approvato il XIV Emendamento che impedisce agli Stati di promulgare leggi statali contrari alla Costituzione federale.

È in questo bilanciamento tra fonti normative che si ricava la concezione americana del rapporto tra sfera pubblica e sfera privata: l'autorità pubblica persegue interessi preminenti collettivi (quali la sicurezza nazionale) e dunque ha, secondo la Costituzione, un ampio potere di intervento e di invadere il privato, potere limitato proprio dal *Bill of Rights*.

Possiamo riconoscere la radici costituzionali della *privacy* in quel principio, riconosciuto già dalla Dichiarazione d'Indipendenza del 1776, secondo cui ogni cittadino americano ha il diritto di perseguire la propria felicità[27].

Alla tutela di tale concetto è ispirato anche il Quarto Emendamento, il quale prescrive "*the right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized*"[28]: è dall'interpretazione estensiva di questa norma che si arriverà, successivamente, a riconoscere il diritto all'inviolabilità della vita privata degli americani. Il Quarto Emendamento tutela, dunque, l'inviolabilità della sicurezza e libertà personali, nonché del domicilio

---

[26] S. I. BENN, *Privacy*, *Freedom and Respect for persons*, in *Philosophical dimensions of Privacy: an Anthology*, Cambridge University Press, 1984, p. 223.

[27] W. FAULKNER, *op. cit.*; N. LUGARESI, *op. cit.*

[28] Il diritto dei cittadini di godere della sicurezza personale, della loro casa, delle loro carte e dei loro beni, nei confronti di perquisizioni e sequestri ingiustificati non potrà essere violato; e non si emetteranno mandati giudiziari se non su fondati motivi sostenuti da giuramento o da dichiarazione solenne e con descrizione precisa del luogo da perquisire e delle persone da arrestare o delle cose da sequestrare.

privato, da intrusioni della forza pubblica non autorizzate preventivamente da un mandato del giudice o dal consenso dell'interessato.

Ed infatti, nel caso *Boyd v. United States* del 1886, la Corte Suprema riconosce che tale disposizione tutela l'attività privata dell'individuo da illegittime invasioni del governo e delle forze di polizia[29].

Si afferma l'inviolabilità dell'abitazione privata, essenziale a garantire la libertà e sicurezza personali tutelate dalla Costituzione[30].

Tuttavia, solo con l'avvento delle nuove tecnologie, si sente l'effettiva necessità di tutelare autonomamente il valore della riservatezza, ossia non più in funzione della tutela di differenti libertà costituzionali.

Il percorso giurisprudenziale che ha portato la Corte Suprema USA al riconoscimento del diritto alla *privacy* è stato lungo svariati decenni. Collateralmente ad esso, continuavano incessanti l'industrializzazione e il rinnovamento tecnologico.

Di seguito analizzo le principali pronunce della Corte Suprema USA che hanno portato al riconoscimento della *privacy* come diritto soggettivo a limitare l'intrusione del potere pubblico nella sfera privata.

3.1. Il caso Olmstead v. United States

Il caso *Olmstead v United States* si colloca nell'anno 1928, ossia nel periodo del proibizionismo americano.

Olmstead era il capo di un'organizzazione criminale che contrabbandava liquori nella British Columbia. Per comunicare con gli affiliati, Olmstead utilizzava tre telefoni, collocati in un ufficio della propria abitazione, collegati ad altrettante linee telefoniche. Ogni affiliato era stato dotato di una linea telefonica privata e tramite telefono venivano gestite tutte le operazioni di trasferimento del liquore, sino alla vendita finale.

Le prove per incastrarlo vengono ottenute intercettando, per cinque mesi, le conversazioni telefoniche tramite una cimice agganciata direttamente ai cavi del telefono. Poiché il posizionamento della cimice non implicava alcuna intrusione nell'abitazione di Olmstead, le forze di polizia avevano ritenuto che non fosse necessario chiedere alcun mandato.

Olmstead, al contrario, chiedeva che tali prove fossero dichiarate illegittime e, dunque, inutilizzabili, sulla base del Quarto Emendamento, che secondo la sua tesi, doveva tutelare, anche le conversazioni private.

---

[29] *The principles laid down in this opinion affect the very essence of constitutional liberty and security. They reach further than the concrete form of the case then before the court, with its adventitious circumstances; they apply to all invasions on the part of the government and its employes of the sanctity of a man's home and the privacies of life*.

[30] N. LUGARESI, *op. cit*., p. 59.

La Suprema Corte conferma la legittimità delle intercettazioni, affermando che i cavi della linea telefonica non appartengono all'abitazione del cittadino, sicché, non essendosi verificata alcuna "intrusione" fisica, non era necessaria la richiesta di un mandato ai sensi del Quarto Emendamento.
Secondo la Corte, il Quarto Emendamento tutelerebbe la sola ricerca materiale sulla persona, nella sua casa, tra i suoi scritti, i suoi beni. Ma l'Emendamento non si applica al telegrafo o al telefono, con riferimento ai quali non può nemmeno configurarsi una "ricerca" in senso letterale, in quanto, al contrario, la conversazione viene semplicemente ascoltata. Dunque, sulla base di un'interpretazione letterale del Quarto Emendamento, la Corte esclude che vi sia stata un'intrusione illecita, non potendo sostenersi che i cavi della linea telefonica, che si estendono ed espandono dalle abitazioni private, appartengano ai privati stessi.

Nota è la *dissenting opinion* del giudice Brandeis, che si pone in perfetta linea di continuità con il precedente saggio a cui aveva partecipato.

Egli evidenzia la necessità di un'interpretazione evolutrice, che consenta all'ordinamento di adeguarsi ai mutamenti sociali e tecnologici, riconoscendo all'individuo protezione da quelle forme di abuso di potere che, se fossero stati conosciuti al tempo della redazione della Costituzione, sarebbero sicuramente stati vietati. Quando il Quarto Emendamento è stato adottato, le "forme" di violenza e intrusione che si volevano vietare erano esclusivamente di natura fisica, materiale. Ma le nuove scoperte ed invenzioni rendono possibile alle forze di polizia l'invasione della *privacy* con modalità prima inimmaginabili, rendendo possibile conoscere tutto ciò che viene sussurrato nel privato della vita domestica[31]. Per queste ragioni, la Corte ritiene essenziale estendere la tutela del Quarto Emendamento anche alle forme di violenza e intrusioni immateriali: lo scopo del *Bill of Rights* è quello di proteggere e garantire la libertà personale da ogni forma di intrusione, materiale e immateriale.

L'*opinion* è proiettata verso il futuro. Brandeis osserva che il progresso della scienza non si fermerà all'intercettazione telefonica, ma porterà a forme potenzialmente sempre più invadenti del vivere privato. Giunge ad immaginare che nel prossimo futuro la scienza avrebbe inventato tecnologie in grado di consentire di "ottenere e riprodurre copia di documenti chiusi in cassetti senza nemmeno toccarli", e che "le scoperte della fisica e delle scienze collegate porteranno a strumenti che renderanno possibile esplorare credenze, pensieri ed emozioni inespressi dall'individuo".

È perciò necessario, secondo Brandeis, interpretare la Costituzione adattandola all'evolversi del contesto tecnologico, avendo riguardo non all'interpretazione letterale di essa, ma alla *ratio* delle

---

[31] *Time works changes, brings into existence new conditions and purposes. Subtles and more far-reaching means of invading privacy have become available to the government. Discovery and invention have made possible for the government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet*.

disposizioni di protezione in essa prevista, perché i padri costituenti hanno riconosciuto "*the significance of man's spiritual nature, of his feelings and of his intellect* […] *They conferred, as against the government, the right to be let alone-the most comprehensive of rights and the right most valued by civilized men. To protect, that right, every unjustifiable intrusion by the government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment*".

3.2. Il caso Katz v. United States

Nel 1965 giunge alla Corte Suprema il caso *Katz v. United States*[32].

Il sig. Katz era stato condannato dalla Corte Distrettuale della California con l'accusa di aver trasmesso, tramite telefono, informazioni sulle scommesse da Los Angeles a Miami e Boston, in violazione di una legge federale.

Nel primo grado di giudizio, gli agenti dell'FBI avevano potuto presentare prove ottenute tramite intercettazioni telefoniche: gli agenti avevano collegato una cimice e un registratore all'esterno della cabina telefonica pubblica dalla quale l'allibratore aveva effettuato le sue chiamate.

Nel confermare la condanna, anche la Corte d'Appello aveva respinto la tesi secondo cui le registrazioni erano state ottenute in violazione del Quarto Emendamento.

L'imputato si difendeva sostenendo che la cabina telefonica pubblica è un luogo costituzionalmente protetto, sicché le prove ottenute collegando un dispositivo elettronico di registrazione dell'ascolto ai cavi di tale cabina erano ottenute in violazione del diritto alla *privacy* dell'utente della cabina stessa.

Al contrario, gli agenti dell'FBI, ritenevano che non vi fosse alcuna violazione del Quarto Emendamento, in quanto non erano entrati fisicamente nella cabina telefonica, sicché non sussisteva alcuna intrusione fisica nella sfera privata del soggetto.

Si trattava di un caso molto simile a quello di Olmstead, ma, questa volta, la Suprema Corte rovescia il risultato dei giudici di merito.

Innanzitutto, la Corte spiega che tali decisioni non avevano correttamente ricostruito la vicenda. Era stato attribuito grande significato alla caratterizzazione della cabina telefonica quale "area costituzionalmente protetta": l'imputato sosteneva tale qualificazione, negata dagli agenti. Il firmatario ha strenuamente sostenuto che lo stand era una "zona costituzionalmente protetta".

La Corte sposta totalmente la questione, osservando che il Quarto Emendamento protegge le persone, non i luoghi. Ciò che una persona espone consapevolmente al pubblico, anche a casa o in ufficio, non è soggetto alla protezione del Quarto Emendamento. Ma ciò che cerca di preservare come privato,

[32] Katz v. United States, 389 U.S. 347 (1967).

anche in un'area accessibile al pubblico, dev'essere tutelato costituzionalmente.
Dunque, la tutela riconosciuta dal Quarto Emendamento ai luoghi privati viene trasferita ai soggetti.
Nel processo, l'accusa aveva sottolineato che la cabina telefonica dalla quale Katz aveva effettuato le telefonate, era stata costruita in parte in vetro, in modo che fosse visibile chiunque vi entrasse, con la conseguenza che Katz non poteva ragionevolmente attendersi alcuna *privacy.*
Ma la Suprema Corte osserva che quello che Katz intendeva escludere, quando entrava nella cabina, non era l'occhio indiscreto, ma "l'orecchio non invitato". Egli non poteva aver perduto il suo diritto di farlo semplicemente perché aveva effettuato le chiamate da un luogo dove poteva essere visto.
L'individuo che entri in una cabina telefonica può contare sulla protezione del Quarto Emendamento, non meno di chi si trovi in un ufficio commerciale, nell'appartamento di un amico, o in un taxi. Colui che occupa la cabina telefonica, nel chiudersi la porta alle spalle per effettuare una telefonata, ha sicuramente il diritto di presumere che le parole che pronuncia nel telefono non saranno trasmesse al mondo. Interpretare la Costituzione in modo più restrittivo significherebbe ignorare il ruolo vitale che il telefono pubblico è arrivato a svolgere nella comunicazione privata.
In queste parole, risulta evidente che la Suprema Corte guarda alla *ratio* del Quarto Emendamento, che ha lo scopo di tutelare il privato, non inteso in senso materiale.
La Corte ritiene espressamente che il Quarto Emendamento disciplini non solo il sequestro di beni materiali, ma si debba estendere anche a registrazione ed ascolto di dichiarazioni orali: una volta riconosciuto questo, e una volta riconosciuto che il Quarto Emendamento protegge le persone – e non semplicemente "luoghi" [33] – da perquisizioni e sequestri illegittimi, è chiaro, secondo la Suprema Corte, che la portata di tale emendamento non può dipendere dalla presenza o dall'assenza di un'intrusione fisica in un determinato luogo.
La Corte conclude affermando che le attività della forza pubblica di ascoltare e registrare elettronicamente le parole o hanno violato la *privacy* su cui l'imputato *"ha legittimamente fatto affidamento*" durante l'utilizzo della cabina telefonica, e quindi hanno costituito una "*perquisizione e sequestro*" ai sensi del Quarto Emendamento. Il fatto che il dispositivo elettronico impiegato per raggiungere tale scopo non sia riuscito a penetrare la parete della cabina viene ritenuto irrilevante.
Con questa sentenza, la Suprema Corte introduce il concetto di "legittima aspettativa di *privacy*", che sussiste quando vi sono due requisiti: l'individuo deve aver dimostrato un'aspettativa (soggettiva) effettiva di *privacy* e, inoltre, tale aspettativa deve essere quella che la società è disposta a riconoscere come "ragionevole".
La casa di un uomo è, nella maggior parte dei casi, un luogo in cui si aspetta *privacy*, ma gli oggetti,

[33] "*The Fourth Amendment protects people, not places*".

le attività o le dichiarazioni che espone alla "semplice vista" degli estranei non sono "protetti", perché non si può rinvenire alcuna intenzione di tenerli per sé. Anche le conversazioni all'aperto non sarebbero protette dall'essere ascoltate, poiché non vi è alcuna aspettativa di *privacy* in tali circostanza. Nel caso di specie, il sig. Katz, nell'occupare la cabina telefonica, chiudendosi la porta alle spalle, sicuramente presumeva che la sua conversazione non potesse essere ascoltata: si trattava di un luogo temporaneamente privato, le cui aspettative di libertà da intrusione degli esterni sono riconosciute come ragionevoli.

Si evidenzia che i due requisiti del "test" sulla legittima aspettativa di *privacy* sono stati elaborati, in particolare, dal Giudice Harlan nella propria *concurring opinion.*

Egli osserva che è necessario estendere la tutela del Quarto Emendamento anche alle intrusioni immateriali della sfera privata, "*poiché le ragionevoli aspettative di privacy possono essere sconfitte dall'invasione elettronica oltre che fisica*".

Vediamo, dunque, che è l'innovazione tecnologica e il diffondersi delle nuove tecnologie a far sentire la necessità di una sempre maggior tutela della sfera privata dell'individuo: tuttavia, il diritto alla *privacy* continua ad essere dogmatizzato esclusivamente come diritto soggettivo dell'individuo.

3.3. Il caso Whalen v. Roe

Nel 1977 la Corte Suprema si trova a definire con maggior dettaglio il diritto alla *privacy*[34].

Viene impugnata una legge del 1972 dello Stato di New York, la quale, con l'intento di evitare il commercio illecito di medicinali pericolosi, prevedeva un sistema di registrazione delle prescrizioni mediche di tali prodotti. In particolare, si prevedeva che la prescrizione dovesse indicare il medico che l'aveva predisposta, la farmacia che aveva venduto il farmaco, con indicazione del dosaggio, nonché i dati anagrafici identificativi del paziente. Una copia di tale prescrizione doveva essere trasmessa e conservata presso il Dipartimento della Salute dello Stato, dove i dati venivano registrati su nastri per una elaborazione informatica. Tutti i moduli venivano conservati per cinque anni, nell'ambito di un sistema che ne salvaguardasse la sicurezza. La divulgazione pubblica dell'identità del paziente era, comunque, vietata, così come l'accesso ai file dei pazienti era limitato a un numero ristretto di medici e personale investigativo.

Alcuni pazienti avevano impugnato la legge, sostenendo che "il rapporto medico-paziente è una delle aree di tutela costituzionale della *privacy*" e che le disposizioni di identificazione del paziente della legge invadevano tale area.

La Suprema Corte osserva che quando si discute di tutela della *privacy* si fa riferimento a due

[34] Whalen v. Roe, 429 U.S. 599 (1977).

tipologie di interessi: il primo è l'interesse individuale ad evitare la divulgazione di questioni personali, il secondo è l'interesse all'indipendenza ad assumere decisioni importanti con riferimento alla propria salute.

Infatti, i pazienti divengono riluttanti a utilizzare determinati medicinali, e alcuni medici riluttanti a prescriverli, anche quando il loro uso sarebbe indicato dal punto di vista medico, proprio perché non voglio essere catalogati come assuntori di queste tipologie di farmaco. Ne consegue che l'assunzione di decisioni su questioni vitali per la salute è inevitabilmente influenzata da questa legge, che minaccia di compromettere sia l'interesse alla non divulgazione di informazioni private, sia l'interesse a prendere decisioni importanti in modo indipendente.

È la prima volta che la Suprema Corte riconosce che nel diritto alla *privacy* rientra anche la possibilità di escludere l'intrusione finalizzata a minare o, comunque, influenzare la volontà del soggetto e a deviarne le decisioni che egli compie.

La Corte afferma che vi sono almeno tre sfaccettature del diritto alla *privacy*:

- il diritto dell'individuo di essere libero nei suoi affari privati dalla sorveglianza e dall'intrusione del governo;
- il diritto di un individuo a non vedere i suoi affari privati resi pubblici dal governo;
- il diritto di un individuo di essere libero nell'azione, nel pensiero, nell'esperienza e nelle proprie credenze, libero dalla costrizione governativa.

È stato osservato[35] che con questa sentenza viene riconosciuto un contenuto più complesso e variegato del diritto alla *privacy*, in quanto ne viene evidenziata una duplice natura: la protezione dell'individuo dall'esterno, dalla curiosità del pubblico; la protezione dell'intimità verso l'esterno, ossia la formazione di una libera volontà.

4. L'approdo della *privacy* nella dottrina italiana

Quando il diritto alla riservatezza diviene oggetto dello studio della dottrina italiana, nell'area nordamericana la *privacy* era già riconosciuta pienamente in veste di diritto soggettivo dell'individuo. Peraltro, l'industrializzazione del periodo e lo sviluppo tecnologico stavano portando ad un ampliamento della nozione di *privacy*: negli anni '60 Westin focalizzerà la propria analisi proprio sul concetto di dato personale degli utenti, ponendolo in relazione all'archiviazione delle informazioni nei *data base* e alla facilità di trasmissione delle stesse tramite computer.

La prima dottrina italiana non si rifà, dunque, ad un concetto di diritto dei dati, ma sofferma la propria

[35] Sul punto, si veda P. MANES, *Il consenso al trattamento dei dati personali*, Cedam, 2001; anche S. RODOTÀ, *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione,* Laterza, 2005; ID, *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali,* in *Riv. crit. dir. priv.*, 1997.

analisi su concetti più ampi, quali riservatezza, diritto alla vita privata, diritto all'intimità personale, diritto alla sfera privata, diritto ad essere lasciati soli[36], nel tentativo di individuare i contenuti in relazione ai dati normativi vigenti.

Anche in Italia lo sviluppo di tali concetti è avvenuto grazie all'elaborazione dottrinale e giurisprudenziale, che hanno saputo cogliere le istanze sociali di tutela, sviluppatesi in relazione alla diffusione dei *mass media* e all'evoluzione di strumenti tecnologici per ricercare, immagazzinare, elaborare e diffondere le notizie: con l'avvento della "cultura informatica" degli anni '50, la tutela della vita privata ha assunto una dimensione totalmente nuova e più espansa.

Il formante dottrinale e giurisprudenziale è stato essenziale perché, per molti anni, il dato normativo è rimasto, al contrario, particolarmente sterile.

Peraltro, nella prima dottrina che si è occupata del tema, vi era piena consapevolezza del processo evolutivo che aveva portato il sistema nordamericano all'elaborazione della *privacy*: nei primi saggi italiani che si dedicano al tema, si fa sovente riferimento a questo nuovo diritto della personalità riconosciuto negli USA[37].

Le prime elaborazioni si sono, infatti, basate su alcune disposizioni che tutelano particolari tratti della personalità, la cui interpretazione è stata via via allargata a fattispecie più distanti dal dato normativo, attraverso l'interpretazione estensiva e il ricorso all'analogia. Anche il ricorso ai principi costituzionali è stato essenziale in questo percorso, perché ha portato alla costituzionalizzazione del diritto all'identità personale, corollario della libertà individuale, che si declina nella tutela di differenti interessi e posizioni soggettive che fanno capo alla persona.

Dopo questo passaggio evolutivo si è giunti (*infra* § 9), in epoca più moderna, a riconoscere il diritto alla protezione dei dati personali, così che specifiche disposizioni sono state predisposte a tutela del diritto al controllo di quelle informazioni personali che individuano la persona o tratti peculiari di essa (l. 675/1996, il Codice della *privacy* e, infine, il GDPR).

La prima dottrina che si è occupata della riservatezza[38] focalizza l'analisi su alcune disposizioni attorno alle quali nasce un vivo dibattito: ci si chiede, in estrema sintesi, se tali disposizioni tutelino ciascuna un interesse specifico o se esse presuppongono l'esistenza di un più ampio diritto alla sfera privata, di cui esse sono manifestazione.

---

[36] G. GIACOBBE, voce «*Riservatezza* (diritto alla)», in *Enc. dir.*, Giuffrè, 1989, pp. 1243 ss.

[37] G. GIAMPICCOLO, *La tutela giuridica della persona umana e il c.d. diritto alla riservatezza*, in *Riv. trim. dir. proc. civ.* 1958, p. 459; G. PUGLIESE, *Il preteso diritto alla riservatezza e le indiscrezioni cinematografiche*, in *Foro it.*, 1954, pp. 116 ss.

[38] A. RAVÀ, *Istituzioni di diritto privato,* Cedam, 1938, pp. 174 s. che afferma "*la qualità di persona richiede ed esige che alla persona stessa sia riservata una certa sfera relativa ai dati più gelosi e più intimi di essa e della sua attività* […] *da ciò deriva un generale diritto alla riservatezza che ha molteplici implicazioni*"; *cfr.* anche F. CARNELUTTI, *Il diritto alla vita privata,* in *Riv. trim. dir. pubbl.,* 1955, pp. 3-18.

Si tratta, in particolare, delle seguenti disposizioni:

- l'art. 10 c.c. ("Abuso dell'immagine altrui"), come integrato dagli artt. 96 e 97 l. 22.4.1941, n. 633, sulla protezione del diritto d'autore, che vieta di esporre e pubblicare l'immagine altrui, senza il consenso della persona raffigurata o dei suoi discendenti;
- gli artt. 10 e 24 l. 22.4.1941, n. 633, da cui si ricava il "diritto all'inedito";
- gli artt. 93-96 della medesima legge, che vietano la divulgazione di memorie personali e della corrispondenza senza il consenso dell'autore;
- gli artt. 616 e 622 c.p., che puniscono la rivelazione di corrispondenza e della conversazione telefonica, nonché la rivelazione di documenti segreti.

Com'è noto, il dibattito è sorto con riferimento ad alcune fattispecie specifiche arrivate all'attenzione dei tribunali: due film sulla vita del tenore Caruso, un romanzo a puntate sulla vita di Claretta Petacci e i suoi rapporti amorosi con Mussolini, un memoriale sulle vicende coniugali dell'attrice Myriam Petacci[39].

Va brevemente evidenziato che un primo orientamento dottrinale negava l'esistenza, nel nostro ordinamento del diritto alla riservatezza[40]. La tesi viene esposta quale critica alla sentenza 14.9.1953 del Tribunale di Roma, che si era trovato a stabilire: 1) se e in quali limiti, un'impresa cinematografica potesse rappresentare in un film la vita di un cantante celebre defunto (il tenore Caruso), senza aver ottenuto il consenso dei suoi discendenti; 2) quali fossero eventualmente i rimedi per questa illecita intrusione nella vita privata.

Il Tribunale aveva ritenuto, in primo luogo, che il nostro ordinamento riconosce, come attributo della personalità, il diritto alla riservatezza, che tollera deroghe in relazione a persone notorie e pubbliche, ma solo se l'invasione nella vita privata corrisponde ad un interesse pubblico; inoltre, l'aspetto della riservatezza viene collegato al diritto all'onore e alla reputazione, nel senso che non occorre il consenso dei discendenti all'opera cinematografica se la narrazione è giustificata da esigenze pubbliche di valutazione della personalità del soggetto notorio.

Ritenuti violati tali valori, il Tribunale commina una tutela di tipo inibitorio, condannando l'impresa a sopprimere le scene lesive della reputazione e dell'onore, riconosce inoltre il risarcimento dei danni morali, nonché dei danni patrimoniali derivanti dall'impossibilità per i discendenti, di cedere ad altri, dietro compenso, la facoltà di utilizzare i medesimi fatti per produrre un diverso film.

La sentenza[41] fa ampio riferimento al riconoscimento di un generale diritto alla riservatezza e

---

[39] G. GIAMPICCOLO, *op. cit.,* p. 459.

[40] G. PUGLIESE, *op. cit*.

[41] Sulla stessa vicenda vi era stata una precedente pronuncia del Pretore di Roma, che aveva negato il sequestro del film, non riconoscendo invece violata la riservatezza del cantante e dei suoi discendenti (tale sentenza è stata annotata da A. DE CUPIS, *Ancora in tema di offesa morale per mezzo della divulgazione cinematografica*, in *Foro it.*, 1952, I, p. 149).

l'affermazione è fortemente criticata da una parte della dottrina[42].

In particolare, Pugliese ritiene che le disposizioni in tema di utilizzo dell'immagine tutelino interessi specifici, sicché non possono essere l'indice della tutela di un più generale diritto alla riservatezza.

Nemmeno sarebbe corretto, secondo Pugliese, far riferimento alle norme sulla tutela della proprietà intellettuale, le quali tutelano la riservatezza solo nel senso che consentono all'individuo di elevare una barriera tra sé e i terzi, per custodire, al riparo da essa, opinioni e giudizi, sentimenti e passioni, fatti e vicende che la persona vuole tenere per sé. Perché la riservatezza sia tutelata, occorre che la persona si sia posta dietro questa barriera e che il terzo abbia violato la specifica disposizione che predispone il divieto di ingerenza. Tuttavia, se il terzo sia venuto a conoscenza di fatti della vita privata altrui senza violare dette norme, non può essere considerata illecita la divulgazione che ne abbia fatto[43]. Dal punto di vista del diritto positivo, non esiste una disposizione che riconosce espressamente il valore della riservatezza; inoltre, le norme citate, che tutelano alcuni aspetti della vita privata (come l'immagine) si pongono come norme eccezionali rispetto ai più generali principi di libertà di parola e di manifestazione del pensiero, con l'effetto che tali disposizioni non possono essere applicate ad altre fattispecie per il divieto di analogia previsto dall'art. 14 disp. preliminari.

Pugliese ne ricava che non possa ritenersi esistente alcun diritto soggettivo alla riservatezza.

Il ragionamento di Pugliese presenta notevoli simmetrie con la teoria proposta da Prosser, che, come abbiamo visto, scompone il diritto alla *privacy* in tanti interessi quante sono le disposizioni che tutelano specifici aspetti della vita umana.

5. Diritto alla personalità e riservatezza

Per definire il rapporto tra personalità e diritto alla protezione dati, è necessaria una breve premessa sulle due teorie, pluralista e monista, della personalità, perché in epoca moderna ne è stato proposto un ripensamento.

Secondo una prima concezione, detta pluralista, l'ordinamento non tutela un unico diritto della personalità, ma molteplici e differenti situazioni giuridiche soggettive, attraverso norme specificamente predisposte.

L'individuo è, dunque, tutelato nella misura in cui è possibile determinare distinte situazioni giuridiche meritevoli di tutela, ossia diversi diritti della personalità, espressamente disciplinati[44].

Questa concezione deve la sua prima elaborazione a De Cupis[45], secondo il quale, prima che

---

[42] *Ibidem.*

[43] G. PUGLIESE, *op. cit.*, p. 118.

[44] G. CHINÈ-A. ZOPPINI, *Manuale di diritto civile,* Neldiritto, 2018, p. 178.

[45] A. DE CUPIS, *I diritti della personalità*, nel *Trattato di diritto civile e commerciale*, IV, t. 1, diretto da A. CICU-F. MESSINEO, Giuffrè, 1959.

l'ordinamento riconosca tutela a posizioni giuridiche interiori dell'individuo, quest'ultimo non è ancora "persona" per l'ordinamento stesso e non può, dunque, avere alcun diritto. Il diritto alla personalità non esiste, semmai esiste un'aspirazione del soggetto ad essere riconosciuto come tale dall'ordinamento, ma si tratta di un'istanza che si colloca in un momento pre-giuridico e, pertanto, non riceve alcuna tutela oggettiva.

Con riferimento alla riservatezza, De Cupis riteneva che essa fosse "*quel modo d'essere della persona il quale consiste nella esclusione dalla altrui conoscenza di quanto ha riferimento alla persona medesima*"[46]. Proprio perché esclude che sussista un unico diritto alla personalità, egli si trova a dover individuare un fondamento normativo del diritto alla riservatezza. Sviluppa, dunque, un ragionamento che si basa, principalmente, sul diritto all'immagine e sulle sue limitazioni normative, per ricavare l'esistenza di un diritto alla riservatezza, che si esplicherebbe secondo differenti manifestazioni: ma appunto, è necessario che tali "manifestazioni" siano espressamente previste e tutelate da norme giuridiche, perché, in caso contrario, l'interesse alla riservatezza non è giuridicamente tutelato.

Nel 1958 Giampiccolo propone una teorizzazione dei diritti della personalità che ha, successivamente, incontrato il favore di giurisprudenza e dottrina ed è giunta sino ai giorni nostri.

Giampiccolo afferma che ogni persona ha un interesse alla privatezza, che attiene all'individualità personale: tale interesse riflette l'aspirazione del soggetto a conservare la tranquillità di spirito, la pace interiore. Nega, come invece aveva fatto Pugliese, che venga in rilievo in qualche modo la segretezza dei pensieri e degli scritti, imposta dal soggetto e tutelata da specifiche norme.

Si tratta, infatti, di una generale aspettativa della persona: in queste parole possiamo notare forti assonanze con quella dottrina nordamericana che elabora il test della ragionevole aspettativa di *privacy* del soggetto.

Tale aspettativa non è nemmeno relegata alla materialità dell'abitazione privata, né presuppone un l'isolamento volontario dal pubblico, in quanto non è una questione di ordine spaziale e materiale, ma si tratta di qualità della vita umana: un fatto che si svolga in un luogo pubblico può, comunque, appartenere all'intimità del soggetto.

L'autore nega che tale diritto alla riservatezza possa effettivamente essere ricondotto alle diverse disposizioni richiamate dalla dottrina per giustificarlo: è necessaria una norma specifica per ritenere meritevole di tutela giuridica un interesse socialmente apprezzabile della personalità?[47] Con riferimento alle diverse norme che vengono richiamate, osserva che queste non tutelano differenti diritti soggettivi dell'individuo. Non è corretto concepire la libertà personale e individuale come la somma delle varie attività consentite dall'ordinamento.

---

[46] A. DE CUPIS, *op. cit.*, p. 257.
[47] G. GIAMPICCOLO, *op. cit.*, p. 463.

La persona umana, infatti, è un valore unitario[48], sicché gli interessi dell'individuo possono essere isolati specificamente e, così, riconosciuti da specifiche disposizioni: tutte le singole norme sono espressione di un unico principio generale, che ne costituisce il denominatore comune. Si tratta dunque di specifiche disposizioni che tutelano tratti differenti di un medesimo diritto (il diritto alla personalità).

Non esistono, dunque, tanti autonomi diritti della personalità, esiste "il" diritto alla personalità, che è un "*diritto unico, a contenuto indefinito e vario, che non si identifica con la somma delle molteplici sue esplicazioni singolarmente protette da norme particolari*".

L'oggetto di tutela di tale diritto non sono, dunque, le specifiche e singole posizioni soggettive tutelate dalle diverse norme dell'ordinamento, ma è, invece, l'"*essere*" stesso della persona, senza necessità di individuare differenti beni giuridici esterni all'individuo. Non vale obiettare la mancanza di una formale diposizione di legge, che tuteli specificamente l'individuo: quest'ultimo è il presupposto stesso dei diritti fondamentali dell'uomo all'essere e alla libertà, tutelato dalla stessa Costituzione. Per tale ragione, qualsiasi elencazione di singoli diritti della personalità sarebbe sempre incompleta, perché il diritto alla personalità non si identifica con la mera somma dei diritti e delle libertà tutelati dall'ordinamento

Ebbene, da questa prospettiva, certamente l'ordinamento tutela anche la "*naturale aspirazione della persona al riserbo della vita privata*", che è un'esigenza di ciascuno, avvertita dalla coscienza sociale. Dunque, non è necessario verificare che l'intrusione nella sfera di riservatezza abbia, o meno, leso onore o reputazione, o altro valore dell'ordinamento: ciò che conta è la lesione della riservatezza e questa lesione trova certamente tutela nel tessuto delle norme.

Questa concezione contribuisce al processo di costituzionalizzazione del diritto alla personalità: la prospettiva del De Cupis, che presto diviene uniformemente accolta da dottrina e giurisprudenza, consente di "risalire all'art. 2 Cost. per documentare l'esigenza di integrale tutela della persona, che volta a volta si concreti nelle diverse forme necessarie per garantirne il libero svolgimento […]

L'art. 2 Cost. non è più una formula riassuntiva dei diversi diritti della persona costituzionalmente riconosciuti, ma una clausola generale attraverso la quale operare il continuo adeguamento delle garanzie giuridiche alle sempre nuove esigenze di tutela della persona"[49].

Com'è noto, l'elaborazione della teoria monista di Giampiccolo è stata successivamente accolta dalla dottrina e dalla giurisprudenza maggioritarie.

Ma è proprio in epoca moderna che, a seguito del riconoscimento del diritto alla protezione dati, la

---

[48] G. GIAMPICCOLO, *op. cit.*, p. 465.

[49] S. NIGER, *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, Cedam, 2006, p. 43.

teoria monista è stata messa in discussione.

È stato osservato[50], infatti, che la teoria pluralista dei diritti della personalità meglio si attaglia ad una realtà moderna, in cui taluni diritti della persona, come quello alla protezione dei dati, possono essere declinati all'interno di un negozio, per divenirne l'oggetto. La tesi monista, che postula l'indisponibilità assoluta della personalità, non consentirebbe, infatti, alcuna cessione a terzi dei dati personali.

6. Il riconoscimento della riservatezza nella giurisprudenza italiana

Il processo giurisprudenziale di riconoscimento del diritto alla riservatezza è stato alquanto travagliato: la prima giurisprudenza che si è confrontata sul tema ne ha negato rilevanza nell'ordinamento; successivamente, se n'è riconosciuta l'esistenza, fondando il diritto sulle disposizioni del codice civile che ne tutelano alcuni aspetti; successivamente, se n'è ancorata la *ratio* all'art. 2 Cost.; ancor in seguito, si è riconosciuto che all'interno della riservatezza rientra anche la tutela dei dati personali, in particolare il controllo ai dati.

Dunque, la prima giurisprudenza di legittimità che si è confrontata sul tema del diritto alla riservatezza, ne ha negato l'esistenza. Come ho evidenziato nella ricostruzione della teoria del Pugliese, il primo caso aveva ad oggetto i film biografici del tenore Caruso. Quando la vicenda giunge alla Corte di Cassazione, il Supremo collegio nega l'esistenza della riservatezza, affermando che la questione "*ben poteva trovare la sua soluzione, senza bisogno di inventare istituti nuovi, nel precetto generale del* neminen laedere*, come specificato per l'appunto nell'art. 2043 c.c*."[51]. Nel caso specifico, la Corte ritiene che, effettivamente, sia stato fatto un uso illecito dell'immagine del cantante, ma ritiene che tale illiceità possa essere sanzionata attraverso il ricorso alle norme che tutelano l'immagine. Afferma ancora la Corte che l'ordinamento non tutela specificamente la riservatezza, ma anzi pone alcuni diritti soggettivi della personalità, che, tuttavia, non possono essere estesi perché tali diritti si pongono come divieto o limitazione rispetto a diritti superiori (come il diritto di cronaca o la libertà di pensiero), dunque vige il divieto dell'analogia. Si tratta di un'applicazione giurisprudenziale della teoria del Pugliese e, infatti, la Corte ritiene che si può reagire al comportamento intrusivo solo qualora esso abbia leso l'onore, la reputazione, il decoro, perché questi solo sono i valori della persona tutelati dall'ordinamento.

Nel 1963 giunge all'attenzione della Corte il caso di Claretta Petacci[52]: un periodico aveva pubblicato un racconto a puntate della sua vita, nel quale vi erano chiari riferimenti alla sua relazione amorosa

---

[50] V. ZENO-ZENCOVICH, *I diritti della personalità*, *I, Le fonti e i soggetti*, a cura di N. LIPARI-P. RESCIGNO, Giuffrè, 2009.
[51] CASS., 22.12.1956, n. 4487, in *Riv. dir. ind.*, 1962, II.
[52] CASS., 20.4.1963, n. 990, in *Foro it.*, 1963, I, 877, p. 1298, con nota di A. DE CUPIS, *Riconoscimento sostanziale, ma non verbale, del diritto alla riservatezza*.

con Mussolini. La Corte supera l'orientamento previgente, affermando che "d*eve bensì riconoscersi che la personalità è il presupposto di diritti ma anche che essa* […] *postula un diritto di concretizzazione, cioè un diritto di libertà di autodeterminazione nei limiti consentiti dall'ordinamento, il quale come diritto assoluto, astratto si distingue dal potere di autonomia inerenti ai singoli concreti diritti e alle concrete manifestazioni*". Il fondamento di tale diritto alla personalità si trova nell'art. 2 Cost., il quale "*ammette un diritto di libera autodeterminazione nello svolgimento della personalità*"; con riferimento alla riservatezza, la Corte non ne riconosce l'esistenza, ma ne afferma la tutela nei limiti in cui venga violato il diritto assoluto di personalità inteso quale diritto alla libertà di autodeterminazione nello svolgimento della personalità dell'uomo come singolo. E questo diritto "*è violato se si divulgano notizie della vita privata, le quali, per loro natura, devono ritenersi riservate, a meno che non sussista un consenso implicito della persona, desunto dall'attività in concreto svolta o, data la natura dell'attività medesima e del fatto divulgato, non sussista un prevalente interesse pubblico di conoscenza", pertanto la violazione "della vita privata come fatto lesivo del diritto assoluto di personalità al libero svolgimento della stessa deve essere accertata con indagine da svolgersi, per singole fattispecie, sulla posizione del soggetto e sulla sussistenza di limiti, la cui inosservanza implichi illiceità e l'obbligo al risarcimento ai sensi dell'art. 2043 c.c*.".

Si trattava di un compromesso: dall'un lato la Corte esclude l'esistenza del diritto alla riservatezza, dall'altro lato, riconoscendo il diritto alla personalità e all'autodeterminazione, che ha anche rilevanza costituzionale, la Corte comunque tutela, indirettamente, anche la vita privata.

Il primo riconoscimento giurisprudenziale della riservatezza si deve ad una sentenza del 1973 della Corte costituzionale[53], in cui la Corte viene chiamata a pronunciarsi sulla legittimità costituzionale dell'art. 161 della legge 22.4.1941, n. 633, in quanto applicabile agli oggetti contenenti immagini che non siano state ancora pubblicate, ma che per essere nella materiale disponibilità di un'impresa giornalistica, si ritengano destinate alla pubblicazione, e dell'art. 700 c.p.c. in quanto applicabile ai medesimi oggetti.

La Corte riconosce il diritto alla riservatezza, in quanto afferma che tra i diritti inviolabili dell'uomo "*rientra quello del proprio decoro, del proprio onore, della propria rispettabilità, riservatezza, intimità e reputazione, sanciti espressamente nell'art. 8 e nell'art. 10 della Convenzione europea sui diritti dell'uomo, l'art. 10 c.c., nell'art. 96 e nell'art. 97 della legge 22 aprile 1941, n. 633*".

Due anni più tardi, il diritto alla riservatezza viene definitivamente riconosciuto anche dalla giurisprudenza di legittimità. Sul periodico "Gente" era apparso un servizio fotografico realizzato con teleobiettivo, in cui risultavano ripresi in vari atteggiamenti amorosi il regista Franco Indovina e la

[53] CORTE COST., 12.4.1973, n. 38.

principessa Soraya Esfandiari nell'interno della villa di quest'ultima. La principessa Esfandiari agiva contro l'editore, per violazione del domicilio, del diritto alla riservatezza e del diritto all'immagine con pregiudizio al decoro, onore e reputazione.

Con la sent. n. 38/1973 la Corte costituzionale afferma che l'ordinamento riconosce "*il diritto alla riservatezza, che consiste nella tutela di quelle situazioni e vicende strettamente personali e familiari le quali, anche se verificatesi fuori del domicilio domestico, non hanno per i terzi un interesse socialmente apprezzabile, contro le ingerenze che, sia pure compiute con mezzi leciti, per scopi non esclusivamente speculativi e senza offesa per l'onore, la reputazione o il decoro, non sono giustificati da interessi pubblici preminenti*".

Nella sentenza viene richiamato diffusamente il concetto di riservatezza, che s'identifica "*nelle formule che fanno riferimento ad una certa sfera della vita individuale e familiare, alla illesa intimità personale in certe manifestazioni della vita di relazione, a tutte quelle vicende, cioè, il cui carattere intimo è dato dal fatto che esse si svolgono in un domicilio ideale, non materialmente legato ai tradizionali rifugi della persona umana (le mura domestiche o la corrispondenza)*".

Con riferimento al suo fondamento normativo, la Corte afferma che l'art. 2 Cost. "*risulta violato dalla divulgazione di notizie della vita privata*", nel quale, infatti, rientra il "diritto *erga omnes* alla libertà di autodeterminazione".

Ulteriore fondamento è costituito dall'art. 3 Cost. sia perché, riconoscendosi la dignità sociale del cittadino, si rende necessaria una sfera di autonomia che garantisca tale dignità, sia in quanto rientrano nei limiti di fatto della libertà ed eguaglianza dei cittadini anche quelle menomazioni cagionate dalle indebite ingerenze altrui nella sfera di autonomia di ogni persona.

Peraltro, la Corte abbraccia una nozione particolarmente estesa di autonomia privata (entro cui "vive" la riservatezza), ricordando che differenti disposizioni della Costituzione descrivono uno spazio di autonomia entro cui l'individuo esercita la propria personalità. Questa sfera di autonomia dell'individuo si compone, innanzitutto, della libertà personale (art. 13), intesa questa in un senso più ampio della libertà meramente fisica. Inoltre, l'art. 29 – che sviluppa l'art. 2 – riconosce il carattere originario e l'inviolabile autonomia della famiglia, dunque la sfera di riservatezza dell'individuo include i legami famigliari. Questo perimetro individuale di riservatezza è tutelato specificamente da alcune intrusioni:

- l'art. 41, comma 2, Cost. prevede che l'iniziativa economica trova un limite nel rispetto della libertà e della dignità umana;
- l'art. 14 Cost., pone il limite della inviolabilità del domicilio, con riferimento alle ispezioni, alle perquisizioni, agli accertamenti per motivi pubblici;
- l'art. 15, tutela l'inviolabilità della libertà e della segretezza della corrispondenza;

- la presunzione di innocenza dell'imputato sino alla condanna definitiva ex art. 27 Cost., pone limiti alla diffusione di notizie sulle vicende dell'imputato e sui c.d. "retroscena" dei delitti.

La Corte evidenzia, inoltre, che la vita "privata" è tutelata da fonti internazionali, in particolare dalla Dichiarazione universale sui diritti dell'uomo (approvata il 10.12.1948 dall'ONU), e dal Patto internazionale relativo ai diritti civili e politici, approvato dall'Assemblea dell'ONU con risoluzione 16.12.1966, n. 2200. Infine, la riservatezza è riconosciuta dagli artt. 8 e 10, n. 2, della Convenzione europea per i diritti dell'uomo.

In merito a tale sentenza, Alpa ha osservato che "*si supera la concezione proprietaria di riservatezza, si pongono limiti al diritto di cronaca, si ammette che anche le persone notorie hanno diritto alla tutela*"; osserva, tuttavia, che sebbene non si metta più in discussione il riconoscimento del diritto alla riservatezza, "*nel disegnarne i limiti i suoi confini rimangono incerti. Sinteticamente, questi limiti riguardano questioni di* status*, di graduatoria di diritti, tipi di danno*"[54].

7. Il successivo sviluppo tecnologico e le nuove istanze di tutela della *privacy*. I dati personali

Come abbiamo visto, la *privacy* viene essenzialmente riconosciuta come diritto soggettivo individuale. Nasce come diritto di ogni persona di escludere dalla propria sfera privata gli altri consociati (es. la stampa) e, successivamente, viene anche riconosciuta la tutela dalle intrusioni della forza pubblica (es. le intercettazioni telefoniche).

Questa seconda prospettiva viene in particolare approfondita da Alan. F Westin, nella propria monografia *Privacy and Freedom* del 1967[55].

Westin nelle prime pagine riafferma gli aspetti tradizionali della *privacy*, osservando che tale diritto garantisce agli individui e ai gruppi la possibilità di conservare spazi di autonomia, momenti di autovalutazione solitaria e di comunicazione protetta.

Dagli anni '40 si assiste ad una nuova epoca dello sviluppo tecnologico, che modifica profondamente le istanze sociali di tutela della *privacy*: Westin evidenzia questi nuovi sviluppi e propone un modello di analisi riferito alla società statunitense, ma i cui tratti salienti possono essere estesi anche all'evoluzione tecnologica che, alcuni anni più tardi, conoscerà l'Europa e l'Italia.

La sua Opera è suddivisa in quattro parti: 1) le funzioni della *privacy* e la sorveglianza nella società; 2) la descrizione dei progressi nelle tecnologie di sorveglianza; 3) l'analisi di cinque casi per spiegare le risposte dell'ordinamento alle nuove tecnologie; 4) prospettive legislative per risolvere il conflitto *privacy*/sorveglianza

---

[54] G. ALPA, *Diritto della responsabilità civile,* Laterza, 2003, p. 234.

[55] A. F. WESTIN, *Privacy and Freedom*, Atheneum New York, 1967. Westin è stato professore emerito di diritto pubblico e governo alla Columbia University, nonché editore di *Privacy & American Business*. È considerato uno dei più importanti studiosi della *privacy* e del diritto dei dati.

L'autore schematizza l'esistenza di sei specifici mutamenti sociali e tecnologici che hanno portato la circolazione dei dati ad evolversi in modo esponenziale; da queste tecnologie deriva il concreto rischio di illecite intrusioni nella sfera personale[56].

1. L'espansione generale della raccolta di informazioni e della conservazione dei dati nella società. Poiché il sistema industrializzato è divenuto più complesso, le funzioni di regolamentazione del governo sono aumentate, le grandi organizzazioni burocratiche sono diventate il modello nel settore privato e le scienze sociali si sono impegnate pesantemente nella raccolta e nell'analisi dei dati, la società moderna è divenuta la società della "produzione dei dati".
2. L'aumento della mobilità delle persone e la standardizzazione della vita nella società di massa hanno portato allo sviluppo di grandi sistemi investigativi privati e governativi la cui funzione è l'accumulo dei fascicoli personali su decine di milioni di persone.
3. La raccolta di informazioni generali e di fascicoli sono stati radicalmente accelerati dall'avvento del computer, con la sua capacità di archiviare più documenti e manipolarli in modo più efficace e rapido di quanto fosse mai possibile prima.
4. Lo sviluppo di molti nuovi programmi pubblici ha prodotto una richiesta di maggiori dati personali degli individui che in passato[57].
5. L'evoluzione dei computer ha accelerato rapidamente la condivisione dei dati tra chi utilizza le macchine. La standardizzazione dei linguaggi dei computer e la perfezione delle macchine che traducono un linguaggio macchina in un altro hanno permesso la diretta comunicazione tra gli stessi, così che i dati possono fluire tra sistemi separati. Tale innovazione ha portato, inoltre, allo scambio di informazioni tra le unità di una stessa grande organizzazione, come ad esempio le agenzie di polizia o della salute in uno stato, o tra organizzazioni indipendenti con interessi comuni, come le compagnie assicurative sulla vita.
6. Il processo automatico dei dati gradualmente sta rimpiazzando molte delle operazioni in contanti del passato, comportando un aumento dei documenti riguardanti le significative operazioni della vita dell'individuo.

Egli sposta l'analisi dal concetto di mera riservatezza, da diritto ad essere lasciati soli, da diritto alla vita privata, ad una nuova prospettiva, che pone l'accento sulla concezione di "dati personali".
Si tratta di una teoria destinata a mutare per sempre lo studio delle discipline dei dati.

---

[56] Peraltro, egli teorizza, oltre ad una sorveglianza di tipo fisico, una sorveglianza "psicologica", introdotta da quelle macchine che consentono di verificare se un soggetto sta affermando il falso, nonché una sorveglianza "dei dati" (raccolta ed elaborazione di informazioni nelle banche dati informatiche): v. *infra* cap. II.

[57] Westin prede come esempio il *Civil Right Acts* del 1964, che esige che l'ufficio per il censimento ottenga informazioni sulla registrazione personale dell'elettore; la disciplina sui datori di lavoro impone che debbano tenere e dare al governo i dati razziali dei dipendenti per dimostrare la loro adeguatezza con la legislazione in materia di pari opportunità, così come lo devono fare le scuole per provare l'integrazione scolastica.

8. Gli elaboratori elettronici

Anche nell'orizzonte italiano, la dottrina studia attentamente – alcuni anni più tardi – la "*sindrome da elaboratore elettronico*", il quale consente una "*possibilità praticamente illimitata di raccolta delle informazioni personali da parte di istituzioni pubbliche e private; accesso rapidissimo all'intero complesso delle informazioni raccolte, grazie al loro trattamento a mezzo di elaborati elettronici; elevata circolazione delle informazioni*"[58].

L'uso dell'elaboratore consente una raccolta di dati di dimensioni che prima non erano pensabili; le informazioni vengono raccolte in dossiers informatici occupando spazi infinitesimali. Inoltre, esso permette una gestione economica delle informazioni, che possono essere catalogate con specifici programmi di raccolta, consentendo, successivamente, di rivendere tali dati. L'elaboratore consente inoltre la completezza dell'informazione, perché nel catalogare i dati, è in grado di restituire un profilo aggregato delle informazioni che riguardano un utente specifico. L'informazione diviene, dunque, "organizzata": i dati, presi singolarmente, non avrebbero alcun valore, essendo al contrario l'aggregazione sistematica ed ordinata degli stessi che determina la creazione di nuovi valori, anche commerciali, degli stessi.

Come osservato da Rodotà, in Italia questo fenomeno viene inizialmente percepito quando viene reso noto, nel 1971, il progetto di istituzione di un'anagrafe tributaria e in occasione del censimento generale della popolazione[59].

Tuttavia, già era diffuso in Italia l'impiego degli elaboratori elettronici da parte della pubblica amministrazione, come strumenti di organizzazione e conservazione dei dati personali[60]. In dottrina è stato osservato che gli elaboratori hanno determinato un "*dominio sociale sull'individuo: il potere informatico*", che viene descritto come "*un potere per certi aspetti occulto e misterioso, ma onnipresente; un potere che, anziché accrescere la capacità di azione dell'individuo, la può mortificare incidendo sulla sua stessa vita di relazione*"[61].

Si sviluppano, dunque, nuove "dimensioni" della *privacy*, perché si percepisce l'impossibilità di considerare la questione solo nella direttrice del bilanciamento tra riservatezza e divulgazione, tra

---

[58] S. RODOTÀ, *Elaboratori elettronici e controllo sociale*, Il Mulino, 1973, p. 10; si v., anche, ID., *La privacy tra individuo e collettività*, in *Politica del diritto*, 1974; ID., *Tecnologie e diritti*, Il Mulino, 1995; ID., *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione,* Laterza, 2005; nonché V. FROSINI, *Teoria e tecnica dei diritti umani: i diritti umani nella società tecnologica*, Editori Riuniti, 1993; ID, *Tecnologie e libertà costituzionali*, in *Dir. inf. e inform.*, 2003.

[59] RODOTÀ, *Elaboratori elettronici*, cit., p. 17.

[60] Rodotà prende ad esempio lo "*schedario dei catturandi dell'arma dei Carabinieri, gli schedari della Direzione Generale Polizia; il ricorso all'elaboratore, presso diversi Ministeri, per la gestione del personale* […] *già oggi esiste una possibilità di utilizzazione congiunta di informazioni raccolte nel settore fiscale e in quello delle assicurazioni sociali*".

[61] E. GIANNANTONIO-M. G. LOSANO-V. ZENO-ZENCOVICH, *La tutela dei dati personali. Commentario alla l. 675/1996*, Cedam, 1997, p. 6.

l'uomo prigioniero dei suoi segreti e l'uomo che non ha nulla da nascondere, tra intimità della vita privata e scena pubblica[62].

La sensibilità per i nuovi rischi connessi alla raccolta dei dati e alla loro organizzazione, sposta il tema della *privacy*, vengono, dunque, "*in primo piano le modalità di esercizio del potere da parte dei detentori pubblici e privati delle informazioni*" e la *privacy* supera "*il tradizionale quadro individualistico e si dilata in una dimensione collettiva, dal momento che non viene più in considerazione solo l'interesse del singolo in quanto tale, ma in quanto appartenente ad un determinato gruppo sociale*"[63].

Rodotà evidenzia questi mutamenti e ammonisce sulla necessità di non rimanere relegati ad una concezione meramente individualistica della *privacy,* impostazione che trascura l'emersione del "*momento collettivo e del controllo del potere*", connessi all'utilizzo dei dati personali degli utenti.

In realtà, è proprio la dogmatizzazione meramente individualistica della *privacy* che viene presa in esame e tipizzata dal legislatore italiano ed europeo che ha successivamente codificato la materia.

Rodotà riconosce la necessità di attribuire agli individui un "potere di controllo" sui dati personali; il problema si sposta, dunque, dalla segretezza delle informazioni, al controllo dei dati. Il problema diviene l'individuazione del tipo di controllo che dovrebbe riconoscersi.

L'autore auspica la creazione di strumenti di controllo anche sociale dei dati, che non limitino la tutela degli stessi al solo ambito giusprivatistico, ritenuto insufficiente per tutelare i dati nella nuova era dell'*information technology*.

Questa nuove istanze sociali, derivanti dai mutamenti tecnologici, hanno dunque affermato la necessità per gli ordinamenti di apprestare specifiche tutele per i dati personali. Dal diritto alla riservatezza si è, dunque, determinato il concetto di "riservatezza informatica", ossia la possibilità di escludere gli altri dall'uso dei propri dati personali, concezione che poi si è evoluta ed espansa sino a riconoscere un diritto all'autodeterminazione informatica.

In Europa la questione del trattamento dei dati attraverso gli elaborati elettronici era particolarmente rilevante e avvertita dalla cultura giuridica, perché tali tecnologie avevano permesso agli Stati autoritari del '900 di svolgere attività di controllo e di discriminazione delle popolari.

Il regime nazista era dotato di un apparato tecnologico di ultima generazione, grazie alla collaborazione tra la Germania e alcune imprese statunitensi, quali IBM. Il governo nazista aveva utilizzato tali elaboratori per svolgere trattamenti automatizzati al fine di individuare e sorvegliare le persone di religione ebraica. Numerosi atti persecutori furono compiuti dal regime grazie a queste

---

[62] S. RODOTÀ, *La privacy tra individuo e collettività*, cit., p. 547.
[63] *Ibidem*, p. 551.

tecnologie[64].

È per tale ragione che nell'ambito europeo si sviluppano due differenti concezioni di *privacy*, entrambe riconducibili alla personalità individuale:

- il diritto di ciascuno di non subire interferenze nella propria vita privata e intima, che si sviluppa in particolare in relazione alla libertà di espressione e di stampa (in questa prima veste viene riconosciuto anche nell'ordinamento italiano);
- il diritto di ciascuno di controllare i propri dati, che nasce originariamente per evitare le discriminazioni fondate sui trattamenti automatizzati.

La *data protection* viene dunque a qualificarsi come un diritto fondamentale dell'individuo, che rientra all'interno del "prisma" del diritto alla *privacy*. Questa concezione spiega anche l'evoluzione successiva della disciplina e giunge sino ai nostri giorni: il tema del consenso all'utilizzo dei dati dimostra che la *data protection* è stata "costruita" principalmente come rimedio per l'individuo. Il Regolamento sposta l'attenzione dall'individuo agli obblighi che gravano sul titolare, per responsabilizzarlo. Ma la concezione originaria non è del tutto superata.

Va tuttavia evidenziato che un diverso orientamento, espresso in particolare a livello transazionale, ritiene che il diritto alla *privacy* e la *data protection* debbano essere tenute del tutto distinti[65], in quanto solo la privacy sarebbe un diritto, mentre la *data protection* sarebbe solo una legislazione finalizzata a proteggere i cittadini da alcune nuove tecnologie. Si afferma che "*privacy has a substance, data protection has none. It is just a series of proportionality tests aiming to protect citizens from harms stemming from a specific set of technologies and operations. As it happens, these harms are also afforded a protection under the right to privacy, so overlaps between the two rights are bound to happen and may even result with different legal outcomes. This, however, is not the point. The point is that data protection can be understood and described from the perspective of risk regulation, and that analyses building upon conceptual categories coming from the right to privacy are, to some extent, a mischaracterization of data protection*"[66].

---

[64] F. PIZZETTI, *op. cit.*, pag. 54; E. BLACK, *L'IBM e l'olocausto. I rapporti fra il Terzo Reich e una grande azienda americana*, Rizzoli, 2001.

[65] R. M. GELLERT, *Understanding data protection as risk regulation* in *Journal of Internet Law*, 2015, pp. 3-15; ID., *Data protection: a risk regulation? Between the risk management of everything and the precautionary alternative*, in *International Data Privacy Law*, 2015, Vol. 5, No. 1, pp. 3-17.

[66] R.M. GELLERT, *op. ult. cit.*, p. 11, secondo cui "…*instead of being associated with Article 7 of the Charter, it 'should rather be associated with the right to environmental protection' (Article 37)*" e, infatti, l'autore evidenzia che anche la disciplina sulla protezione dell'ambiente si basa sul controllo e sulla gestione dei rischi ambientali e per la salute umana e, infatti, si tratta di una disciplina che prevede specifici meccanismi e procedure per gestire scientificamente e tecnologicamente i tali rischi, ad esempio attraverso le valutazioni d'impatto ambientale, connotate da evidenti elementi di somiglianza con la valutazione d'impatto prevista dal GDPR.

9. Il diritto alla protezione dati nel contesto europeo

Sebbene gli Stati europei avessero conosciuto gli effetti devastanti del nazismo e del totalitarismo, ancora non vi era, nel periodo post-bellico, una cultura della tecnologia sufficientemente avanzata per riconoscere e rendere autonomo il diritto alla protezione dati.

Questo è testimoniato dal fatto che nessuna delle Costituzioni adottate dopo la Seconda Guerra Mondiale prevede un simile diritto: esse fanno riferimento ai tradizionali concetti di famiglia, di vita privata, ma il diritto alla protezione dei dati non era ritenuto una posizione giuridica soggettiva sufficientemente concettualizzata.

È stato osservato, inoltre, che se dall'un lato l'Europa aveva conosciuto gli effetti devastanti della tecnologia in mano al nazismo, dall'altro lato le banche dati e gli elaboratori furono utili strumenti per individuare i collaborazionisti e i membri dei governi nazisti e fascisti[67].

È questa la ragione per cui anche la Convenzione europea dei diritti dell'uomo non considera il diritto alla protezione dei dati, ma enuclea solamente il diritto al rispetto della vita privata e familiare, del domicilio e della corrispondenza (art. 8).

Solo successivamente alcuni Stati nazionali iniziarono ad approvare leggi[68] a tutela del diritto dei dati e così fece anche il Consiglio d'Europa con la Convenzione 28.1.1981, n. 108 sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale (ratificata in Italia con l. n. 98/1989).

Lo scopo della Convenzione era di estendere la protezione dei diritti e delle libertà fondamentali di ciascuno, in particolare il diritto al rispetto della vita privata, tenendo conto dell'intensificazione della circolazione attraverso le frontiere di dati a carattere personale oggetto di elaborazioni automatizzate, riaffermando, al contempo, l'impegno a tutelare la libertà di informazione: si trattava, dunque, di individuare un bilanciamento tra i valori fondamentali del rispetto della vita privata e della libera circolazione dell'informazione tra i popoli[69]. La Convezione aveva preso atto della nuova esigenza di tutela della persona a fronte del crescente impiego degli strumenti della tecnologica informatica, idonei a schedare la generalità dei cittadini per le più svariate finalità di controllo e di sfruttamento[70].

La Convenzione anticipa definizioni (come quella di dato personale e di trattamento automatizzato),

---

[67] F. PIZZETTI, *op. cit.*, p. 57.

[68] Nel 1970 veniva approvata in Francia una legge che riconosceva, per la prima volta, il "*droit a la vie privèe*"; tale legge veniva successivamente modificata dalla l. 6.1.1978, n. 17, la quale istituiva la *Commission Nationale de l'Informatique et des Libertes* (CNIL). Nello stesso anno, inoltre, una legge del Land dell'Assia introduceva il divieto di schedature di massa e regolamentava il trattamento dei dati personali attraverso banche dati. Nel 1977, anche la Germania si dotava di una legge per la protezione dei dati personali. La prima legge per la protezione dei dai personali in UK veniva approvata solo nel 1984 (*Data Protection Act*).

[69] Preambolo Convenzione 28.1.1981, n. 108.

[70] C. M. BIANCA-F. D. BUSNELLI, *La protezione dei dati personali. Commentario al D.Lgs. 30 giugno 2003, n. 196*, Cedam, 2007.

criteri di legittimità del trattamento (principio di raccolta legittima e corretta, registrazione per scopo determinato, esattezza, pertinenza, conservazione per tempo non superiore al necessario), diritti (conoscere l'esistenza di una banca dati che conservi i propri dati, rettifica, cancellazione), che saranno poi destinati ad entrare nelle legislazioni di tutti gli Stati europei e negli atti successivamente adottati dall'Unione.

Con la Convenzione viene sancito il limite per gli Stati di raccogliere arbitrariamente i dati delle persone, così da evitare la possibilità per gli individui di essere discriminati.

Soltanto in data 24.10.1995, il Parlamento europeo e il Consiglio adottano un atto legislativo a tutela dei dati personali: la Direttiva 95/46 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, che ha per oggetto "*la tutela dei diritti e delle libertà fondamentali delle persone fisiche e particolarmente del diritto alla vita privata, con riguardo al trattamento dei dati personali*" (art. 1)[71].

La Direttiva ha avuto un effetto fondamentale, quello di gettare le basi, all'interno dell'Unione Europea, di un mercato digitale libero per lo scambio dei dati. Essa afferma, infatti, il principio del riconoscimento reciproco della legittimità del trattamento: un titolare effettua un trattamento lecito dei dati personali se si conforma alla normativa dello Stato in cui risiede, anche se vi è scambio di dati tra due paesi europei.

Cadono le frontiere interne per la circolazione dei dati, che si spostano, invece, ai confini dell'Europa.

Viene ampliata la nozione di "trattamento dei dati": mentre il primo testo della Convezione 108 si applicava solo ai trattamenti "automatizzati", la Direttiva introduce una nozione ampia, includendo qualsiasi tipo di operazione – o complesso di operazioni – che abbia ad oggetto i dati personali[72].

In tema di responsabilità, l'art. 23 della Direttiva indicava agli Stati di disporre che "*chiunque subisca un danno cagionato da un trattamento illecito o da qualsiasi altro atto incompatibile con le disposizioni nazionali di attuazione della Direttiva abbia il diritto di ottenere il risarcimento del pregiudizio subito dal responsabile del trattamento*".

La Direttiva non dettava alcun criterio a cui gli Stati dovevano conformarsi per l'attuazione in tema di responsabilità. In assenza di parametri di riferimento, ogni Stato ha adottato provvedimenti legislativi di diversa portata per la tutela dei dati personali e l'obiettivo dell'armonizzazione non è

---

[71] Si v. anche, il considerando n. 10 che recita "*le legislazioni nazionali relative al trattamento dei dati personali hanno lo scopo di garantire il rispetto dei diritti e delle libertà fondamentali, in particolare del diritto alla vita privata, riconosciuto anche dall'articolo 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali e dai principi generali del diritto comunitario*".

[72] L'art. 2 lett. b) della Direttiva definisce il "*trattamento dei dati" come "qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali, come la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione o la modifica, l'estrazione, la consultazione, l'impiego, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, nonché il congelamento, la cancellazione o la distruzione*".

stato raggiunto, perché gli Stati adottano sistemi di responsabilità civile anche molto distanti tra di loro, in particolar modo con riferimento all'onere della prova a carico del danneggiato, danni concretamente risarcibili, ai metodi di quantificazione degli stessi.

Successivamente, il Trattato sul funzionamento dell'Unione affermerà che il diritto alla protezione dei dati è un diritto fondamentale degli individui: viene cristallizzato nell'art. 16, secondo cui "*ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano*".

Analoga formulazione è contenuta nell'art. 7 della Carta dei diritti fondamentali dell'Unione Europea.

10. Prime leggi italiane sulla tutela dei dati personali

In Italia, in data 31.12.1996, veniva approvata la l. n. 675, sulla "tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali".

Si tratta di una delle poche leggi di diritto privato posta espressamente a tutela della persona, nel senso che tutela espressamente i diritti della personalità, come risulta dall'*incipit* dell'art. 1, che prevede che lo scopo della legge è di garantire che il trattamento dei dati personali si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale.

Secondo la dottrina che per prima ha commentato la legge, sarebbe un equivoco ritenere che l'art. 1 l. n. 675/1996 intendesse riconoscere legislativamente i diritti della personalità di creazione giurisprudenziale, come la riservatezza e l'identità personale, in quanto "*la legge introduce e disciplina un diritto sui propri dati personali, diverso dai tradizionali diritti della personalità*"[73]. Da questa prospettiva, i diritti all'onore, all'identità personale e alla riservatezza hanno ad oggetto la proiezione sociale dell'individuo ma non direttamente la protezione dei dati personali, i quali ultimi diventano rilevanti solo nella misura in cui, dalla loro diffusione e comunicazione, derivi una violazione dei valori della personalità.

La legge n. 675/1996 tutela, invece, direttamente i dati personali, indipendentemente dalla loro diffusione e dal fatto che dalla comunicazione a terzi derivi una violazione per l'onore o la riservatezza del soggetto. Essa non ha quale finalità la tutela del "prestigio sociale" della persona, ma la libertà rispetto al potere informativo e al potere della persona di controllo sui propri dati[74].

V'è da evidenziare, comunque, che la l. n. 675/1996 non offre una statuizione netta del "diritto alla protezione dei dati", preferendo "*individuare i singoli diritti di accesso, di rettifica e di controllo che compongono e costituiscono il nuovo diritto e ne sono alla base*"[75].

---

[73] E. GIANNANTONIO-M. G. LOSANO-V. ZENO-ZENCOVICH, *op. cit.*, p. 5.
[74] *Ibidem.*
[75] G. FINOCCHIARO, *Privacy e protezione dei dati. Disciplina e strumenti operativi*, Zanichelli, 2012, p. 2.

Comunque, l'importanza della Dir. 95/46 e della l. n. 675/1996 è di aver apprestato un primo sistema di tutela per i dati personali, il cui utilizzo era diventato ormai diffuso nella società. Tuttavia, traspare dalla Direttiva un concetto statico di trattamento dei dati, in cui lo scambio degli stessi avviene esclusivamente tra interessato e titolare del trattamento[76]. Tale impostazione deriva dalla tecnologia dell'epoca che coinvolgeva i dati personali, ossia, in particolare, gli elaboratori elettronici e le banche dati.

Il diritto alla protezione dei dati viene espressamente sancito con il successivo d.lgs. 30.6.2003, n. 196 (Codice per la protezione dei dati personali), che all'art. 1 afferma "*chiunque ha diritto alla protezione dei dati personali che lo riguardano*".

Com'è stato autorevolmente affermato "*il diritto alla protezione dei dati personali consiste nel diritto del soggetto cui i dati si riferiscono di esercitare un controllo, anche attivo, su detti dati, che si estende dall'accesso alla rettifica*", in particolare esso identifica "*il diritto di un soggetto di controllare l'insieme delle informazioni che alla medesima si riferiscono e che quindi costituiscono il suo riflesso e delineano lo stesso suo essere nella società dell'informazione*" [77].

Pochi giorni prima dell'entrata in vigore del Codice della *privacy*, Rodotà – allora Presidente dell'Autorità garante per la protezione dei dati personali – osservava che "*È nata una nuova concezione integrale della persona, alla cui proiezione nel mondo corrisponde il forte diritto di non perdere mai il potere di mantenere il pieno controllo sul proprio "corpo elettronico", distribuito in molteplici banche dati, nei luoghi più diversi*"[78].

Si tratta di un diritto ad oggetto particolarmente ampio, come conseguenza della stessa definizione di dato personale data dal Codice della *privacy*, secondo cui è dato personale "*qualunque informazioni relativa a persona fisica identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale*".

11. Rapporto tra diritto alla protezione dati e riservatezza

Numerose elaborazioni dottrinali sono state sviluppate sul rapporto tra diritto alla protezione dei dati personali, dall'un lato, e diritto alla riservatezza dall'altro[79].

---

[76] G. FINOCCHIARO, *Il quadro d'insieme sul Regolamento europeo*, in *La protezione dei dati personali in Italia,* diretto da G. FINOCCHIARO, Zanichelli, 2019, p. 19.

[77] *Ibidem.*

[78] S. RODOTÀ, *Relazione 2002*, 20.5.2003; sul tema si v. anche R. PARDOLESI, *Diritto alla riservatezza e circolazione dei dati personali*, Giuffrè, 2003.

[79] G. FINOCCHIARO, *op. cit.*; E. GIANNANTONIO-M. G. LOSANO-V. ZENO-ZENCOVICH, *op. cit.*; F. CARDARELLI-S. SICA-V. ZENO-ZENCOVICH, *Il codice dei dati personali. Temi e problemi*, Giuffrè, 2004; P. PALLARO, *Libertà della persona e trattamento dei dati personali nell'Unione Europea*, Giuffrè, 2002; G. BUTTARELLI, *Banche dati e tutela della riservatezza*, Giuffrè, 1997, pp. 103 ss.; E. TOSI, *Responsabilità civile per illecito trattamento dei dati personali e danno*

Come abbiamo visto, il concetto di protezione dei dati è stato individuato sviluppando la concezione di riservatezza personale, dal quale è venuto successivamente ad emarginarsi.
Entrambi i concetti rientrano – insieme al diritto all'identità personale (digitale) – nella più ampia situazione giuridica soggettiva definitiva quale diritto alla *privacy*.
Tuttavia, differente è il fondamento normativo di questi due diritti e il loro oggetto.
Con riferimento alla Carta dei diritti fondamentali dell'UE, il diritto alla protezione dei dati personali è previsto all'art. 8 (rubricato "Protezione dei dati di carattere personale"), il quale stabilisce che "*ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica*".
Il diritto alla riservatezza trova, invece, riconoscimento all'art. 7 (rubricato "Rispetto della vita privata e della vita familiare"), secondo cui "*Ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni*".
Il diritto alla protezione dei dati è, dunque, il diritto all'autodeterminazione informativa, il diritto dell'individuo a mantenere il controllo dei dati che lo riguardano e identificano: è la libertà di ogni soggetto di autodefinirsi e autodeterminarsi[80].
Come emerso dalla ricostruzione storica, il diritto alla riservatezza è, invece, il diritto a non subire intrusioni ed interferenze nella propria sfera di vita privata e nella propria intimità.
Anche il diritto alla protezione dei dati personali rientra tra i diritti della personalità, in quanto esso esplica la "*difesa dell'individuo nei confronti del potere informatico, l'habeas corpus della moderna era cibernetica*"[81].

12. Rapporto tra diritto alla protezione dati e identità personale (digitale)

L'identità personale[82] è un diritto di matrice prettamente giurisprudenziale che ha numerosi punti di contatto con il diritto alla riservatezza.
Com'è noto, l'identità personale è concetto sviluppato nella storica sentenza n. 3769/1985 della

non patrimoniale, Giuffrè, 2019; G. ALPA, *La disciplina dei dati personali. Note esegetiche sulla Legge 31 dicembre 1996, n. 675 e successive modifiche,* Seam, 1998; G. M. RICCIO-G. SCORZA- E. BELISARIO, *GDPR e normativa privacy,* Cedam, 2018.
[80] G. BUTTARELLI, *op. cit.,* p. 103.
[81] E. GIANNANTONIO-M. G. LOSANO-V. ZENO-ZENCOVICH, *op. cit*., p. 7.
[82] Sul tema dell'identità personale e della sua successiva evoluzione come identità personale "digitale", *cfr.* G. ALPA, *L'identità digitale e la tutela della persona,* in *Contr. e impr.*, 2017, pp. 723 ss.; G. FINOCCHIARO, voce «*Identità personale* (diritto alla)», in *Digesto, Disc. priv. sez. civ.*, 2010, pp. 721 ss.; A. SCALISI, *Il diritto alla riservatezza*, Giuffrè, 2002, pp. 179 ss.

Cassazione[83], secondo cui "*ciascun soggetto ha interesse, ritenuto generalmente meritevole di tutela giuridica, di essere rappresentato, nella vita di relazione, con la sua vera identità, così come questa nella realtà sociale, generale o particolare, è conosciuta o poteva essere conosciuta con l'applicazione dei criteri della normale diligenza e della buona fede soggettive*"; si tratta del diritto dell'individuo "*a non vedersi all'esterno alterato, travisato, offuscato, contestato il proprio patrimonio intellettuale, politico, sociale, religioso, ideologico, professionale, ecc. quale si era estrinsecato od appariva, in base a circostanze concrete ed univoche, destinato ad estrinsecarsi nell'ambiente sociale*".

Il diritto all'identità personale si è sviluppato, negli ultimi anni, in una sua veste anche informatica: si tratta del diritto di autodeterminazione informativa digitale, ossia quel diritto a vedere tutelata la proiezione digitale del sé, la rappresentazione che l'individuo ha di sé stesso sul *web*, sulle piattaforme digitali, sui *social network.* Dev'essere inteso secondo un'accezione ampia, volta a ricomprendere tutto il "complesso di dati, informazioni, attività che servono non solo ad individuare ma a rappresentare compiutamente la storia personale di un dato soggetto, la persona stessa come emergente dai dati personali più svariati che la compongono in una dimensione tendenzialmente omnicomprensiva[84].

Mentre il diritto al nome e all'immagine identificano le persone da un punto di vista fisico-materiale, nella citata sentenza la Cassazione rileva che l'identità personale identifica la persona nella complessità e globalità delle sue specifiche caratteristiche e manifestazioni esteriori e sociali; si tratta della proiezione dell'effettiva personalità della persona.

Dunque, ancorché vi sia una stretta correlazione tra diritto al nome e all'immagine (nonché agli altri segni distintivi ex artt. 6 ss. c.c.) e il diritto all'identità personale, queste posizioni soggettive non coincidono e non può esservi alcuna immedesimazione tra le stesse.

Inoltre, mentre il diritto al nome e all'immagine tutelano l'individuo nella sua staticità, l'identità personale è un concetto mutevole e dinamico, che comprende tutti quei dati materiali e non dalla cui composizione si ricava la personalità dell'individuo, il suo essere soggetto di diritto. Così inteso, il diritto all'identità riceve la tutela costituzionale dell'art. 2, il cui scopo è proprio quello di tutelare l'individuo in ogni suo modo d'essere[85].

Evidentemente, il diritto alla protezione dei dati personali e quello all'identità personale si possono

---

[83] CASS., 22.6.1985, n. 3769, in *Foro it.*, 1985, I, p. 2211. Tale diritto era stato, in realtà, elaborato in precedenza nella sentenza PRET. ROMA, 6.5.1974, in *Giur. it.*, 1975, I, p. 514, secondo cui l'identità personale "*è il diritto a non vedersi travisare la propria personalità individuale*".

[84] E. TOSI, *op. cit.*, pp. 18-19.

[85] *Ibidem*, p. 20, dove peraltro l'a. afferma, per meglio definire i confini dell'identità personale, che "*nell'illecito relativo all'identità personale la lesione riguarda il principio di verità; nell'illecito relativo alla reputazione riguarda il principio di valore*".

intersecare. All'interno della protezione dei dati rientrano vari diritti che possono essere funzionali alla tutela dell'identità personale, come ad esempio il diritto alla correzione dei dati, alla limitazione dei dati, alla cancellazione dei dati, all'oblio dei dati.

L'esercizio di questi diritti, che rientrano prettamente nell'ambito della *data protection*, garantisce anche la corretta rappresentazione e proiezione digitali dell'individuo: attraverso il loro esercizio la persona può evitare o rimuovere il travisamento e l'alterazione della sua immagine personale.

Per comprendere l'importanza del fenomeno dell'identità personale digitale, che viene a costituire un vero e proprio frammento della personalità, non può non evidenziarsi la questione della successione *mortis causa* dell'"eredità digitale", venuta recentemente all'attenzione della dottrina[86] e della giurisprudenza[87]. Quest'ultima ha affermato che "*il legislatore nell'ottica della tutela dei diritti alla dignità ed all'autodeterminazione (diritti che riguardano sia la dimensione fisica della persona che quella che attiene al rapporto con i dati personali che esprimono e realizzano una parte dell'identità della persona stessa) ha espressamente valorizzato l'autonomia dell'individuo, lasciandogli la scelta se lasciare agli eredi ed ai superstiti legittimati la facoltà di accedere ai propri dati personali (ed esercitare tutti o parte dei diritti connessi) oppure sottrarre all'accesso dei terzi tali informazioni*". Affermazioni, dunque, che dimostrano la massima attualità del dibattito attorno al diritto all'identità personale digitale.

13. Responsabilità per illecito trattamento nel Codice della *privacy* (rinvio)

L'art. 15 del Codice della privacy prevedeva[88] che "*chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento del danno ai sensi dell'art. 2050 c.c.*".

Se il risarcimento per illecito trattamento dei dati soggiacesse alla regola dell'art. 2043, il danneggiato dovrebbe provare tutti gli elementi costitutivi dell'illecito[89]. Invece, grazie al rinvio operato all'art. 2050 c.c., il danneggiato dovrà provare esclusivamente l'evento lesivo, il danno (nell'*an* e nel *quantum*, ma anche in via presuntivo/equitativa) e che tra questi due elementi sussiste un nesso di causalità giuridica, ma non l'elemento soggettivo del fatto illecito.

Peraltro, a seguito del rinvio all'art. 2050 c.c. operato da questa disposizione, è sorto un dibattito in dottrina sulla possibilità, o meno, di qualificare come "pericolosa" l'attività di trattamento dei dati personali. La soluzione più corretta sembra quella per cui il legislatore ha voluto rinviare

---

[86] M. TAMPIERI, *Il patrimonio digitale oltre la vita: - quale destino?*, in *Contr. e impr.*, 2021, pp. 543 ss.; A. ZACCARIA, *La successione* mortis causa *nei diritti di disporre di dati personali digitalizzati*, in *Studium Iuris*, 2020, pp. 1368 ss.; M. CINQUE, *L'"eredità digitale" alla prova delle riforme*, in *Riv. dir. civ.*, 2020, pp. 72 ss.

[87] TRIB. MILANO, 10.2.2021, in *Corr. giur.*, 2021, pp. 658 ss., con nota di A. MANIACI-A. D'ARMINIO MONFORTE, *La prima decisione italiana in tema di "eredità digitale": quale tutela post mortem dei dati personali?*

[88] L'art. 15 d.lgs. n. 196/2003 è stato abrogato espressamente dal decreto di coordinamento (d.lgs. n. 101/2018) della normativa italiana al GDPR.

[89] Secondo il principio generale per cui chi avanza una pretesa deve dare la prova del suo fondamento.

esclusivamente al regime della prova liberatoria di cui all'art. 2050 c.c. e non ha, invece, voluto qualificare come pericolosa l'attività di trattamento dei dati[90].

Dunque, lo scopo del rinvio sarebbe stato quello di armonizzare la disciplina nazionale con la Dir. 95/46, che all'art. 23 prevedeva, quale prova liberatoria della responsabilità, che "*il responsabile del trattamento può essere esonerato in tutto o in parte da tale responsabilità se prova che l'evento dannoso non gli è imputabile*".

Com'è noto, attorno alla natura della responsabilità da attività pericolosa ex art. 2050 c.c. si sono formati due differenti orientamenti[91]: il primo che la qualifica come "responsabilità oggettiva", il secondo come responsabilità per colpa ma "aggravata". Si tratta di un dibattito che involge, nello specifico, la questione del contenuto della prova liberatoria del danneggiante e, evidentemente, il rinvio operato dall'art. 15 Codice della *privacy* ha l'effetto di portare all'interno della materia dei dati personali la medesima questione.

Interpretando la disposizione dell'art. 2050 c.c. come un'ipotesi di responsabilità di tipo oggettivo, la responsabilità del danneggiante sarebbe esclusa solo dalla prova del caso fortuito o dalla forza maggiore[92].

Al contrario, qualificando tale responsabilità come aggravata[93], si giunge a ritenere prevista una mera inversione dell'onere della prova, nel senso che il danneggiante potrebbe liberarsi dalla responsabilità provando di aver adottato tutte le misure idonee ad evitare l'evento.

Il secondo comma dell'art. 15 prevede, inoltre, l'espressa risarcibilità del danno non patrimoniale, nel caso in cui il trattamento sia stata posto in essere violando i principi posti dall'art. 11 del medesimo Codice[94].

Sul tema del danno non patrimoniale, va ricordato che dal 2003 la Cassazione[95] ha sostenuto un'interpretazione costituzionalmente orientata dell'art. 2059 c.c. che ha portato a ricomprendere, nell'ambito applicativo della norma, il danno morale soggettivo, il danno biologico, nonché "ogni

---

[90] Si tratta, comunque, di una qualificazione che non ha effetti sulla disciplina applicata.

[91] Su questo dibattito, si vedano i rinvii contenuti in E. TOSI, *op. cit.*, pp. 31-32; F. GRITTI, *La responsabilità civile nel trattamenti dei dati personali*, in *Il codice del trattamento dei dati personali*, a cura di CUFFARO-R. D'ORAZIO-V. RICCIUTO, Giappichelli, 2007, p. 161; A. FUSARO, *Attività pericolose e dintorni. Nuove applicazioni dell'art. 2050 c.c*., in *Riv. dir. civ*., 2013, p. 1137.

[92] Propende per questa soluzione M. FRANZONI, *Responsabilità derivante da trattamento dei dati personali,* in *Diritto dell'informatica*, a cura di G. FINOCCHIARO-F. DELFINI, Utet, 2014, pp. 831 ss.;

[93] Questa è la soluzione recentemente affermata da CASS., 7.5.2017, n. 16637; nello stesso senso C. M. BIANCA, *Diritto civile*, 5, *La responsabilità*, Giuffrè, 2012, p. 709.

[94] L'art. 11 poneva i principi del trattamento, secondo cui i dati devono essere: a) trattati in modo lecito e secondo correttezza; b) raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi; c) esatti e, se necessario, aggiornati; d) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati; e) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

[95] CASS., 31.5.2003, nn. 8827 e 8828.

danno derivante dalla lesione di diritti e interessi inerenti della persona di rango costituzionale" (artt. 2, 29, 30 Cost.). Ciò comporta, di conseguenza, la risarcibilità anche dei danni derivanti dalla lesione del diritto alla protezione dati, rendendo superflua l'espressa previsione legislativa.

Con riferimento al danno non patrimoniale per illecito trattamento dati, la Cassazione si è attestata su una posizione che rende assai arduo il concreto ottenimento del risarcimento da parte del danneggiato. In particolare, la Corte ha enunciato il principio di diritto secondo cui il danno non patrimoniale risarcibile, ai sensi del art. 15 d.lgs. n. 196 del 2003, pur determinato da una lesione del diritto fondamentale alla protezione dei dati personali tutelato dagli artt. 2 e 21 Cost. e dall'art. 8 CEDU, "*non si sottrae alla verifica della "gravità della lesione" e della "serietà del danno" (cd. "doppio filtro" del risarcimento del danno), in quanto anche per tale diritto opera il bilanciamento con il principio di solidarietà ex art. 2 Cost., da cui deriva (come intrinseco precipitato) quello di tolleranza della lesione minima e, sicché determina una lesione ingiustificabile del diritto non la mera violazione delle prescrizioni poste dall'art. 11 del codice della privacy, ma solo quella che ne offenda in modo sensibile la sua portata effettiva, restando comunque il relativo accertamento di fatto rimesso al giudice di merito*" [96].

14. Il Regolamento europeo per la protezione dei dati

A seguito dei mutamenti tecnologici intervenuti negli anni 2000-2015, si è resa necessaria l'adozione, da parte dell'UE, di una nuova disciplina della protezione dei dati, che considerasse il mutato contesto tecnologico e sociale e che superasse l'impianto della Dir. 95/46, la quale ruotava attorno all'idea di un singolo scambio di dati, tra l'interessato e il titolare che poi li conservava.

Il 25.5.2016 viene approvato il Reg. UE 2016/675 (che abroga la Dir. 95/46), divenuto esecutivo negli Stati europei il 25.5.2018, il quale ha avuto il compito di fornire una risposta legislativa al nuovo mercato digitale europeo, nel quale i flussi di dati sono cresciuti esponenzialmente, come sono cresciuti i monopoli di alcune *Big Companies* nel settore.

Il Regolamento muta radicalmente la prospettiva da cui viene affrontato il tema della protezione dei

---

[96] CASS., 26.4.2021, n. 11020; CASS., 20.8.2020, n. 17383. La Cassazione ha anche affermato che il danno alla *privacy*, pur non essendo, come ogni danno non patrimoniale, in "*re ipsa*", non identificandosi il danno risarcibile con la lesione dell'interesse tutelato dall'ordinamento, ma con le conseguenze di tale lesione, "*può essere, tuttavia, provato anche attraverso presunzioni*" (CASS., 26.10.2017, n. 25420).

Si registrano, tuttavia, anche precedenti non del tutto conformi. Recentemente la Cassazione ha affermato, infatti, che la fattispecie delineata dai due commi del d.lgs. n. 196 del 2003, art. 15, pone due presunzioni:

1) quella secondo la quale il danno è da addebitare a chi ha trattato i dati personali o a chi si è avvalso di un altrui trattamento a meno che egli non dimostri di avere adottato tutte le misure idonee per evitarlo ai sensi dell'art. 2050 c.c.;

2) quella secondo la quale le conseguenze non patrimoniali di tale danno – sia esso di natura contrattuale che extracontrattuale – sono da considerare *in re ipsa* a meno che il danneggiante non dimostri che esse non vi sono state ovvero che si tratta di un danno irrilevante o bagatellare ovvero ancora che il danneggiato abbia tratto vantaggio dalla pubblicazione dei dati (CASS., 4.6.2018, n. 14242).

dati.

Mentre la Direttiva previgente (e il Codice della *privacy*) era focalizzato sui diritti dell'interessato, il Regolamento sposta l'attenzione sui soggetti (titolare, co-titolare, responsabile) che trattano tali dati. Infatti, impone nuovi obblighi, soprattutto di tipo strutturale e organizzativo, che devono essere osservati dai soggetti depositari dei dati: esso muove chiaramente dall'idea secondo cui, onde evitare trattamenti illeciti, sia necessaria un'organizzazione efficiente della struttura aziendale dell'impresa, permeata da misure di sicurezza tecnologiche e organizzative, tra cui una rete di controlli interni, con l'individuazione di specifiche figure della società (come il DPO) che hanno il compito di vegliare sui trattamenti effettuati dalla società stessa. Quest'organizzazione interna ha il compito di verificare costantemente, in modo dinamico, la continua armonizzazione della struttura aziendale ai principi e alle regole del GDPR (ciò che viene definito come *privacy compliance*).

Più nello specifico, il GDPR ruota attorno al principio della *accountability* del titolare del trattamento, come risulta dalla formulazione dell'art. 5, che al par. 1 detta i principi del lecito trattamento dei dati[97] e al par. 2 affida al titolare il compito del rispetto del par. 1 (principio della "responsabilizzazione")[98]. Il titolare viene individuato nel soggetto che dev'essere in grado di porre in essere tutte le misure tecniche e organizzative adeguate per garantire che il trattamento dei dati sia sempre lecito; inoltre, deve poter documentare all'Autorità garante tale attività in ogni momento.

Il titolare viene obbligato, prima di tutto, a svolgere un'analisi delle procedure interne ed esterne all'impresa che coinvolgono il trattamento di dati personali (mappatura dei trattamenti), individuando

---

[97] I dati personali sono:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);
b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»);
c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);
d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);
e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);
f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

[98] Sull'*accountability*, si v. G. FINOCCHIARO, *Privacy e protezione dei dati personali. Disciplina e strumenti operativi*, Zanichelli, 2012, pp. 289 ss.; ID., *Introduzione al regolamento europeo sulla protezione dei dati*, in *Nuove leggi civ. comm*., 2017, p. 10; C. BISTOLFI, *Le obbligazioni di* compliance *in materia di protezione dei dati personali*, in *Il regolamento privacy europeo, Commentario alla nuova disciplina sulla protezione dei dati personali*, a cura di L. BOLOGNINI-E. PELINO-C. BISTOLFI, Giuffrè, 2016, p. 321; F. DI CIOMMO, *Civiltà tecnologica, mercato e insicurezza: la responsabilità del diritto*, in *Riv. crit. dir. priv*., 2010, p. 590.

i profili di rischio che ogni operazione potrebbe comportare, e deve documentare questa "valutazione del rischio *privacy*" attraverso elenchi e registri che vengono aggiornati costantemente.

Deve, inoltre, dimostrare di aver predisposto le misure tecniche e organizzative (art. 24 GDPR) idonee a prevenire i rischi individuati (ad es. l'accesso riservato e registrato ai locali in cui vengono conservati i dati, *firewall*, password). Le misure organizzative devono essere calibrate sulla specifica realtà dell'impresa a cui si riferiscono, a seconda della "grandezza" della realtà aziendale e delle specifiche tipologie di trattamenti effettuati. È lo stesso titolare che deve impegnarsi proattivamente per verificare quale sia lo strumento più adeguato per garantire il lecito trattamento dei dati e deve dimostrare di svolgere costantemente questa auto-verifica[99].

In questo contesto, muta anche il valore che viene attribuito al consenso dell'interessato al trattamento dei dati. La Direttiva e il Codice della *privacy* ponevano tutta l'attenzione alla fase dell'informativa e del consenso, per la visione prettamente individualista del diritto dei dati e per il fatto che il trattamento era generalmente limitato ad una relazione biunivoca tra interessato e titolare. Con il GDPR il consenso rimane presupposto per il trattamento, ma il giudizio di legittimità si sposta sul rispetto, da parte del titolare, dei principi di precauzione e responsabilità in relazione al trattamento dei dati.

D'altronde, da tempo è stato evidenziato che un corretto sistema della protezione dei dati personali non può essere focalizzato esclusivamente su una logica meramente consensuale del diritto[100]. Numerose sono, in tal senso, le ammonizioni della dottrina; in relazione al GDPR è stato affermato che "*resta il grande tema ancora irrisolto: esiste un modello alternativo a quello incentrato sul consenso? Certamente non può soddisfare un sistema basato su un consenso che spesso è vuoto di effettivo significato, perché prestato nell'inconsapevolezza o nell'assenza di alternative praticabili. Si tratta di un modello, sotto il profilo, teorico, centrato sull'autodeterminazione, che tuttavia spesso manca dei presupposti sui quali dovrebbe basarsi*"[101].

Infatti, con l'avvento delle tecnologie moderne, l'utente non è sempre in grado di comprendere effettivamente l'uso che viene fatto dei suoi dati personali: le numerose informative *privacy* e *cookies* che compaiono sui siti web, ad esempio, illustrano in modo estremamente complesso il funzionamento delle tecnologie utilizzate e, per comprenderle, l'utente dovrebbe impiegare molto

---

[99] Ad esempio, vi saranno enormi fabbriche con migliaia di dipendenti, che in realtà trattano solo i dati di questi ultimi e la trasmissione all'esterno dei dati ai dipendenti avviene solo per esigenze di contabilità, in cui il rischio *privacy* sarà molto basso; o piccole *start up*, che detengono enormi masse di dati, svolgono complesse procedure di profilazione per cedere ulteriori servizi a terzi sul mercato: in quest'ipotesi, sarà necessario un forte atteggiamento *risk approach.*

[100] S. RODOTÀ, *Elaboratori elettronici*, op. cit.

[101] G. FINOCCHIARO, *Il quadro d'insieme sul Regolamento europeo*, in *La protezione dei dati personali in Italia*, diretto da G. FINOCCHIARO, Zanichelli, 2019, p. 8; F. GRITTI, *La responsabilità civile nel trattamenti dei dati personali ,* in *Il codice del trattamento dei dati personali*, a cura di V. CUFFARO-R. D'ORAZIO-V. RICCIUTO, Giappichelli, 2007, p. 129.

tempo. Inoltre, è un dato di fatto che i beni e i servizi più moderni sono sviluppati e programmati – anche laddove questo non sarebbe necessario – in modo da poter offrire tutte le proprie funzionalità solo qualora l'utente decida di cedere l'utilizzo dei propri dati personali. La cessione e il consenso alla successiva riutilizzazione di tali dati sono, dunque, obbligati: l'utente non è nella posizione di esprimere un consenso effettivo[102].

15. L'art. 82 GDPR. Cenni

In continuità con il previgente art. 15 Codice della *privacy*, l'art. 82 GDPR (rubricato "Diritto al risarcimento e responsabilità") prevede che "*chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento*".

La disposizione differenzia la posizione del soggetto danneggiante, perché, mentre il titolare "*risponde per il danno cagionato dal suo trattamento che violi il presente regolamento*", il responsabile "*risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento*".

In ossequio al principio secondo cui rispondono solidalmente tra di loro tutti i soggetti che abbiano concorso alla causazione dell'evento dannoso, il par. 4 dell'art. 82 prevede che "*ogni titolare del trattamento o responsabile del trattamento è responsabile in solido per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dell'interessato*".

Pertanto, nei rapporti esterni, ossia tra interessato e danneggianti, questi ultimi rispondono per l'intero: è fatto salvo che, nei rapporti interni, colui il quale abbia pagato l'intero debito possa rivalersi nei confronti degli altri danneggianti per ottenere, a titolo di regresso, il pagamento delle quote di spettanza, determinate dal Giudice. Infatti, il par. 5 prevede che "*qualora un titolare del trattamento*

---

[102] Sul tema del consenso, in data 4.5.2020, il Comitato Europeo per la Protezione dei Dati (European Data Protection Board - EDPB) ha rilasciato le nuove *Guidelines On Consent under Regulation 2016/679 n. 05/2020*. Le Linee Guida dell'EDPB modificano e integrano quelle già adottate il 28.11.2017 ed aggiornate il 10.4.2018 (dall'allora WP29).
Secondo le Linee guida, la manifestazione di volontà deve essere "libera", nel senso che l'interessato deve avere una scelta effettiva e il controllo sui propri dati. Il consenso non viene considerato validamente prestato, se l'interessato non dispone di una scelta effettiva o si sente obbligato ad acconsentire oppure subisce conseguenze negative se non acconsente. Se il consenso è un elemento non negoziabile delle condizioni generali di contratto/servizio, secondo le Linee guida si presume che non sia stato prestato liberamente. Le Linee guida prendono in considerazione anche la fattispecie di squilibrio di potere tra titolare del trattamento e interessato. Nel valutare se il consenso sia stato prestato liberamente, si deve anche tener conto dell'eventualità che il consenso sia collegato all'esecuzione di un contratto o alla prestazione di un servizio. Ad es. un'applicazione mobile per il fotoritocco chiede agli utenti di attivare la localizzazione GPS per l'utilizzo dei suoi servizi. L'applicazione comunica agli utenti che utilizzerà i dati raccolti per finalità di pubblicità comportamentale. Né la geolocalizzazione né la pubblicità comportamentale online sono necessarie per la prestazione del servizio di fotoritocco e vanno oltre la fornitura del servizio principale. Poiché gli utenti non possono utilizzare l'applicazione senza acconsentire a tali finalità, il consenso non può essere considerato liberamente espresso (esempio riportato dalle Linee guida).

o un responsabile del trattamento abbia pagato, conformemente al paragrafo 4, l'intero risarcimento del danno, tale titolare del trattamento o responsabile del trattamento ha il diritto di reclamare dagli altri titolari del trattamento o responsabili del trattamento coinvolti nello stesso trattamento la parte del risarcimento corrispondente alla loro parte di responsabilità per il danno conformemente alle condizioni di cui al paragrafo 2".

Il par. 3 prevede il regime della prova liberatoria: "*il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità, a norma del paragrafo 2 se dimostra che l'evento dannoso non gli è in alcun modo imputabile*".

Si tratta di una formulazione che si discosta da quella adottata dal Codice previgente, che richiamava l'adozione di "*tutte le misure idonee ad evitare l'evento*" di cui all'art. 2050 c.c.

Tuttavia, da una prima lettura emerge, evidentemente, la natura oggettiva della responsabilità per illecito trattamento dei dati personali.

Sul tema, il sistema di tutela introdotto dal nuovo Regolamento – che, come abbiamo visto, focalizza l'attenzione sulle misure di precauzione e prevenzione del rischio da parte del titolare – è mosso dall'intenzione di individuare il soggetto che può avere il controllo del trattamento (titolare, co-titolare, responsabile), per attribuire allo stesso la responsabilità per i danni conseguenti al risarcimento, secondo una logica di "allocazione dei rischi". In sostanza, si guarda al soggetto che può rispondere del danno, perché ne ha la capacità economica, nonché al soggetto che ricava un guadagno da quell'attività o prodotto tecnologicamente avanzato che può determinare un danno agli utenti.

16. Natura anche patrimoniale del diritto alla protezione dei dati

Dall'analisi compiuta sino a qui, emerge inequivocabilmente che il tema della protezione dei dati viene ricondotto, dalla dottrina e giurisprudenza maggioritarie, nell'ambito dei diritti della personalità.

Si può evidenziare che la teoria monista dell'unico diritto della personalità sembra essere messa in discussione a seguito del riconoscimento del diritto alla protezione dei dati e all'autodeterminazione digitale. La dottrina moderna che ha affrontato tali temi tende, infatti, a ricercare specifici interessi protetti dal diritto dei dati che sembrerebbero fuoriuscire dal diritto alla personalità come tradizionalmente inteso.

Ma che si tratti di abbracciare ancora la tesi monista, ovvero di riconoscere una dimensione pluralista della personalità, le conclusioni sulla natura del diritto alla protezione dei dati non vengono modificate. Nella sostanza, il diritto dei dati è ricondotto prettamente alla dimensione personale-

individuale: esso è inteso esclusivamente come diritto della personalità[103].

Questo lo si ricava anche dalla qualificazione che la dottrina ha fornito del consenso per il trattamento dei dati[104], che è stato inquadrato in una prospettiva non contrattuale, per rimanere confinato nell'ambito delle esimenti per escludere l'illiceità del trattamento[105], ovvero di natura meramente autorizzatoria[106].

Le ragioni di tale impostazione risiedono nella stessa storia evolutiva che ha portato all'affermazione del diritto dei dati, il quale, come abbiamo visto, è stato originariamente enucleato nell'ambito del diritto alla *privacy*, sicché i due termini (*privacy* e protezione dei dati) sono stati per lungo tempo ritenuti quasi fungibili[107]. In realtà, abbiamo visto che non v'è piena coincidenza di concetti, ben potendosi profilare situazioni in cui la lesione della *privacy* non derivi da trattamenti illeciti di dati personali: questo perché i beni giuridici tutelati dai due diritti non sono identici.

Proprio perché il diritto alla protezione dei dati viene originariamente concepito nell'ambito della *privacy* dall'esperienza statunitense, in questa veste esso giunge allo studio della nostra dottrina, la quale, conseguentemente, lo riconduce nell'alveo dei diritti della personalità, negandone ogni aspetto patrimoniale.

Anche quando venne approvata la l. n. 675/1996, la dottrina italiana interpretava il diritto dei dati come un diritto che tutela aspetti meramente morali, interiori, immateriali dell'individuo: nessun cenno al fenomeno dei dati personali quale circolazione di ricchezza.

Tale assunto è confermato anche dalle recenti prese di posizione, sul punto, del Garante europeo per la protezione dei dati personali. In un parere del 17.3.2017[108], l'Autorità europea, pur riconoscendo (non senza evidenti contraddizioni) l'esistenza di un mercato dei dati personali nei quali essi sono economicamente oggetto di controprestazione nell'ambito di operazioni di scambio di beni e servizi

---

[103] Per un'analisi approfondita in ambito europeo, si v. Y. HERMSTRUWER, *Contracting Around Privacy: The (Behavioral) Law and Economics of Consent and Big Data*, in *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 2017, p. 9, all'indirizzo https://www.jipitec.eu/issues/jipitec-8-1-2017/4529.

[104] V. RICCIUTO, *Il contratto ed i nuovi fenomeni patrimoniali: il caso della circolazione dei dati personali*, in *Riv. dir. civ.*, 2020, p. 648;

[105] G. COMANDÈ, *Commento all'art. 11, l. n. 675/ 1996*, in *La tutela dei dati personali. Commentario alla l. 675/1996*, a cura di E. GIANNANTONIO-M.G. LOSANO-V. ZENO-ZENCOVICH, Cedam 1997, p. 102; D. MESSINETTI, *Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali*, in *Riv. crit. dir. priv.*, 1998, pp. 350 ss.

[106] S. SICA, *Il consenso al trattamento dei dati personali: metodi e modelli di qualificazione giuridica*, in *Riv. dir. civ.*, 2001, pp. 621 ss. Sul punto, si veda P. MANES, *Il consenso al trattamento dei dati personali*, Cedam, 2001, p. 37, secondo il quale "*l'attività dispositiva consta di due diverse fasi: la prima, relativa al soggetto, consente che il terzo sfrutti l'utilità ed è necessariamente un atto unilaterale di natura concessoria che ha lo scopo di rendere lecita l'attività altrui; la seconda, ha invece natura contrattuale e riguarda la concreta esecuzione dell'attività del terzo*".

[107] V. RICCIUTO, *Il contratto ed i nuovi fenomeni patrimoniali: il caso della circolazione dei dati personali*, cit., pp. 642 ss.; A. L. ALLEN, *Privacy-as-Data Control: Conceptual, Practical, and Moral Limits of the Paradigm*, in *Connecticut Law Review*, 2000, pp. 861 ss.; S. RODOTÀ, *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali,* in *Riv. crit. dir. priv.*, 1997, pp. 588-589.

[108] EDPS, Opinion 4/2017, all'indirizzo www.dps.europa.eu.

compiute dai consumatori[109], ha osservato che "*frasi popolari come "valuta digitale" e "pagare con i dati" potrebbero non solo essere fuorvianti, ma possono anche essere pericolose, se prese alla lettera e trasformate in un principio giuridico*".

Analoga posizione ha espresso il Garante italiano, che, nella Relazione sull'attività svolta nell'anno 2020[110], ha affermato che "*la* zero price economy *ha reso prassi ordinaria lo schema negoziale "servizi contro dati"; riconoscere la possibilità della remunerazione del consenso rischia di determinare una rifeudalizzazione dei rapporti sociali, ammettendo che si possa pagare con i propri dati e, quindi, con la propria libertà. Su questo "pendio scivoloso" è in gioco, forse più che in ogni altro campo, l'identità europea come "Comunità di diritto", fondata sulla sinergia tra libertà, dignità, eguaglianza, quali presidi essenziali che nessuna ragion di Stato o, tantomeno, di mercato può violare*"[111].

Sennonché, la concezione prettamente individualistica del diritto alla protezione dei dati offre il fianco a talune obiezioni.

Innanzitutto, questa prospettiva non considera che esiste un mercato digitale, all'interno del quale i dati personali vengono negoziati: vi sono società di notevoli dimensioni, sia in America che in Europa, il cui *core business* è proprio l'estrazione e la trasformazione dei dati personali. In questo contesto, i dati personali vengono ceduti dagli utenti quale corrispettivo per la controprestazione, ossia il servizio acquistato dall'utente.

Dunque, il fenomeno della negoziazione e della patrimonializzazione dei dati esiste, è realtà e, soprattutto, è tenuto in stretta osservazione dal legislatore europeo. Si veda l'art. 1 GDPR, che prevede "*1. Il presente regolamento stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati.* […] *La libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali*".

Pertanto, il legislatore europeo considera la libera circolazione dei dati come uno degli obbiettivi dell'UE, cui tende il GDPR stesso.

Nel settore dei servizi digitali, la Dir. UE 2019/770 20.5.2019, relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali, il cui art. 3, par. 1 considera quale oggetto di disciplina: *i*) i contratti con cui un operatore economico fornisce, o si impegna a fornire,

---

[109] V. RICCIUTO, *op. cit.*, p. 654.

[110] AUTORITÀ GARANTE PER LA PROTEZIONE DEI DATI, *Relazione 2020*, p. 12.

[111] Il Garante per la protezione dei dati personali italiano ha recentemente investito il Garante europeo sulla questione della commerciabilità dei dati personali, relativamente alla società Weople, che svolge attività di acquisizione di dati personali dagli interessati in cambio di corrispettivo, dati che vengono poi ricollocati venduti a terzi. La società opera nel mercato digitale quale "intermediaria nel rapporto tra aziende e utenti" dei quali gestisce i dati personali consentendo loro di lucrare sul valore del dato.

un bene o un servizio digitale dietro corrispettivo di un prezzo; *ii*) i contratti con cui l'operatore economico fornisce o si impegna a fornire contenuto digitale o un servizio digitale al consumatore e il consumatore fornisce o si impegna a fornire dati personali all'operatore economico. Il fenomeno della patrimonializzazione dei dati personali non può, dunque, essere ancora ignorato.

In secondo luogo, negare il valore patrimoniale dei dati e la loro commerciabilità, significherebbe rendere nulli tutti i contratti che prevedono la cessione dei dati personali, i quali, tuttavia, sono realtà quotidiana[112].

Tuttavia, si tratta di una conseguenza che, per l'appunto, non tiene in considerazione la realtà attuale del mercato digitale.

Diviene perciò necessario riconoscere che il dato personale può essere l'oggetto di un contratto, o – a seconda della tesi che si preferisca condividere – l'oggetto della prestazione di uno dei contraenti (l'utente)[113]: e di conseguenza, il diritto alla protezione dei dati ha natura mista, personale e patrimoniale.

È pur vero che il GDPR e la citata direttiva non tipizzano uno schema contrattuale astratto per la cessione dei dati, né identificano la natura del bene "dato personale" e il successivo diritto all'utilizzo una volta avvenuta la cessione, ma ciò non toglie che questi provvedimenti indubbiamente riconoscono il fenomeno della circolazione dei dati personali come fenomeno di circolazione di ricchezza. La direttiva descrive un'operazione economica di scambio di servizi contro scambio di dati e, infatti, prescrive che il consumatore presti un doppio consenso, finalizzato, il primo, ad ottenere il servizio e, il secondo, a cedere i dati personali: si tratta di due contro-prestazioni legate da un nesso funzionale.

E, infatti, la dottrina che si è occupata recentemente del tema ha dimostrato essenziale, per comprendere l'operazione sottostante, non tanto inquadrarla in uno schema contrattuale tipico, quanto, al contrario, far ricorso alla teorica della causa in concreto, per spiegare la meritevolezza e la tutelabilità di questo tipo di operazioni[114].

È stato opportunamente osservato che il riconoscimento di questa doppia natura tutela maggiormente gli utenti, i quali, in caso di lesione, avranno a disposizione non solo i rimedi previsti per la tutela dei diritti della personalità, ma anche le tutele previste dall'ambito contrattuale e, talvolta, dal diritto proprio dei consumatori. In questo senso, la patrimonialità non elide la personalità, perché tale

---

[112] Infatti, affermando la natura meramente personalistica del diritto dei dati, ne deriverebbe l'indisponibilità degli stessi, con la conseguenza irrealistica che qualsiasi contratto che li abbia ad oggetto sarebbe affetto da nullità radicale.

[113] Sulla qualificazione dei dati personali quali "beni", si v. G. RESTA, *I dati personali oggetto del contratto. Riflessioni sul coordinamento tra la Direttiva (Ue) 2019/770 e il Regolamento*, in *Annuario del diritto dei contratti*, Giappichelli 2018, pp. 127 ss.

[114] V. RICCIUTO, *op. cit*.

prospettiva si aggiunge alla natura personale del diritto alla protezione dei dati, con la conseguenza di arricchire "*la sfera delle tutele azionabili anche di quegli strumenti – tipicamente propri del diritto patrimoniale e contrattuale – che diversamente non sarebbero accessibili per l'interessato: l'azione di esatto adempimento; la tutela contrattuale; la disciplina sulle pratiche commerciali scorrette ed in genere la tutela del consumatore*"[115].

La natura anche patrimoniale dei dati personali è stata espressamente riconosciuta dall'Autorità garante della concorrenza e del mercato, nonché da due pronunce della giurisprudenza di merito.

Nel 2017 e 2018 l'Autorità di vigilanza ha comminato due sanzioni a Facebook Inc. e Facebook Ireland Ltd.[116], per pratica commerciale sleale ai sensi del codice del consumo: la condotta illecita del *provider* consisteva nell'aver indotto i propri utenti a conferire i propri dati personali, prospettando loro l'asserita gratuità del servizio fornito (di utilizzo dell'omonimo social network), enfatizzata dall' avviso pubblicitario *"Iscriviti! È gratis e lo sarà per sempre"*. La gratuità era tuttavia solo apparente, perché tali dati venivano utilizzati per ottenere un "surplus commerciale" attraverso servizi a valore aggiunto, che il provider commercializzava con utenti professionali[117].

Il *provider* ha impugnato i provvedimenti avanti all'autorità giurisdizionale amministrativa[118], la quale ha ribadito che la disciplina in materia di dati personali non è da ravvisare solamente nelle norme a protezione dei diritti e delle libertà fondamentali dell'interessato (presidiate dal GDPR e dal Codice in materia di protezione dei dati personali, oltre che dall'art. 8 della Carta dei diritti fondamentali dell'UE e dall'art. 16 TFUE), ma anche nelle norme, anch'esse di derivazione europea, previste a tutela dei consumatori e del mercato (incluse dunque quelle in tema di pratiche commerciali sleali ed altre norme a presidio delle persone fisiche nelle dinamiche di consumo, che trovano collocazione – appunto – nel codice del consumo[119]). Per tale ragione, il Consiglio di stato ha affermato che "*la patrimonializzazione del dato personale, che nel caso di specie avviene inconsapevolmente, costituisce il frutto dell'intervento delle società attraverso la messa a disposizione del dato - e della profilazione dell'utente - a fini commerciali*".

La commercializzazione dei diritti personali, in particolare il diritto al nome e il diritto all'immagine, è fenomeno ormai comune, sviluppatosi principalmente nel campo dell'industria americana dello spettacolo: negli anni '50 le esigenze di Hollywood e Broadway necessitavano di un diritto che fosse

---

[115] V. RICCIUTO, *op. cit.*

[116] AGCM, Provv 11.5.2017, n. 26596; AGCM, Provv. 29.11.2018, n. 27432.

[117] F. BRAVO, *Software di intelligenza artificiale e istituzione del registro per il deposito del codice sorgente*, in *Contr. e impr.*, 2020, p. 1422.

[118] TAR LAZIO, 10.1.2020 n. 260 e 261; CONS. STATO, 29.3.2021, n. 2631.

[119] N. ZORZI GALGANO, *Persona e mercato dei dati. Riflessioni sul GDPR*, Cedam, 2019; V. RICCIUTO, *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione fenomeno*, in *I dati personali nel diritto europeo*, a cura di V. CUFFARO-R. D'ORAZIO-V. RICCIUTO, Giappichelli, 2019, pp. 23 ss.

"*the reverse side of the coin*"[120].

In questo caso, il dato dell'individuo ha un valore intrinseco ed originario, poiché legato alla persona (es. l'attore) a cui si riferisce: evidente, dunque, che la commercializzazione di questo dato presuppone un determinato schema giuridico, fondato sul contratto e su un tipo di tutele e di vincoli legali specifici.

Tuttavia, la disciplina per la protezione dei dati personali (Direttiva e GDPR) prende in considerazione dati che rivestono una natura completamente differente: il loro valore commerciale non è né originario né legato specificamente all'individuo a cui afferiscono, il quale rileva unicamente un *quisque de populo*. Questi dati assumono un valore solo nel momento in cui vengono aggregati ed elaborati attraverso algoritmi che ricavano da essi ulteriori dati, dunque valori ed utilità commerciali. È, perciò, evidente la necessità di una forma di tutela che tenga in considerazione dall'un lato il valore irrisorio dei dati personali per il singolo consumatore, dall'altro lato il plusvalore economico generato a favore del titolare dal loro trattamento.

Il valore sempre più crescente assunto dai dati personali sta generando un vivo dibattito nella dottrina. Le maggiori perplessità originano dalla circostanza che il tradizionale statuto regolamentare e protettivo del contratto risulta di assai difficile applicazione al rapporto tra utente e titolare con riguardo alle operazioni di cessione e utilizzo dei dati personali (sui problemi relativi al consenso per l'utilizzo dei dati personali, v. *infra* cap. III, par. 12).

[120] M. B. NIMMER, *The right of Publicity*, in *Law and Contemp. Probs*, 1954, p. 204; *G. Versaci*, *La contrattualizzazione dei dati personali dei consumatori*, Esi, 2020.

Capitolo II

IL VALORE SOCIALE DEL DIRITTO

ALLA PROTEZIONE DEI DATI

SOMMARIO: 1. La contemporanea società dei dati. - 2. Dati personali, IOT, Intelligenza Artificiale e Big Data. - 3. Valore sociale dei dati personali e sorveglianza della società. - 4. Rapporto tra principali teorie della sorveglianza e tutela dei dati. - 4.1. *La prima teorizzazione della sorveglianza: Bentham e Foucault.* - 4.2. *Le teorie post-panottiche.* - 4.3. *(Segue) Il capitalismo della sorveglianza di Zuboff.* - 4.4. *Cenni sulle teorie della "terza fase" della sorveglianza*. - 5. Nuove prospettive legislative: Digital Services Act e Digital Markets Act. - 6. Riflessioni conclusive.

1. La contemporanea società dei dati

Negli ultimi anni è emerso con insistenza il tema del diritto al trattamento lecito dei dati personali.

Nel 2016 è stata fondata negli USA l'associazione OwnYourData Foundation[121], che si occupa di sensibilizzare ed informare i cittadini sul tema del diritto dei dati. L'organizzazione no-profit promuove l'alfabetizzazione digitale, ossia si occupa, attraverso piattaforme educazionali sul web, di insegnare come proteggere la vita digitale da intrusioni illecite e da illeciti trattamenti di dati personali.

Questa associazione è stata creata a seguito degli scandali che hanno coinvolto l'*entourage* di Trump nella campagna alle presidenziali del 2016.

In un'inchiesta del 2018, New York Times[122] e The Guardian riportavano di aver ottenuto e analizzato svariati documenti interni provenienti dalla società Cambridge Analytica[123], dai quali risultava

---

[121] Si veda il relativo sito web: https://ownyourdata.foundation/.

[122] Si v. tra i vari, *How Trump Consultants Exploited the Facebook Data of Millions*, New York Times, 17.3.2018, ove si legge che Cambridge Analytica sarebbe in possesso di uno strumento che può identificare le personalità dei votanti americani e influenzarne il loro comportamento (*tools that could identify the personalities of American voters and influence their behavior*); *Cambridge Analytica and Facebook: The Scandal and the Fallout So Far*, New York Times, 4.4.2018*; 'You Are the Product': Targeted by Cambridge Analytica on Facebook*, New York Times, 8.4.2018; Revealed: *50 million Facebook profiles harvested for Cambridge Analytica in major data breach*, The Guardian, 17.3.2018; si v., altresì, I. LLOYD, *UK: Classification of Software as Goods? UK: Administrators of Cambridge Analytica No Data Controllers* in *Computer Law Review International*, 2019, pp. 84-87-96.

[123] Il punto focale da cui nasce questa vicenda è proprio un illecito trattamento dei dati personali, che sono stati raccolti da Cambridge Analytica dal 2010 sino ai primi giorni di maggio dell'anno 2015 (sul tema di v., in particolare, A. DERSHOWITZ, *The Mueller Report. The final report of the special counsel into Donald Trump, Russia and collusion*, Skyhorse Publishing, 2019; FEDERAL TRADE COMMISSION, *Opinion about Cambridge Analytica*, 9383, 25.11.2019. Si veda, anche A. G. PARISI, *op. cit.*, pp. 113 ss.; B. KAISER, *Targeted: My Inside Story of Cambridge Analytica and How*

l'illecita raccolta e utilizzo di dati di almeno 50 milioni di individui (ma articoli successivi raccontano di oltre 240 milioni), i quali sarebbero stati utilizzati dal candidato Trump per vincere le elezioni presidenziali USA nei confronti della sfidante Clinton. In particolare, questa società raccoglieva illecitamente dati da social network come Facebook, studiando così la personalità dei soggetti e, attraverso modelli di calcolo e algoritmi specializzati fondati sulla psicometria e la psicografia[124], determinava profili, anche psicologici dei singoli utenti; attraverso la successiva presentazione di notizie, anche distorte o false, ma, comunque, personalizzate nel contenuto e nell'aspetto grafico, gli

---

Trump and Facebook Broke Democracy, HarperCollins, 2019, ossia la biografia della direttrice, all'epoca delle condotte illecite, del *business development* della SCL group, che ha successivamente collaborato alle indagini nei confronti della società e ha testimoniato avanti al Parlamento del Regno Unito e al Parlamento europeo il giorno prima dell'approvazione del GDPR).

La società reperiva tali dati con differenti modalità: alcuni database di dati venivano direttamente acquistati da altre società, che li avevano raccolti presso i rispettivi utenti, del tutto ignari del fatto che i propri dati sarebbero stati ceduti ad una società terza per perseguire trame di profitto. Si trattava, ad esempio, di dati relativi alla situazione economico-patrimoniale delle persone, le loro scelte sulle vacanze, le preferenze negli acquisti.

Una mole notevole di dati veniva raccolta/acquistata tramite i *social network*. In particolare, quando l'utente utilizzava le "applicazioni di terze parti" di Facebook e ne accettava le condizioni di servizio, autorizzava tali applicazioni a raccogliere i dati personali nonché quelli della cerchia di "amici" dell'utente. Si trattava, ad esempio, di giochi messi a disposizione della piattaforma, oppure di applicazioni che proponevano i sondaggi apparentemente più inutili. Facebook ha consentito questa raccolta di dati anche se gli amici dell'utente non avevano avuto alcuna interazione diretta con l'app o il sito web. Solo nell'aprile 2014 Facebook informò che stava introducendo una nuova versione dell'API Graph che avrebbe consentito agli sviluppatori di raccogliere i dati del profilo solo degli utenti stessi, e non degli amici interessati,

Dopo aver raccolto i primi dati personali degli utenti, Cambridge Analytica utilizzava le iniziali risposte a sondaggi dei partecipanti e i "mi piace" di Facebook per addestrare il suo algoritmo in modo che potesse prevedere i tratti della personalità degli utenti. Questi dati venivano elaborati da un "algoritmo psicometrico" creato presso il Centro di Psicometria dell'Università di Cambridge, denominato "OCEAN", ossia un modello psicometrico che misura l'apertura di un individuo alle esperienze, la coscienziosità, l'estroversione, la gradevolezza e il nevroticismo.

Ad esempio, mettere mi piace alle pagine Facebook relative ad app quali "*Come perdere un ragazzo in 10 giorni*" potrebbe essere collegato a un conservatore con personalità convenzionale.

I ricercatori affermavano che tale algoritmo avrebbe potenzialmente potuto prevedere la personalità dell'individuo in un modo più preciso dei suoi colleghi, degli amici, della famiglia e persino del coniuge.

Una volta creato il modello psicografico degli utenti, gli psicologi della società determinavano cosa spingesse gli individui ad agire e cosa li motivasse e veniva creati messaggi specifici, ideati appositamente per determinate personalità, attraverso il cd. *microtargeting comportamentale* (ogni messaggio era altamente personalizzato, tanto che nelle aree in cui quest'attività digitale era più intensa, vi erano città in cui veniva proposto un messaggio diverso ad ogni elettore che viveva nella medesima strada. Si veda B. KAISER, *op. cit.*, p. 259.

La società si concentrava sugli individui che avevano tratti comuni della personalità e gli stessi interessi, per inviare loro messaggi personalizzati: veniva svolta un'analisi predittiva particolarmente efficiente, attraverso la quale si poteva ipotizzare con forte probabilità quale comportamento avrebbe assunto l'elettore dopo aver ricevuto un determinato numero di questi messaggi, che venivano inoltrati agli utenti attraverso l'utilizzo dei *sociale network.*

Questi messaggi avevano lo scopo di modificare il comportamento elettorale degli elettori. Si spingevano elettori indecisi a votare un determinato candidato a recarsi alle urne e procedere al voto (Trump); dall'altro lato, si reprimeva la volontà di taluni elettori, le cui analisi statistiche e psicografiche lasciavano intendere che tale soggetto avrebbe preferito votare il candidato avversario (Clinton).

Si realizza così, una lesione al diritto all'autodeterminazione dei singoli, attuata attraverso l'uso illecito dei dati personali. V'è da chiedersi quale sia il confine tra propaganda negativa e repressione dell'elettorato: è vero che tale repressione non è stata attuata attraverso l'uso della forza o dell'esercito, come accade in alcuni Paesi non democratici. Ma tale repressione è stata possibile attraverso l'uso distorto della tecnologia di *internet* e l'utilizzo illecito dei dati personali degli americani.

[124] La psicometria è "*l'insieme dei metodi d'indagine psicologica che tendono al raggiungimento di valutazioni quantitative del comportamento umano o animale […] L'uso dei calcolatori ha consentito alla psicometria l'utilizzazione di metodologie statistico-matematiche, quali l'analisi fattoriale e la regressione multipla, che meglio rispettano la complessità dei fenomeni da misurare*"; la psicografia è "*lo studio e il riconoscimento delle caratteristiche psichiche di un soggetto attraverso l'interpretazione di elaborati grafici*" (in *Enciclopedia Treccani online*, rispettivamente all'indirizzo https://www.treccani.it/enciclopedia/psicometria/ e https://www.treccani.it/enciclopedia/psicografia/).

individui potevano venire influenzati anche a livello emotivo e sentimentale: un'attività sostanzialmente analoga a quella che avviene nel *marketing* commerciale, ma qui applicata per convincere gli elettori a votare un determinato candidato[125].

Da tale notizia è originata un'indagine approfondita da parte dell'FBI, il cui resoconto finale viene descritto nel cd. rapporto Mueller[126], dal nome del procuratore che ha svolto le indagini.

La vicenda mostra come le nuove tecnologie permettano la captazione e conservazione di dati sempre più personali e segreti delle persone e nuovi algoritmi di calcolo e profilazione permettano di esercitare una forma di controllo sociale, arrivando a plagiare le volontà dei cittadini: questo è un danno per la comunità complessiva e per il singolo individuo.

Sempre nell'orizzonte statunitense, è noto che a seguito dell'assalto a Capitol Hill del 6.1.2021, l'Oversight Board (organismo di sorveglianza) di Facebook e Instagram ha deciso di "sospendere definitivamente" gli account dell'ex Presidente Trump, impedendogli l'uso di tutti i servizi del social network, così intervenendo non solo sui suoi dati personali, ma direttamente sulla sua "identità digitale", sopprimendola e annullandola: si tratta della massima intrusione nella sfera digitale del soggetto, che determina il massimo danno. E questo si propaga nella comunità perché si tratta, in definitiva, di esercitare sin da ora una diretta influenza sull'esito della prossima campagna per le presidenziali, cagionando un danno effettivamente irreparabile.

Va evidenziato che, sebbene il concetto di *privacy* nasca nell'ordinamento statunitense, l'attuale disciplina americana è certamente meno avanzata di quella europea.

Attualmente, sono in discussione negli USA alcuni disegni di legge volti ad introdurre una disciplina *privacy* che, per certi aspetti, ricalchi quella europea; si tratta (senza alcuna pretesa di esaustività)[127]:

- *Consent Bill* (senatore Markey), che obbliga le aziende a chiedere il consenso degli utenti per determinati trattamenti e sviluppa tecniche di sicurezza dei dati;
- *Corporate Executive Accountability Act* (senatrice Warren), che introduce sanzioni penali per i dirigenti d'azienda in caso di trattamento illecito di dati personali;
- *"Your are the Product" Legislative Initiative* (senatore Steyer), che permette la proposizione di ricorsi giurisdizionali per determinati abusi nel trattamento dei dati personali;

---

[125] Per un'analisi dell'uso, in Europa, dei *social network* per la campagna elettorale, si v. C. J. BENNETT, *Voter databases, micro-targeting, and data protection law: can political parties campaign* in *Europe as they do in North America? in International Data Privacy Law,* Vol. 6, No. 4, 2016, pp. 261-275, nonché M. GERCKE, *"Hacking an Election". An overview of attacks in the context of democratic elections and the role of criminal law in defending against such attacks* in *Computer Law Review International*, 2017, pp. 129-134; W. UNGER, *How the Poor Data Privacy Regime Contributes to Misinformation Spread and Democratic Erosion,* in *The Columbia Science & Technology law review,* 2021*,* pp. 308-345.

[126] Si tratta del Report "*On The Investigation Into Russian Interference In The 2016 Presidential Election*", pubblicato dal Dipartimento di Giustizia USA, in data 18.4.2019.

[127] Il Sito web https://ownyourdata.foundation/ raccoglie le principali e più recenti iniziative legislative nell'ambito della protezione dei dati personali.

- *Data Dividend Law* (Governatore della California Newsom), che riconosce la necessità di un compenso per l'uso che viene fatto dei dati personali degli utenti;
- *Detour Act* (senatore Warner), che introduce principi di trasparenza e vieta l'uso di algoritmi di elaborazione dei dati che abbiano lo scopo di manipolare l'utente;
- *Digital Asset Legislation* (Stato del Wyoming), che definisce i dati personali come proprietà privata intangibile;
- *Scientific Integrity Act* (Government Accountability Project), che supporta gli informatori, proteggendolo quando decidono di rivelare abusi, sfruttamento e illeciti trattamenti di dati personali.

L'Unione Europea ha adottato il Reg. UE n. 2016/679, unanimemente considerato la più moderna disciplina esistente per la tutela del diritto dei dati: l'art. 82 è la disposizione su cui, in sostanza, si misura l'effettività del sistema di *private enforcement* adottato dall'Unione Europea per la protezione dei dati personali.

L'esponenziale sviluppo tecnologico degli ultimi anni, a disposizione sia degli Stati sia di operatori privati, unitamente all'affermarsi di "colossi del web" nel mercato di *internet*, pone seriamente il problema della tutela dei dati personali.

Anche da questa prospettiva è necessario verificare l'effettiva portata dell'art. 82 e se esso sia in grado di soddisfare le istanze di tutela del diritto alla protezione dei dati, di cui il GDPR stesso si fa catalogo.

Per tale ragione, l'analisi del sistema di *private enforcement* previsto in ambito *privacy* verrà effettuata individuando le nuove istanze sociali di tutela a cui il diritto alla protezione dei dati risponde, per verificare se la nuova disciplina fornisca adeguata risposta.

Calabresi ha dimostrato che un corretto approccio ad un sistema di responsabilità civile deve essere svolto "*in funzione di una prospettiva che compendi al tempo stesso la dimensione privatistica del rapporto tra danneggiante e danneggiato e quella pubblicistica del suo impatto complessivo sul sistema economico e sociale*"[128].

2. Dati personali, *IOT*, Intelligenza Artificiale e Big Data

[128] G. CALABRESI, *The Cost of Accidents: A Legal and Economic Analysis*, New Haven 1970; ID., *Costo degli incidenti e responsabilità civile. Analisi economico-giuridica*, trad. di A. DE VITA-V. VARANO-V. VIGORITI, Giuffrè, 1975; ID., *Ideals, beliefs, attitudes, and the law: private law perspectives on a public law problem*, Syracuse, 1985; ID., *The Future of Law and Economics*, New Haven, 2016, sul quale si v. l'analisi di E. AL MUREDEN, il quale afferma che "*in quest'ottica il legislatore e la P.A. si appropriano di un ruolo sempre più esteso e pregnante nell'individuazione dei rischi connessi ad attività di produzione di beni o servizi e nella definizione di standard di sicurezza ragionevole formulati all'esito di una complessa attività di bilanciamento di molteplici esigenze di carattere etico e sociale che concorrono con quelle evidenziate dalle scienze mediche, statistiche, epidemiologiche ed economiche*" (E. AL MUREDEN, *Il futuro del Law and Economics nel pensiero di Guido Calabresi*, in *Riv. dir. civ.*, 2018, p. 778, spec. 786).

Dagli anni Sessanta ad oggi vi è stato un nuovo, esponenziale, sviluppo tecnologico[129], iniziato con la creazione di Internet[130].

Ricordiamo che questa tecnologia nasce come un progetto di connessione di rete, per scambiare messaggi, all'interno di basi militari, che viene, poi, utilizzato anche all'interno di università e pubbliche amministrazioni. Successivamente, grazie all'invenzione di protocolli uniformemente adottati, si è potuto collegare le differenti reti tra di loro; questo ha permesso la creazione dei primi elaboratori elettronici che facevano da server e da banca dati. Negli anni Novanta, la rete collegava già interi continenti e fu permesso l'utilizzo da parte dei privati, che ha portato al rapido sviluppo di nuove forme di business, basate proprio sulla raccolta e lo scambio di dati tra i diversi server connessi. Ancor successivamente, si sono sviluppate le piattaforme digitali e i *social network* e si è posta la questione dei *big data*[131].

I fenomeni tecnologici dell'epoca moderna, in particolare, *IOT*, Big Data, Intelligenza Artificiale, Robotica, hanno conseguenze rilevanti per il diritto alla protezione dati[132].

Con il termine *Internet of Things* (*IOT*)[133] s'intende quell'insieme di tecnologie costantemente connesse che dialogano tra di loro, scambiando flussi di dati, per raggiungere obiettivi di efficienza, organizzazione e funzionalità del vivere umano[134].

---

[129] Per un'analisi della privacy in relazione allo sviluppo tecnologico e, dunque, dei nuovi concetti che vengono ad identificare questo diritto, si v. J. E. COHEN, *What privacy is for* in *Harward Law Review,* 2013, Vol. 126: 1934, pp. 1904-1932.

[130] Già negli anni '60, Westin aveva evidenziato che dalla Seconda Guerra Mondiale il progresso nei dispositivi di spionaggio elettronico presentava crescenti minacce alla *privacy* nella società. L'incremento della sorveglianza sugli individui è stato possibile in ragione del basso conto dei nuovi dispositivi elettronici e alla loro diffusione; ulteriore fattore è stato il cambiamento nei costumi sociali: gli individui dimostravano di voler divulgare maggiori informazioni private; vi è poi l'elemento della curiosità del pubblico di conoscere l'intimità della vita privata degli altri. L'autore afferma che nella società moderna vi è un conflitto tra *privacy* e sorveglianza sociale resa possibile dai moderni sviluppi tecnologici dell'epoca, che rischia di pregiudicare il valore sociale della *privacy*. (sul tema, si v. anche R. L. BLAND, *Book Notes*, *Washington and Lee Law Review*, Vol. 25, 1968).

[131] Per una panoramica approfondita dello sviluppo di Internet, si veda A. QUARTA, *Mercati senza scambi. Le metamorfosi del contratto nel capitalismo della sorveglianza*, Esi, 2020, pp. 29 ss.; M. O' ROURKE, *Fencing Cyberspace: drawing borders in a virtual world*, in *Minnesota Law Review*, 82, 1998, pp. 620 ss.; D. BOLLIER*, The promise and peril of big data*, The Aspen Institute*,* 2010, pp. 1-52.

[132] Ricordiamo che, come osservato da Westin, da concetto riservato ad una élite, diviene concetto di risonanza diffusa nella società tra gli anni '60 e '70 e immediatamente ci si rende conto che le minacce più gravi ai dati personali derivano proprio dalla diffusione dei computer e delle nuove tecnologie; così A. WESTIN, *Entering the Era of Databank Regulation and How We Got There*, in *Policy Issues in Data Protection and Privacy*, *Principles and Perspectives*, OECD, Paris, 1976, p. 95. Nella società dell'informazione, anche detta società post-industriale, la forza lavoro è sostituita dalla conoscenza e dal capitale e le informazioni divengono la nuova valuta, secondo il detto "*data is the new oil*"; in questi termini, C. J BENNETT, *Regulating Privacy*, Cornell University Press, Ithace 1992, pp.16–17, il quale evidenzia che "*the needs of modern administrations in terms of data to the ends of performing their functions, which spurred the need and the development of the first personal data processing systems*".

[133] F. PIZZETTI, *op. cit*., p. 9. Sul tema, si veda A. DAVOLA-R. PARDOLESI, *In viaggio col robot: verso nuovi orizzonti della r.c. auto ("driverless")?*, in *Danno e resp*., 2017, pp. 616 ss..; M. C. GAETA, *La protezione dei dati personali nell'Internet of Things: l'esempio dei veicoli autonomi*, in *Dir. inf*., 2018, p. 147.

[134] A.S. BOHM-EJ GEORGE-B. CYPHERS-S. LU, *Privacy and Liberty in an Always-on, Always-listening World* in *The Columbia Science & Technology law review,* 2017, pp. 1-45, dove gli autori analizzano i dispositivi *always-on*, in particolare i differenti tipi di sensori e di modalità con cui gli stessi raccolgono i dati.

Secondo una delle definizioni più accreditate, con il termine *Big Data* si indicano quelle architetture pubbliche o private in cui confluiscono, dalle fonti più disparate – ma soprattutto informatiche – dati personali ed informazioni degli utenti (e non solo), che vengono elaborate nelle forme più diverse, in particolare per ricavarne ulteriore valore informativo[135].

Il termine Intelligenza Artificiale indica "*sistemi che mostrano un comportamento intelligente analizzando il proprio ambiente e compiendo azioni, con un certo grado di autonomia, per raggiungere specifici obiettivi. I sistemi basati sull'IA possono consistere solo in software che agiscono nel mondo virtuale (per esempio assistenti vocali, software per l'analisi delle immagini, motori di ricerca, sistemi di riconoscimento vocale e facciale); oppure incorporare l'IA in dispositivi hardware (per esempio in robot avanzati, auto a guida autonoma[136], droni o applicazioni dell'Internet delle cose)*"[137].

Il GDPR non tiene in considerazione le applicazioni dei *Big Data*, dell'Intelligenza Artificiale[138] e della Robotica, le quali sono sempre più rilevanti dal punto di vista quantitativo e qualitativo[139]: per il suo sviluppo e funzionamento, l'Intelligenza Artificiale e la Robotica necessitano di moli ingenti di dati, i quali devono, comunque, trovare adeguata tutela nell'utilizzo che la macchina successivamente ne deve fare[140].

---

[135] C. O'NEIL, *Armi di distruzione matematica. Come i big data aumentano la disuguaglianza e minacciano la democrazia*, Bompiani, 2017; sul tema si v. anche V. MAYER-SCHONBERGER-K.N. CUKIER, *Big data. Una rivoluzione che trasformerà il nostro modo di vivere e già minaccia la nostra libertà*, Garzanti, 2013; L. MOEREL, *Big Data Protection. How to Make the Draft EU Regulation on Data Protection Future Proof*, Tilburg University, 2014, pp. 3-63; K. WATERMAN – P.J. BRUENING, *Big Data analytics: risks and responsibilities* in *International Data Privacy,* Vol. 4, No. 2, 2014, pp. 89-95; M. R. LEISER-F. DECHESNE, *Governing machine-learning models: challenging the personal data presumption* in *International Data Privacy Law,* Vol. 10 No. 4, 2020, pp. 187-200.

[136] Con riferimento ai veicoli a guida autonoma, la maggior parte dei dati personali che vengono elaborati riguardano i passeggeri, come le abitudini di viaggio, le destinazioni, le soste, i percorsi, la corporatura della persona (che si ricava dalle impostazioni del sedile), il numero di passeggeri trasportati (tramite il numero di cinture di sicurezza allacciate ad ogni viaggio), le preferenze musicale, i dati ambientali, ecc. Sui diversi tipi di sensori per raccogliere i dati, nonché per un'analisi dei principi del trattamento in relazione ai veicoli a guida autonoma, si v. E. SALAMI, *Autonomous transport vehicles versus the principles of data protection law: is compatibility really an impossibility?* in *International Data Privacy Law,* Vol. 10, No. 4, 2020, pp. 330-345.

[137] Definizione tratta dalla Comunicazione della Commissione UE (SWD(2018) 137 final), *L'intelligenza artificiale per l'Europa*, 25.4.2018.

[138] È stato osservato che il "Regolamento appare in parecchi casi molto orientato a dare "risposte puntuali a problemi attuali", col rischio di dettare, almeno per alcune parti, una disciplina destinata ad invecchiare rapidamente"; così F. PIZZETTI, *op. cit.*, 176.

[139] AUTORITÀ GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *op. cit.*

[140] Il Garante italiana ha affermato che "*non stupisce allora – ed anzi costituisce un positivo invito alla riflessione e all'approfondimento critico (anche in ordine alla congruità degli strumenti posti a disposizione delle autorità di controllo per affrontare gli inediti rischi sollevati dai Big Data) − che nella segnalata cornice normativa, da taluno avvertita come inadeguata rispetto al fenomeno preso in esame, da un lato, con apprezzabile realismo, si formulino inviti a monitorare il fenomeno in ragione della sua (relativa) novità; dall'altro, si sia rimarcata la necessità di un approfondimento delle implicazioni etiche connesse all'introduzione dei Big Data che, ove non adeguatamente "governati", possono alimentare (più di quanto i trattamenti in essere già non contribuiscano a fare) un regime della classificazione e della sorveglianza. È a questo proposito necessario guardare agli effetti sui singoli derivanti dall'utilizzo dei Big Data – specie ove, a seguito di attività di profilazione (cfr. Considerando 71 e art. 4, n. 4, GDPR), possano condurre all'adozione di misure*

Si tratta di un tema attualissimo, come dimostra il fatto che, recentemente, l'Unione Europea ha adottato il Libro Bianco sull'Intelligenza Artificiale[141], sottolineando l'importanza che l'Intelligenza Artificiale si sviluppi, in ambito europeo, su valori comuni e diritti fondamentali, condivisi da tutti i Paesi membri, quali la dignità umana e la tutela della *privacy*. Inoltre, è stata ribadita la necessità di un approccio comune europeo all'Intelligenza Artificiale, al fine di evitare la frammentazione del mercato unico attraverso l'introduzione di singole e diversificate iniziative nazionali, suscettibili di compromettere la certezza del diritto e di indebolire la fiducia dei cittadini.

Il tentativo di bilanciamento tra diritto alla protezione dei dati e necessità di sviluppo dell'Intelligenza Artificiale traspare dagli atti che l'Unione Europea sta valutando di adottare per regolamentare questo fenomeno. È stato osservato che "condivisione e disponibilità dei dati sono infatti annoverate tra le azioni strategiche volte a promuovere lo sviluppo dei sistemi di intelligenza artificiale, purché tali obiettivi vengano perseguiti nel rispetto dei diritti delle persone e dei valori europei"[142].

Il "Piano Coordinato sull'Intelligenza Artificiale"[143] prevede che "*affinché l'IA possa svilupparsi ulteriormente è necessario un valido ecosistema dei dati basato sulla fiducia, sulla disponibilità dei dati e sull'infrastruttura" e che l'accesso ai dati "è un elemento fondamentale per un panorama di IA competitivo*", ma si precisa che l'accesso ai dati deve avvenire "*nel pieno rispetto delle norme sulla protezione dei dati personali*".

Inoltre, nella Risoluzione del Parlamento Europeo del 12.2.2019 su una "politica industriale europea globale in materia di robotica e intelligenza artificiale"[144] si riconosce che il diritto al rispetto della

---

discriminatorie –, ma anche alle aspettative individuali in relazione al potenziale utilizzo di dataset contenenti dati personali che li riguardano, potendo essere minata, con usi inattesi delle informazioni, la fiducia riposta nel titolare del trattamento (che, va ribadito, è mero "custode" e non dominus dei dati personali raccolti per finalità che la legge vuole determinate e rese note all'interessato e quindi non arbitrariamente modificabili). Già solo sul piano etico, la trasparenza dei processi che si avvalgono di tecniche Big Data – valore al quale dà corpo la disciplina relativa agli obblighi informativi contenuta nel RGPD – rappresenta un fattore chiave il cui perseguimento è irrinunciabile, sia nel settore privato che in quello pubblico" (AUTORITÀ GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Indagine conoscitiva sui big data*, febbraio 2020, pp. 53-54).

[141] COMMISSIONE UE, *White Paper on Artificial Intelligence: a European approach to excellence and trust* COM(2020) 65 final, 19.2.2020. Gli ulteriori atti dell'UE che considerano l'Intelligenza Artificiale sono la Risoluzione del Parlamento Europeo del 16.2.2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica [2015/2103(INL)]; la Risoluzione del Parlamento Europeo del 20.10.2020 recante *raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale* [2020/ 2014(INL)];

[142] G. FINOCCHIARO, *Intelligenza artificiale e protezione dei dati personali*, in *Giur. it.*, 2019, 7, pp. 1657 ss.; sul tema del rapporto tra dati personali e Intelligenza Artificiale, si v. F. BRAVO, *Software di intelligenza artificiale e istituzione del registro per il deposito del codice sorgente*, op. cit., 2020, pp. 1422 ss.; R. MESSINETTI, *La tutela della persona umana* versus *l'intelligenza artificiale. Potere decisionale dell'apparato tecnologico e diritto alla spiegazione della decisione automatizzata*, in *Contr. e impr.*, 2019, pp. 891 ss.; G. FINOCCHIARO, *Il contratto nell'era dell'intelligenza artificiale*, in *Riv. trim. dir. proc. civ*., 2018, pp. 441 ss.; G. PIZZETTI, *Intelligenza artificiale, protezione dei dati personali e regolazione*, Giappichelli, 2018; G. SARTOR, *Le applicazioni giuridiche dell'intelligenza artificiale: la rappresentazione della conoscenza*, Giuffrè, 1990; ID., *Intelligenza artificiale e diritto. Un'introduzione*, Giuffrè, 1996;

[143] Racchiuso nella Comunicazione della Commissione al Parlamento Europeo, al Consiglio Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni del 7.12.2018 (COM(2018) 795).

[144] Risoluzione 2018/2088(INI).

vita privata e il diritto alla protezione dei dati personali, quali sanciti dagli articoli 7 e 8 della Carta dei diritti fondamentali e dall'articolo 16 del Trattato sul funzionamento dell'Unione europea, "*si applicano a tutti i settori della robotica e dell'intelligenza artificiale e che il quadro giuridico dell'Unione per la protezione dei dati deve essere pienamente rispettato*", e si invita la Commissione "*a garantire che qualsiasi futuro quadro normativo dell'UE in materia di IA garantisca la riservatezza e la confidenzialità delle comunicazioni e la protezione dei dati personali*".

Come evidenziato, il GDPR è basato sulla concezione del consenso informato che legittima l'utilizzo dei dati: pur permanendo il diritto di controllo, l'interessato ne rende lecito l'utilizzo ad altri tramite una manifestazione di volontà, secondo una supposta logica di autodeterminazione individuale.

Tuttavia, questa logica non si attaglia propriamente all'utilizzo e trattamento di grandi masse di dati, tantomeno se questo è finalizzato al funzionamento di una tecnologia avanzata come l'Intelligenza Artificiale.

Infatti, è stato evidenziato che "*il consenso, astrattamente il miglior modello possibile, si rivela spesso non adeguato nel fornire una tutela effettiva ed inefficace. Ciò tanto più se ci si confronta con applicazioni di intelligenza artificiale basate sui Big data, nelle quali la determinabilità a priori dei processi di elaborazione non è scontata e nelle quali la finalità del trattamento sovente non è chiara*"[145].

Lo sviluppo degli algoritmi alla base dell'Intelligenza Artificiale e della Robotica, che a sua volta si fondano sull'uso dei *Big Data*, può determinare lesioni gravissime per la libertà di autodeterminarsi informatica ed avere ripercussioni negative sulla società nel suo complesso che, a loro volta, determinano nuovi effettivi negativi per gli individui[146].

Tali tecnologie consentono di "leggere la mente degli utenti" e di condizionarne fortemente il pensiero e il comportamento. In tema di intelligenza artificiale, è stato evidenziato "*quanto breve possa essere il passo tra il "leggere" il pensiero umano ed il "modificarlo" o "controllarlo", sino*

---

[145] G. FINOCCHIARO, *Intelligenza artificiale e protezione dei dati personali*, op. cit.

[146] Sulle utilità sociali che possono ricavarsi dall'uso dei *Big Data* si v. il report di G. B. AGABA, F. AKINDÈS, L. BENGTSSON, J. COWLS, M.I. GANESH, N. HOFFMAN & OTHERS, *Big data and positive social change in the developing world: a white paper for practitioners and researchers*, in *Rockefeller Foundation Bellagio Centre conference*, 2014, pp. 1-35, ove gli autori sottolineano che "*it is time for civil society groups in particular to become part of the conversation about the power of data. These groups, broadly defined, are essential to building sustainable and relevant big data capacity on the national level, since they are the connectors between individuals and the level of government, corporations and governance institutions. For big data analysis to be locally driven and rooted, technical expertise and understanding must be built locally and nationally, not only on the international scale in elite data science centres. Civil society groups are also crucially important but currently underrepresented in debates about privacy and the rights of technology users. Although big data analytics are a worldwide phenomenon, most LMICs still lack locally enforceable data protection rules and standards. If civil society groups are not involved in exerting pressure for fair principles to guard citizens' data effectively, then the rules and standards will evolve to benefit corporations and governments, leaving the citizen out entirely*" (p. 33).

ad obliterare il libero arbitrio"[147].

Con riferimento a tali tecnologie, diviene ancor più centrale la definizione di dato personale contenuta nel GDPR e la differenza con i dati non personali. Su questi ultimi si sofferma il Considerando n. 26 GDPR, secondo cui "*i principi di protezione dei dati non dovrebbero pertanto applicarsi a informazioni anonime, vale a dire informazioni che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato*". La distinzione è essenziale, perché se la nuova tecnologia utilizza dati non personali, le tutele del GDPR non trovano applicazione.

Trattasi, comunque, di definizione non già statica ma destinata a mutare con l'evolversi delle tecnologie, nonché relativa, poiché dipendente dalle tecnologie a disposizione del titolare del trattamento[148]: ciò che oggi è un dato non personale, domani potrebbe diventarlo.

In relazione a tali tecnologie, è assolutamente attuale il dibattito sulla responsabilità per trattamento illecito dei dati. Nello specifico, ci si domanda chi sia il soggetto responsabile nel caso di danni cagionati dalle applicazioni dell'Intelligenza Artificiale e della Robotica, soprattutto in quei casi in cui gli algoritmi di funzionamento siano dotati di una determinata discrezionalità che può portare l'elaborazione ad esiti differenti. Si discute se il responsabile del trattamento illecito debba essere l'autore dell'algoritmo, il produttore della macchina, il venditore; a rendere ancor più complesso tale quadro, v'è la circostanza che sovente le nuove tecnologie racchiudono al proprio interno decine di *software* sviluppati da soggetti differenti che interagiscono tra di loro, sicché non è sempre possibile individuare a quale tra di essi sia imputabile il danno subito dall'utente.

Come evidenziato nei paragrafi precedenti, il GDPR ruota intorno al principio dell'autodeterminazione e del consenso, ancorché attenuati, rispetto all'impianto previgente della Direttiva e del Codice, dal principio dell'*accountability*. Tuttavia, è evidente che tale logica di fondo non si presta ad essere applicata alle nuove tecnologie descritte, che trattano masse di dati e non singoli dati dell'utente, sicché la prospettiva individualistica della tutela non appare adeguata[149]. Per

---

[147] U. RUFFOLO-A. AMIDEI, *Intelligenza artificiale e diritti della persona: le frontiere del "transumanesimo"*, in *Giur. it.*, 2019, pp. 1657 ss.

[148] G. FINOCCHIARO, *Intelligenza Artificiale e protezione dei dati personali*, op. cit., pp. 1670 ss.; sul tema si v. in generale (anche per i riferimenti bibliografici), la discussione "*Intelligenza Artificiale e diritto*" a cura di E. GABRIELLI-U. RUFFOLO, in *Giur. it.*, 2019, pp. 1657 ss.; per un'analisi sulla responsabilità in tema di intelligenza artificiale A. LIOR, *AI strict liability vis-à-vis ai monopolization,* in *The Columbia Science & Technology law review,* 2020, pp. 90-126.

[149] Si evidenzia anche l'utilizzo massiccio di dati personali da parte dei veicoli a guida autonoma. La dottrina sottolinea la necessità che questi veicoli siano progettati ponendo molta attenzione al rispetto dei principi sulla legittimità del trattamento di cui al GDPR; si osserva che "*AV are capable of attaining compliance with the principles of data protection law. Recommendations are also made regarding how compliance with these principles can be possibly attained. However, there is a need for regulators and stakeholders to have a forum where basic rules and standards can be formulated in this regard. This would ensure that the principles are in sync with the framework of data protection law and compliance with them would be very helpful in achieving a high level of data protection compliance as far as AV are concerned. It is*

tale ragione, la dottrina più recente propone di adottare nuove forme di responsabilità non più basate sui principi tradizionali: è stato, ad esempio, proposto di introdurre forme di responsabilità basate sull'allocazione del "rischio da sviluppo"[150].

3. Valore sociale dei dati personali e sorveglianza della società

A seguito dei più recenti sviluppi tecnologici, il tema della *privacy* è venuto ad intrecciarsi con quello della sorveglianza e del controllo sociale[151].

La diffusione degli strumenti informatici, che pervadono ogni aspetto del vivere sociale, e la connessione tra di essi, agevola le attività di controllo[152], le quali sono poste in essere non più solo dalle autorità governative centrali, ma soprattutto dai fornitori di servizi informatici, i quali, sono i "*depositari finali delle informazioni e interazioni della maggior parte della popolazione, costituendo quelli che vengono chiamati i* Big Data"[153].

Anche le operazioni più banali che ogni utente compie sul web vengono monitorate e conservate come informazioni tramite l'uso dei *cookies* o di altri strumenti tecnologici; questo è accentuato dal

---

not expected that data protection law would re-invent itself for AV. However, necessary modifications and conscious regulation must be put in place if AV are to ever become a daily part of our legitimate human existence. The institution of proper data protection measures will ensure that when legal actions challenging the legality of AV start pouring in, Controllers will be fully ready to defend the legality of their processing activities thereby aiding the acceptability of AV as a regular piece of necessary technology"; così E. SALAMI, *Autonomous transport vehicles versus the principles of data protection law: is compatibility really an impossibility?* in *International Data Privacy Law,* Vol. 10, No. 4, 2020, pp. 330-345.

[150] AR. FUSARO, *Quale modello di responsabilità per la robotica avanzata? Riflessioni a margine del percorso europeo*, in *Nuova giur. civ. comm.*, 2020, pp. 1344 ss.

[151] Sul tema la dottrina è amplissima. Si v. L. BRANDIMARTE-A. ACQUISTI-G. LOEWENSTEIN, *Misplaced confidences: Privacy and the control paradox* in *Social psychological and personality science,* 2012, pp. 1-22; P. PERRI, *Sorveglianza elettronica, diritti fondamentali ed evoluzione tecnologica*, Giuffrè, 2020; ID., *Privacy, diritto e sicurezza informatica*, Giuffrè, 2007; R. CASO, *La società della mercificazione e della sorveglianza: dalla persona ai dati. Casi e problemi di diritto civile*, Ledizioni, 2021; G. ZICCARDI, *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica*, Raffaello Cortina Editore, 2015.

Sul tema della sorveglianza e il connesso concetto di società "liquida", D. LYON, *Theorizing Surveillance: The panopticon and beyond,* Routedge, 2006; ID., *Surveillance Studies: An Overview*, Cambridge, 2007.

[152] Sul potere di controllo esercitabile dalle autorità pubbliche tramite l'uso dei dati si v., inoltre, A. MANTELERO-G. VACIAGO, *The "Dark Side" of big data: private and public interaction in social surveillance. How data collections by private entities affect governmental social control and how the EU reform on data protection responds* in *Computer law review international*, 2013, pp. 161-169; G. PHILLIPS, *The Abuse and Misuse of Technology. A UK Newspaper Lawyer's Perspective*, in *Computer Law Review International*, 2016, pp. 43-51. L'autore analizza il dilemma tra libertà individuale e controllo, affermando che "*No one seriously disputes that law enforcement and intelligence agencies needed to have investigatory powers, which may be intrusive, and may need to be conducted in secret. However, use of these powers cannot be unlimited and must be subject to the rule of law (i.e. must be clear and certain, legitimate, transparent, necessary and proportionate); further the executive must be properly accountable and there must be proper access to justice. There is a battle going on across many fronts and involving many players (ISPs, telecommunications companies, business, individual users, traditional media, social media, state agencies) in different jurisdictions over who should have ownership and control of information and what jurisdictional norms should apply and prevail in that battle*".

[153] P. PERRI, *Introduzione,* in *Sorveglianza elettronica, diritti fondamentali ed evoluzione tecnologica*, Giuffrè, 2020 p. XI. In tema di *Big Data*, si v. A. DE MAURO-M. GRECO-M. GRIMALDI, *A Formal definition of Big Data based on its essential features*, in *Library Review*, 2016, n. 65, pp. 122 e ss.; E. NUNZIANTE, *Big Data. Come proteggerli e come proteggerci. Profili di tutela tra proprietà intellettuale e protezione dei dati personali*, in *Law and Media Working Paper Series*, 2017, p. 6; G. DE GREGORIO-R. TORINO, *Privacy, tutela dei dati personali e Big Data*, in AA.VV., *Privacy Digitale*, a cura di E. TOSI, Giuffrè, 2019, pp. 447 ss.

fatto che, sempre più spesso, ogni dispositivo di nuova costruzione è costantemente connesso alla rete (*IOT*) affinché il suo utilizzo possa essere monitorato e studiato, così indirettamente monitorando l'individuo in ogni sua attività quotidiana (ad es. dispositivi informatici, domotica, sistemi di *contact tracing*).

Come affermato recentemente dal Garante per la protezione dei dati personali, la digitalizzazione crescente della società (cui la pandemia Covid-19 ha impresso un'accelerazione formidabile) e il programma di azione verso la trasformazione digitale, che costituisce uno dei pilastri dell'azione politica già in essere a livello europeo[154] e nazionale (con il Piano Razionale di Ripresa e Resilienza), presuppongono una consapevolezza piena e diffusa (a livello individuale e sociale) dei "diritti digitali" della persona: tra questi una posizione centrale spetta al diritto alla protezione dei dati personali[155].

I dati personali di ciascuno possono essere utilizzati, anche illecitamente, per condizionare il comportamento degli individui, così violando il diritto di autodeterminazione dei singoli, impattando sulla sfera privata ma, altresì, creando un forte danno anche per la collettività. Il valore sociale della *privacy*, che negli anni '70 era stato evidenziato da Rodotà, è divenuto sempre più rilevante e, anzi, il baricentro dell'interesse giuridico protetto ormai non può più dirsi spostato verso l'individuo: si tratta di un fenomeno che ammanta la collettività e che, per tale ragione, deve anche essere considerato dall'ordinamento in tale prospettiva. Nel recente discorso per la Relazione annuale 2020, il Presidente del Garante per la protezione dei dati personali ha affermato che "*la funzione sociale della privacy è resa ancor più evidente in una congiuntura, come l'attuale, contraddistinta da rilevanti trasformazioni nel rapporto tra singolo e collettività, tra libertà e poteri, che rendono questa una stagione quasi costituente sotto il profilo della garanzia dei diritti*"[156].

Per tale ragione, la dottrina moderna sta spostando l'attenzione dalla *privacy* intesa meramente come diritto soggettivo, ad una prospettiva più ampia, che analizzi il rapporto tra il trattamento dei dati personali e la cd. sorveglianza sociale. Si tratta di un aspetto che deve certamente essere considerato nell'analisi del sistema di *private enforcement* predisposto per la tutela del diritto dei dati.

Questo è fondamentale, perché, l'effetto principale negativo della sorveglianza è proprio la violazione della *privacy*, da cui derivano ulteriori lesioni a valori fondamentali dell'ordinamento, come la partecipazione democratica[157].

---

[154] v. la Comunicazione della Commissione europea, 2030 *Digital Compass: the European way for the Digital Decade*, Brussels, 9.3.2021, COM(2021) 118 final.

[155] AUTORITÀ GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Relazione 2020*, pp. 10-11.

[156] P. STANZIONE, *Tecnica, protezione dei dati e nuove vulnerabilità,* 2.7.2021, all'indirizzo https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9676499.

[157] D. LYON, *The culture of Surveillance. Watching as a way of life,* Polity Press, 2018. Si v. anche la traduzione italiana a cura di G. BALBI-P. DI SALVO, *La cultura della sorveglianza*, Luiss, 2020.

4. Rapporto tra principali teorie della sorveglianza e tutela dei dati

Il rapporto tra potere pubblico e interesse privato, nonché, più specificamente, della sorveglianza sociale, è un tema che ha da sempre interessato, oltre ai giuristi, i sociologi e i filosofi, che hanno sviluppato teorie che dovrebbero essere tenute in considerazione per predisporre adeguate forme di tutela dei dati[158].

È bene precisare che la sorveglianza può assumere un valore sia positivo sia negativo.

Nel primo caso, ci si riferisce alle questioni di sicurezza nazionale, alla tutela del patrimonio e dell'incolumità delle persone, alla prevenzione di fenomeni terroristici; recentemente, l'uso di tecnologie di sorveglianza basate su *Big Data* ha permesso ad alcune nazioni di sviluppare strategie molto efficaci per contrastare l'epidemia Covid-19[159].

Ma la sorveglianza può invadere la *privacy*, limitare la libertà di espressione del pensiero e in generale le libertà democratiche, può agevolare la conquista e la conservazione del potere da parte di governi autoritari.

È stato osservato che "*se prive di regole, le nuove tecnologie possono alimentare un regime della sorveglianza tale da rendere l'uomo una non-persona, l'individuo da addestrare o classificare, normalizzare o escludere. Perché ogniqualvolta ciò costituisce la proiezione del sé nella dimensione digitale – il dato, appunto – viene considerato una mera cifra, da sfruttare senza considerarne l'impatto sulla persona, essa stessa si riduce a un'astrazione priva di individualità e, dunque, di dignità. E questo non solo per il lucido calcolo di profitto o per politiche statali illiberali, ma anche solo per assuefazione alla cessione indiscriminata e disattenta, di quei frammenti di libertà che sono i dati e che incorporano sempre più relazioni tra persone e rapporti di potere*"[160].

Stante il recente fenomeno della "*dataficazione*" della società, moderni studiosi hanno coniato il concetto di "*dataveglianza*"[161], per descrivere il fenomeno della sorveglianza del comportamento delle persone attraverso le tracce di dati che il loro comportamento genera.

In particolare, la teoria della dataveglianza indica che, attraverso l'uso delle informazioni digitali e dei mezzi computazionali, le autorità pubbliche o private che detengono questi dati possono

---

[158] Si veda G. ZICCARDI, *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica*, op. cit., il quale sottolinea la necessità, in questo ambito, di mantenere un approccio interdisciplinare, poiché "*le componenti giuridiche, politiche, informatiche, economiche e sociologiche sono talmente legate e interconnesse tra loro che risulta assai difficile isolare i singoli argomenti o focalizzare l'attenzione su un unico aspetto, tecnico o legale che sia*"; in particolare, questo lo si nota quando "*le riflessioni arrivano a sfiorare i temi afferenti ai diritti umani o a prendere in considerazione nuovi comportamenti portati dalla società digitale*".

[159] A. CINQUE, *Privacy, big-data e contact tracing; il delicato equilibrio fra diritto alla riservatezza ed esigenze di tutela della salute*, in *Nuova. giur. civ. comm*., 2021, p. 957; J. WU-J. WANG-S. NICHOLAS-E. MAITLAND-Q. FAN, *Application of Big Data Technology for COVID-19 Prevention and Control in China: Lessons and Recommendations*, in *J. Med. Internet Res*. 2020, vol. 22, iss. 10, pp. 1 ss.

[160] A. SORO, *Democrazia e potere dei dati*, BaldiniCastoldi, 2019, p. 23.

[161] R. CLARKE, *Information technology and dataveillance*, Communications of the ACM, 1988, 31(5), pp. 498–512.

rintracciare individui o gruppi di persone in modi più precisi, efficienti e meno costosi di quanto non fosse possibile sino a pochi anni, anche con l'uso degli elaboratori elettronici e delle banche dati.
Inoltre, "*le attuali forme di sorveglianza hanno potenzialmente un maggiore impatto e un potere modellante sulla vita quotidiana dei cittadini rispetto ai dati cartacei pre-Internet a causa dell'accessibilità delle banche dati digitali e della relativa facilità di combinazione e condivisione di diversi tipi di dati*"[162].

Le teorie della sorveglianza hanno incontrato tre fasi principali[163]:

- il progetto liberale di Bentham legato alla progettazione architettonica di una prigione e di altri edifici e la successiva analisi della disciplina di Foucault, in cui il Panopticon diviene metafora per parlare di istituzioni e società. Ciò ha posto le basi della teoria della sorveglianza sotto forma di un quadro concettuale oggi ancora attuale;
- le teorie post-panottiche della sorveglianza. La seconda fase si allontana dal Panopticon per sviluppare quadri teorici alternativi per catturare la sorveglianza. Si sviluppa in questa fase il concetto di società di controllo (ad opera di Deleuze e Guattari[164]), legata alla burocrazia e agli albori di una società informatizzata e in rete, seguite dall'assemblea di sorveglianza di Haggerty ed Ericson[165] e dal capitalismo della sorveglianza di Zuboff[166].
- concettualizzazioni contemporanee della sorveglianza. Piuttosto che sviluppare quadri teorici completi nuovi o alternativi, gran parte della teoria della sorveglianza contemporanea è caratterizzata da perfezionamenti e aggiunte ai principali quadri concettuali sviluppati in precedenza. La teoria della sorveglianza si dirama in diverse direzioni, da nuovi tipi di Panopticon e sorveglianza digitale a prospettive di partecipazione e resistenza più incentrate sull'individuo[167].

Di seguito analizzo quelle tra le principali teorie della sorveglianza che hanno rilevanza maggiore per lo studio del diritto dei dati: si tratta di teorie che aiutano a comprendere i nuovi meccanismi di sorveglianza sociale che possono essere attuati attraverso l'uso, illecito o meno, dei dati personali e, di conseguenza, si tratta di teorie fondamentali per individuare i valori sociali che il diritto alla *privacy* dovrebbe proteggere.

---

[162] M. GALIC-T. TIMAN-B.-J. KOOPS, *Bentham, Deleuze and Beyond: an overview of Surveillance theories from the Panopticon to Participation*, in *Philosophy & Technology*, Berlin, 2016, vol. 30 n. 1.
[163] Questa schematizzazione dei momenti della sorveglianza è tratta da M. GALIC -T. TIMAN -B.-J. KOOPS, *op. cit.*
[164] G. DELEUZE – F. GUATTARI, *Mille plateaux*, 1980, (ed. italiana *Mille piani, Capitalismo e schizofrenia*, a cura di P. VIGNOLA, Orthotes, 2017.
[165] K. D. HAGGERTY – R.V. ERICSON, *The surveillant assemblage*, in *British Journal of Sociology*, Vol. No. 51 Issue No. 4, 2000, pp. 605–622.
[166] S. ZUBOFF, *The age of surveillance capitalism, the fight for a human future at the new frontier of poweri*, Pubblic affairs, 2019 (ed. italiana *Il capitalismo della sorveglianza*. *Il futuro dell'umanità nell'era dei nuovi poteri*, Luiss, 2019).
[167] G. ZICCARDI, *Resistance, liberation technology and human rights in the digital age,* Springer, 2013, all'indirizzo https://www.springer.com/gp/book/9789400752757.

Come ho evidenziato, le nuove dimensioni della *privacy* impongono di riconsiderare fortemente i valori che devono essere protetti da tale settore del diritto, alla luce della nuova era tecnologica.
Ritengo che questa metodologia di analisi consenta di verificare l'efficienza e l'adeguatezza del sistema per la tutela del diritto dei dati.

4.1. La prima teorizzazione della sorveglianza: Bentham e Foucault

La teorizzazione di Bentham[168], sviluppata da Foucault, costituisce indubbiamente il primo momento storico della sorveglianza.
La prigione-Panopticon raffigura una prigione progettata come un edificio circolare, con un ispettore nella torre centrale che sorveglia le attività dei detenuti nelle loro celle. È un'idea essenzialmente architettonica, una "strategia dello spazio", ma che si traduce in un "nuovo modo di ottenere il potere della mente sulla mente in una quantità finora senza esempio". Attraverso questo design architettonico, viene creata un'illusione di sorveglianza costante: i prigionieri non sono realmente osservati costantemente, ma sanno di poter essere sorvegliati in ogni istante[169].
A differenza dell'epoca moderna, al tempo di Bentham, le possibilità di sorveglianza erano significativamente vincolate da limitazioni fisiche. La sorveglianza viene svolta da un unico punto, e l'ispettore nella sua loggia centrale possiede questo potere esteso di sorvegliare. L'ispettore è percepito come un'onnipresenza invisibile, "una macchia completamente oscura", nello spazio tutto trasparente del carcere panottico, dove si vedono i detenuti senza che essi possano sapere se e quando sono sorvegliati. È proprio l'apparente onnipresenza dell'ispettore che sostiene la perfetta disciplina nella prigione panottica: anche un'esposizione momentanea agli occhi dei prigionieri distruggerebbe l'idea della sua onnipresenza nelle menti dei prigionieri. Nella percezione dei prigionieri, l'ispettore è onniveggente, onnisciente e onnipotente.
Questa descrizione del Panopticon viene sviluppata da Foucault, che teorizza la sorveglianza come coinvolgente un ispettore che tutto vede. Foucault definisce il panottismo come "*un tipo di potere che si applica agli individui sotto forma di supervisione individuale continua, sotto forma di controllo, e punizione, e sotto forma di correzione, cioè la modellazione e la trasformazione degli individui*" [170] dove "panottico" significa "vedere tutto, tutti, sempre".
Nell'analizzare il Panopticon, Foucault spiega che dal diciottesimo e diciannovesimo secolo le società occidentali possono essere definite da una nuova forma di potere che è capillare e colpisce "gli individui, tocca i loro corpi e si inserisce nelle loro azioni e atteggiamenti, nei loro discorsi, nei

---

[168] J. BENTHAM, *Panopticon ovvero la casa d'ispezione*, a cura di M. FOUCAULT-M. PERROT, trad. italiana a cura di V. FORTUNATI, Marsilio, 1997.
[169] M. GALIC – T. TIMAN – B.-J. KOOPS, *op. cit*.
[170] M. FOUCAULT, *Sorvegliare e punire – nascita della prigione*, Einaudi, 1976.

processi di apprendimento e nella vita quotidiana". In termini più semplici, il sistema di governo penitenziario del Panopticon è diventato presente e attivo in molti o nella maggior parte degli aspetti delle società occidentali.

Attraverso questo sistema di controllo, il sorvegliato è vittima di un rapporto di potere, a cui paradossalmente si è volontariamente sottomesso, e tende, dunque, a tenere determinati comportamenti, proprio per il timore della sorveglianza continua[171].

La teorizzazione del Panopticon è certamente attuale nella nuova era digitale; come osservato, "*la vera trasformazione nella sorveglianza generalizzata per il controllo disciplinare e per l'irreggimentazione dei dominanti avviene a partire da quando sono divenutati disponibili strumenti che consentono la raccolta dei dati su larga scala e strumenti che permettono di analizzare e organizzare in modo soddisfacente i dati raccolti. Ciò è stato reso possibile dallo sviluppo tecnologico dei sistemi di sorveglianza, ovviamente, ma soprattutto dal fatto che ai dati personali "tradizionali" si sono adesso affiancati dati personali di tipo nuovo – anche questi conseguenza dello sviluppo tecnologico – che hanno finito addirittura per diventare più interessanti per il sorvegliante di quanto non lo siano i dati del vecchio tipo*"[172].

4.2. Le teorie post-panottiche

Gli studiosi più moderni della sorveglianza abbandonano la figura del Panopticon per concettualizzare la sorveglianza nelle moderne società occidentali.

Deleuze e Guattari[173] individuano nuovi luoghi di sorveglianza in un ambiente fisicamente e tecnologicamente mutato, mentre Haggerty ed Ericson[174] guardano in particolare a nuove combinazioni di esseri umani e tecnologia che esercitano forme di sorveglianza.

La questione sollevata da Deleuze e Guattari, in relazione alla sorveglianza, è che le persone non sono più rilevanti come soggetti di sorveglianza; non sono più le persone reali e i loro corpi che contano o che hanno bisogno di essere assoggettati e disciplinati, ma piuttosto le rappresentazioni dei consumatori. È il loro comportamento di acquisto, che è diventato importante da monitorare e controllare. Laddove la società si sta frammentando, lo stesso fa l'individuo; il Panopticon si offusca e l'individuo si scompone in pezzi, con la potenza del consumismo che richiede ogni tipo di attenzione da parte dei cittadini-consumatori. Nella società come descritta da Deleuze, il punto non è più plasmare gli individui, ma plasmare i consumatori: peraltro, non è importante il corpo reale-materiale dell'individuo, perché quest'ultimo è considerato come "data-body", ossia come somma di dati

---

[171] P. PERRI, *op. cit.*, p. 6.
[172] P. TINCANI, *Sorveglianza e potere. Disavventure dell'asimmetria cognitiva*, in *Ragion pratica*, 2018, I, p. 63.
[173] G. DELEUZE-F. GUATTARI, *op. cit.*
[174] K. D. HAGGERTY-R.V. ERICSON, *op. cit.*

personali che possono essere ricavati dallo stesso[175].

Anche Haggerty e Ericson osservano che non sono più gli individui materiali che vengono controllati, ma sono i loro dati personali ad esserlo: gli individui disperdono i propri dati che vengono raccolti e poi riassemblati per lo scopo necessario. I dati delle persone fluiscono, in modo incontrollabile, nel *cyberspazio* (uno spazio concettuale che combina tecnologie di Internet, realtà virtuale e telecomunicazioni convenzionali, insieme a spazi ibridi emergenti[176]) attraverso diversi database, che consentono il collegamento delle diverse fonti di flussi di dati. La sorveglianza non è statica, ma è mutevole, è la rete di rapporti di potere e di conoscenza, è un fenomeno malleabile, fluido e instabile, che scorre sempre attraverso il *cyberspazio*; la sorveglianza è deterritorializzata ed opera – in metafora – come un rizoma: il controllo sociale oggi è decentralizzato e mutaforma, non è focalizzato solo sulla raccolta di informazioni ma su decodificare e ricodificare, ordinare, alterare, far circolare e riprodurre le informazioni[177].

4.3. (Segue) Il capitalismo della sorveglianza di Zuboff

Tra le teorie post-panottiche, merita particolare attenzione, per lo studio del diritto dei dati, quella recentemente sviluppata da Zuboff[178], il filone cd. neomarxista della sorveglianza, la quale delinea i contorni di un altro quadro teorico, il capitalismo della sorveglianza, analizzando come la sorveglianza abbia modificato le strutture di potere nell'economia dell'informazione. Quest'autore supera i modelli di analisi di Bentham e Foucault, sostenendo che sono necessari nuovi strumenti analitici per lo studio della società del controllo.

Zuboff afferma che il capitalismo della sorveglianza "*si appropria dell'esperienza umana usandola come materia prima da trasformare in dati sui comportamenti. Alcuni di questi dati vengono usati per migliorare prodotti o servizi, ma il resto diviene un surplus comportamentale privato, sottoposto a un processo di lavorazione avanzato noto come "intelligenza artificiale" per essere trasformato in prodotti predittivi in grado di vaticinare cosa faremo immediatamente, tra poco e tra molto tempo. Infine, questi prodotti predittivi vengono scambiati in un nuovo tipo di mercato per le previsioni comportamentali, che io chiamo mercato dei comportamenti futuri. Grazie a tale commercio i capitalisti della sorveglianza si sono arricchiti straordinariamente, dato che sono molte le aziende bisognose di conoscere i nostri comportamenti futuri"*[179].

---

[175] M. GALIC-T. TIMAN-B.-J. KOOPS, *op. cit.*

[176] M. DODGE-R. KITCHIN, *Code/space: software and everyday life*, Massachusetts: MIT Press, 2011.

[177] M. GALIC-T. TIMAN-B.-J. KOOPS, *op cit.*

[178] S. ZUBOFF, *op. cit.*

[179] S. ZUBOFF, *Il capitalismo della sorveglianza*, cit., p. 17-18. In questa parole non può non leggersi una fortissima assonanza con quanto è accaduto nel caso Cambridge Analytica, vicenda che ha messo in luce le pericolose conseguenze

Si tratta di una "teoria onnicomprensiva" su "scala di civiltà"[180], secondo cui il capitalismo della sorveglianza pervade costantemente ogni livello della società[181], grazie alla diffusione totale di strumenti costantemente connessi che generano costanti flussi di dati, i quali vengono raccolti per sviluppare modelli predittivi e di modifica, istantanea ed in tempo reale, del comportamento, Questi modelli vengono venduti sul mercato, secondo la regola che prevede che "*un individuo vale meno delle scommesse altrui sul suo comportamento*"[182].

Anche quando gli utenti sono consapevoli di questa costante estrazione dei dati, vi consentono: i capitalisti della sorveglianza dall'un lato ripetono che la condivisione de dati è facoltativa da parte dell'utente, ma dall'altro i clienti che si rifiutano di condividerli ricevono un prodotto con funzionalità limitate[183].

Il capitalismo della sorveglianza è una nuova sottospecie del capitalismo (dell'informazione) che si è gradualmente costituita nell'ultimo decennio, in cui "i profitti derivano dalla sorveglianza unilaterale e dalla modifica del comportamento umano"[184], che avviene istantaneamente ed in tempo reale, senza che l'utente se ne accorga, perché gli algoritmi sono in grado di prevedere il comportamento ipotetico dell'utente a determinati stimoli.

I big data sono la componente fondamentale di questa nuova logica economica, che si basa su estrazioni di dati, loro rielaborazione algoritmica (che genera, attraverso l'aggregazione, un "surplus comportamentale e informativo"), previsione e monetizzazione: viene venduto l'accesso al flusso in tempo reale della vita quotidiana delle persone al fine di influenzare e modificare direttamente il loro comportamento a scopo di lucro[185]. Si viene, dunque, a creare "*un panopticon ancora più pervasivo di quello immaginato da Foucault, in quanto la possibilità di modificare i comportamenti dei "sorvegliati" è ancora più immediata da realizzare, proprio in virtù della profonda conoscenza predittività tipica dei* big data"[186].

Zuboff cerca di dimostrare che la sorveglianza come parte fondamentale della nuova logica dell'accumulazione dei dati va ben oltre le considerazioni sulla *privacy*. Cerca di dimostrare che minaccia la democrazia stessa, perché elimina il canone politico del moderno ordine liberale, che è

---

a cui può portare l'utilizzo illecito dei dati personali: si tratta di conseguenze gravissime per gli individui, i cui dati personali sono stati acquisiti e utilizzati illecitamente per modificare il comportamento elettorale degli americani, arrivando persino a reprimerlo, ossia convincendo taluni cittadini a non recarsi alle urne.

[180] M. GALIC -T. TIMAN-B.-J. KOOPS, *op. cit.*

[181] S. ZUBOFF, *The Secrets of Surveillance Capitalism,* Frankfurter Allgemeine, Feuilleton, 2016, all'indirizzo https://www.faz.net/aktuell/feuilleton/debatten/the-digital-debate/shoshana-zuboff-secrets-of-surveillance-capitalism-14103616.html.

[182] S. ZUBOFF, *Il capitalismo della sorveglianza*, *op. cit.*, p. 103.

[183] EAD., *op. ult. cit*, pp. 250-252.

[184] EAD., *Big other: surveillance capitalism and the prospects of an information civilization*. Journal of Information Technology, 2015, 30, pp. 75–89, all'indirizzo https://journals.sagepub.com/doi/pdf/10.1057/jit.2015.5.

[185] M. GALIC -T. TIMAN -B.-J. KOOPS, *op. cit.*

[186] P. PERRI, *op. cit.*, p. 17.

stato definito dai principi fondamentali dell'autodeterminazione, nella vita privata e nelle relazioni sociali degli individui, nella politica e nel governo.
Il pensiero di Zuboff si dimostra illuminante per spiegare la moderna realtà tecnologica.

4.4. Cenni sulle teorie della "terza fase" della sorveglianza

Alcuni autori hanno osservato che, con l'aumento delle dimensioni e della complessità dei metodi di sorveglianza, sembra quasi impossibile sviluppare una teoria generale della sorveglianza che catturi la sorveglianza come un concetto o un fenomeno largamente unitario.
In questa "terza fase" gli studiosi, piuttosto che sviluppare teorie generali onnicomprensive, tendono a spiegare determinate ipotesi o concetti, perfezionando e adattando le teorie sviluppate nella fase prima e seconda.
Tali teorie sono tutte strettamente legate alle tecnologie e al continuo sviluppo di strumenti tecnologici, con la conseguenza che gli stessi autori sono consci che i concetti definiti sono presto destinati a mutare[187]. Essendo impossibile menzionare tutte le differenti concezioni, mi limito a quelle che hanno un'attinenza maggiore con l'uso dei dati e i diritti che ne sono connessi.
Alcuni autori hanno coniato la nuova definizione di oligopticon, in cui "*la sorveglianza consiste in un insieme di punti di vista parziali da posizioni fisse con capannoni di vista limitati*"[188].
Innanzitutto, si evidenzia che non esiste un unico sorvegliante perché gli stessi sorvegliati a loro volta esercitano la sorveglianza. Inoltre, il sorvegliante non dovrebbe necessariamente svolgere una sorveglianza continua per raggiungere sempre il suo risultato, in quanto in talune situazioni gli sono necessari pochi dati. Questi autori citano l'esempio dell'impiegata dell'università che deve gestire le lezioni e gli esami: non deve sapere in ogni momento cosa fanno gli studenti, ma le è necessario avere la lista degli iscritti ai vari corsi, l'orario delle lezioni, la disponibilità delle aule[189]. Dunque, spiegano che i data base contengono pochi dati; il punto è che l'interazione e la connessione tra tali data base consente di aumentare la sorveglianza in modo esponenziale, proprio come accade quando gli individui utilizzano strumenti tecnologici connessi che scambiano flussi di dati[190].
Un altro autore ha sviluppato l'idea del banopticon, ossia della sorveglianza finalizzata ad escludere determinati individui o gruppi di individui. Si tratta di una teoria sviluppata per spiegare il fenomeno del terrorismo, che si è sviluppata dopo gli attentati dell'11 settembre. Secondo questa concezione, diversi *data base*, che conterrebbero solo frammenti di dati quasi insignificanti, vengono combinati tra di loro per identificare quei soggetti "*che non si conformano alle regole di ingresso e di accesso*

---

[187] M. GALIC -T. TIMAN- B.-J. KOOPS, *op. cit.*
[188] M. DODGE-R. KITCHIN, *Code/space: software and everyday life*, MIT Press, 2011.
[189] P. PERRI, *op. cit.*, p. 19.
[190] *Ibidem*.

in una determinata società"[191].

Nel banopticon la profilazione è attuata per individuare soggetti specifici per bloccarne i movimenti e vietarne l'accesso nella società: esso è permesso da leggi eccezionali che limitano le libertà degli individui, i quali sono portati ad accettarle per lo stato di costante disagio e di insicurezza globale in cui si trovano. Questo modo di pensare ha portato all'introduzione di nuove tecnologie di sorveglianza, come i *body scanner* negli aeroporti, i passaporti biometrici e ad algoritmi che studiano in tempi reale i video di sorveglianza per individuare movimenti sospetti (come introdotti in alcuni aeroporti o stazioni metropolitane per evitare attacchi terroristici).

Peraltro, non può non notarsi un'analogia con la recente introduzione del Green Pass europeo per i vaccinati Covid-19: si tratta di una tecnologia di sorveglianza che consente, attraverso l'identificazione personale, di monitorare gli spostamenti della popolazione vaccinata per regolarizzare l'ingresso degli individui in una data società.

5. Nuove prospettive legislative: Digital Services Act e Digital Markets Act

Soro ha affermato che il GDPR ha tentato di arginare "*la concentrazione illegittima di potere fondata sullo sfruttamento di quei frammenti di libertà che sono i nostri dati, tracciando il limite tra capitalismo digitale e capitalismo estrattivo o della sorveglianza*"[192].

In effetti, nei confronti del recente sviluppo tecnologico, l'UE sta valutando l'adozione di ulteriori misure per tutelare gli individui.

Le istituzioni dell'Unione stanno iniziando a considerare il tema della sorveglianza e del controllo sociale che avvengono attraverso i *Big Data*; peraltro, è divenuto evidente che mentre prima le informazioni erano raccolte e conservate principalmente dalle autorità statali, con la conseguenza che il tema del trattamento dei dati si risolveva nel bilanciamento tra potere pubblico e sfera privata, ora il patrimonio di conoscenza è detenuto principalmente da pochi attori privati internazionali, di dimensioni gigantesche[193]: le conseguenze negative di tale ultima evoluzione sono state evidenziate nella parte relativa alle teorie della sorveglianza.

È questo un tema cruciale della *data protection*: l'esigenza di una cooperazione delle piattaforme (o di un'imposizione del legislatore) per "*impedire che la rete divenga uno spazio anomico dove impunemente si possano violare diritti, senza tuttavia ascrivere loro un ruolo arbitrale rispetto alle libertà fondamentali e al loro bilanciamento, da riservare pur sempre all'autorità pubblica*"[194].

---

[191] D. BIGO, *Globalized (in)security: the field and the Ban-opticon,* in N. SAKAI-J. SOLOMON, *Traces 4: Translation, Biopolitics, Colonial difference,* Hong Kong, 2006, pp. 109-156.
[192] A. SORO, *op. cit.*, p. 29.
[193] AUTORITÀ GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Indagine conoscitiva sui big data*, 2020.
[194] *Ibidem.*

Per una più efficiente regolamentazione delle piattaforme digitali, l'Unione Europea ha in progetto di adottare due Regolamenti, il Digital Services Act (DSA) e Digital Markets Act (DMA).

Il primo è finalizzato ad introdurre forme di responsabilizzazione delle piattaforme, il cui potere di moderazione dei contenuti viene assoggettato ad obblighi di trasparenza e a rimedi impugnatori che ne consentano una verifica esterna; il DMA è finalizzato a stabilire condizioni di parità per promuovere l'innovazione, la crescita e la competitività, sia nel mercato unico europeo che a livello globale.

Il DSA (più rilevante per la presente analisi) si pone lo scopo di regolamentare il *microtargeting* fondato sulle tecniche psicometriche/psicografiche, che, utilizzando dati personali e non, influenza il comportamento dell'utente. In particolare, esso prescrive che le piattaforme informatiche debbano fornire agli utenti un'informativa che consenta loro di comprendere il funzionamento degli algoritmi che propongono pubblicità e messaggi. Quest'informativa deve indicare i principali parametri utilizzati dall'algoritmo, con spiegazioni rilevanti sulla logica seguita dallo stesso, nonché sulle metodologie di profilazione dell'utente.

La proposta di Regolamento prevede che "*le prescrizioni del presente regolamento sulla fornitura di informazioni relative alla pubblicità lasciano impregiudicata l'applicazione delle pertinenti disposizioni del regolamento (UE) 2016/679, in particolare quelle riguardanti il diritto di opposizione e il processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione e specificamente la necessità di ottenere il consenso dell'interessato prima del trattamento dei dati personali per la pubblicità mirata*" (Considerando n. 52).

Questi regolamenti europei hanno lo scopo espresso di contrastare il "capitalismo estrattivo" delle piattaforme e per la tutela dell'autodeterminazione informativa, "*che presuppone del resto, come ha chiarito una recente sentenza di legittimità, la piena conoscenza della logica algoritmica applicata al trattamento, che deve essere inclusa dunque nell'oggetto del consenso. L'autodeterminazione informativa è, infatti, il necessario presupposto di scelte libere e, appunto, consapevoli, in un contesto in cui servizi apparentemente gratuiti sono invece pagati al caro prezzo dei nostri dati e, quindi, della nostra libertà*"[195].

V'è da evidenziare, dunque, che il DSA si propone di regolamentare il complesso fenomeno del *microtargeting* attraverso lo strumento – ormai comune nel tema qui trattato – dell'informativa all'utente: si tratterà, probabilmente, dell'ulteriore "banner" a piè di pagina (come quello relativo ai *cookies*), che nessun utente leggerà.

[195] AUTORITÀ GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Relazione 2020*, pp. 10-11.

6. Riflessioni conclusive

Nel percorso evolutivo che ha portato all'affermazione del diritto alla protezione dei dati, quale espressione del diritto alla *privacy*, ha dunque rivestito un ruolo fondamentale il contesto tecnologico in cui è avvenuto questo riconoscimento.

Il diritto alla protezione dei dati è stato tradizionalmente inteso quale diritto alla personalità, in una veste propriamente di diritto soggettivo individuale. Per giungere alla dimostrazione di tale assunto, è stato necessario ripercorrere brevemente i primi sviluppi del diritto alla *privacy*, avvenuti nel sistema nordamericano. Di questa ricostruzione dogmatica costituiscono tappe fondamentali le teorie statunitensi di Warren-Brandeis, Faulkner, Prosser e Westin.

Parallelamente, sono state viste le principali sentenze della Corte Suprema USA che si sono occupate del tema, sino al riconoscimento del diritto alla *privacy* con il caso Katz v. United States: ne è emersa la concezione di diritto alla riservatezza quale diritto dell'individuo in una chiave prettamente individualistica.

È questa la prospettiva che dall'ordinamento statunitense è approdata nella prima dottrina italiana occupatasi del tema, che si è "appropriata" del concetto di *privacy* in chiave puramente soggettivo-individualista.

Questa concezione del diritto alla *privacy* ha condizionato il successivo inquadramento del diritto alla protezione dei dati personali, che da sempre viene analizzato in una chiave principalmente privatistica e da una prospettiva antropocentrica. È evidente che il diritto alla protezione dei dati personali ha numerosi punti di contatto con il diritto alla riservatezza, il diritto all'identità personale, il diritto all'autodeterminazione.

Lo sviluppo tecnologico degli anni '60, in particolare il diffondersi delle banche dati e degli elaboratori elettronici, ha fatto sorgere un nutrito dibattito dottrinale in merito alla necessità di riconoscere tutele specifiche per la protezione dei dati personali.

La creazione di un mercato digitale europeo, nel quale i dati vengono scambiati dagli utenti al fine di ottenere servizi, dimostra che il diritto alla protezione dei dati enuclea in sé anche un valore patrimoniale, come evidenziato dalla più recente dottrina e giurisprudenza, nonché dai più recenti provvedimenti legislativi europei che si stanno occupando di questo tema.

L'evoluzione esponenziale delle nuove tecnologie dell'epoca moderna (in particolare la creazione di internet, le piattaforme informatiche, i *social network*, lo sviluppo dell'intelligenza artificiale e gli algoritmi predittivi) mette in crisi la concezione tradizionale del diritto alla protezione dei dati personali. Tali strumenti, infatti, rischiano di rendere del tutto inefficiente ed inadeguato un sistema di tutela basato su una concezione meramente individualistica del diritto alla protezione dati: tutta la disciplina del trattamento dei dati ruota, infatti, attorno ai concetti di consenso e di informazione

dell'utente, categorie classiche di diritto civile che poco s'attagliano per le nuove istanze sociali di protezione dei dati.

È noto che ormai dagli anni '70 una parte della dottrina ha iniziato a sottolineare il "valore sociale" della *privacy* e i nuovi rischi per la società derivanti dall'utilizzo dei dati personali. Di qui l'esigenza di individuare i nuovi valori sociali cui dovrebbe tendere una disciplina adeguata per la protezione dei dati, nonché individuare i pericoli per l'utente e la collettività derivanti dal trattamento illecito dei dati personali.

La dottrina moderna ha sottolineato, infatti, che l'utilizzo sempre più diffuso dei dati personali ha innescato una "*cultura della sorveglianza*"[196]. Gli utenti vengono monitorati costantemente sul web e tramite gli strumenti stabilmente connessi alla rete (*smartphone*, dispositivi indossabili, automobili, prodotti *smart* per la casa) viene realizzata un'operazione di controllo sociale, che pregiudica fortemente il diritto degli individui ad autodeterminarsi ed al libero arbitrio. Esistono, infatti, nuovi strumenti algoritmici che consentono non solo di controllare gli individui, ma soprattutto di influenzarne il comportamento, portandoli a compiere scelte che non avrebbe compiuto o, anche, a reprimere la volontà dell'individuo di tenere un certo comportamento che, invece, avrebbe tenuto.

Questi rischi collettivi sono stati analizzati dalla filosofia del diritto e dalla sociologia, scienze che si sono occupate del fenomeno del controllo sociale, anche nell'era digitale.

Le teorie della sorveglianza sociale, suddivise nelle c.d. "tre fasi", dimostrano l'esistenza di possibili risvolti negativi per la collettività; per tale motivo, dovrebbe trovare accoglimento quella proposta[197] volta a far sì che i *Big Data* considerino maggiormente i rischi sociali e siano orientati al perseguimento di un fine etico e sociale positivo.

---

[196] D. LYON, *La cultura della sorveglianza*. *Come la società del controllo ci ha reso tutti controllori*, Luiss University Press, 2020.

[197] D. WRIGHT, K. WADHWA, M. LAGAZIO, C. RAAB, E. CHARIKANE, *Integrating privacy impact assessment in risk management,* in *Data Privacy Law,* Vol. 4, No. 2, 2014, pp. 155-170; D. WRIGHT, *A framework for the ethical impact assessment of information technology* in *Ethics and Information Technology,* 2011, pp. 199-226.

Capitolo III

SOGGETTI E PRESUPPOSTI DI LICEITÀ DEL TRATTAMENTO

SOMMARIO: 1. Le figure soggettive del trattamento. - 2. L'interessato dal trattamento. - 2.1. *La tutela dei dati di defunti e nascituri.* - 2.2. *Forme di tutela "aggregata".* - 3. Il titolare del trattamento: dalla disciplina previgente al GDPR. - 4. Il responsabile del trattamento. - 5. La contitolarità nel trattamento ex art. 26 GDPR. - 6. Il responsabile "interno": inammissibilità della figura. - 7. Il DPO ex art. 37 GDPR. - 8. Presupposti e modalità del trattamento dei dati: premessa. - 9. Il principio di liceità. - 10. Il principio di necessità. - 11. Analisi delle condizioni di liceità ex art. 6 alla luce dei principi di liceità ex art. 5. - 12. Il consenso come condizione di liceità. - 12.1. *(segue) La libertà del consenso.* - 12.2. *(segue) Il consenso e l'attività di marketing attraverso profilazione.* - 12.3. *(segue) Il problema del consenso nell'attuale società tecnologica.* - 13. Il trattamento necessario per l'esecuzione dei contratti per i servizi digitali. - 14. Il legittimo interesse del titolare. - 15. Il principio di correttezza e trasparenza (alla luce della liceità). - 16. Il principio di finalità. - 17. Il principio della qualità dei dati. - 18. Il principio di accountability. - 19. Riflessioni conclusive.

1. Le figure soggettive del trattamento

Il GDPR ha un esteso ambito di applicazione materiale[198], in quanto ha per oggetto ogni trattamento "*interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi*" (art. 2): peraltro, le stesse definizioni di "dato personale"[199] e di "trattamento"[200] adottate dal regolamento sono estremamente estese, andando a ricomprendere qualsiasi dato da cui possa risultare identificabile un individuo, nonché ogni operazione, anche estremamente limitata, che abbia ad oggetto dati personali.

---

[198] G. ALPA, *La disciplina dei dati personali. Note esegetiche sulla legge 31 dicembre 1996, n. 675 e successive modifiche*, op. cit., 1998; A. SPANGARO, *L'ambito di applicazione materiale della disciplina del Regolamento*, in *La protezione dei dati personali in Italia,* diretto da G. FINOCCHIARO, Zanichelli, 2019, p. 28; R. PARDOLESI, *Diritto alla riservatezza e circolazione dei dati personali*, Giuffrè, 2003.

[199] L'art. 4, n. 1), prevede che per "dato personale" s'intende "*qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"; si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale*".

[200] L'art. 4, n. 2), definisce il "trattamento" come "*qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione*".

Questa impostazione dimostra l'attenzione riservata dal legislatore europeo alla disciplina della protezione dei dati personali, considerata parte integrante dei diritti fondamentali e della persona e, al tempo stesso, strumento essenziale per la regolamentazione del mercato interno e per garantire una crescita efficiente del mercato digitale, in condizioni di paritaria concorrenza.

La disciplina complessiva emergente dal Regolamento è quella di un sistema di tutela che affida ad Autorità pubbliche compiti e poteri di sorveglianza e controllo, anche di tipo sanzionatorio, nell'ambito del quale la responsabilità civile costituisce solo uno dei meccanismi atti alla protezione dei dati personali: la tutela civilistica si affianca e dovrebbe essere complementare alla tutela posta in essere dall'Autorità di controllo pubblico.

Come vedremo *infra*, il GDPR ruota attorno al principio di responsabilizzazione del titolare: si individua il soggetto che ha il potere di controllo sui dati e questo soggetto diviene responsabile di attuare il trattamento dei dati secondo una prospettiva di gestione dei rischi che dagli stessi possono derivare per i diritti e le libertà degli interessati. Individuato questo soggetto, il GDPR ne fa conseguire, dunque, la necessaria responsabilità di risarcire i danni materiali o immateriali causati agli interessati a causa di trattamento illecito. Infatti, l'art. 82, par. 2, afferma che "*un titolare del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento che violi il presente regolamento. Un responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento*".

È dunque essenziale soffermarsi sull'analisi delle differenti figure soggettive coinvolte nel trattamento dei dati, per verificare chi sia effettivamente tenuto a risarcire i danni determinati dall'illecito trattamento[201], nonché analizzare i principi che devono conformare le attività di trattamento, in particolare l'*accountability* e il principio della gestione dei rischi. Si tratta di temi che saranno essenziali per definire la natura della responsabilità da illecito trattamento di dati, nonché il regime della prova liberatoria per il danneggiante.

2. L'interessato dal trattamento

[201] Sul tema la dottrina è amplissima. *Cfr.* E. GIANNANTONIO-M. G. LOSANO-V. ZENO-ZENCOVICH, *La tutela dei dati personali. Commentario alla L. 675/1996*, Cedam, 1997; V. CUFFARO-V. RICCIUTO, *Il trattamento dei dati personali*, Giappichelli, 1999; A. SCALISI, *Il diritto alla riservatezza*, Giuffrè, 2002; E. PELLECCHIA, *La responsabilità civile per trattamento dei dati personali*, in *Resp. civ. e prev*., 2005, pp. 232 ss.; R. PARDOLESI, *Diritto alla riservatezza e circolazione dei dati personali*, Giuffrè, 2003; R. PANETTA, *Libera circolazione e protezione dei dati personali*, Giuffrè, 2006; V. CUFFARO-R. D'ORAZIO-V. RICCIUTO, *Il codice del Trattamento dei dati personali*, Giappichelli, 2007; C. BIANCA-M. BUSNELLI, *La protezione dei dati personali*, Cedam, 2007; G. FINOCCHIARO, *Privacy e protezione dei dati personali. Disciplina e strumenti operativi*, Zanichelli, 2012.

L'art. 4 del Regolamento n. 2016/679/UE (GDPR), rubricato «*Definizioni*», non elenca la nozione di «interessato» dal trattamento[202]. Quest'ultima, nondimeno, è ricavabile dalla definizione di «dato personale»: ai fini del citato Regolamento s'intende per «dato personale» "*qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente*, […]".

Pertanto, «interessato» al trattamento – c.d. *data subject* – è la persona fisica, identificata (perciò distinguibile) o identificabile, alla quale si riferiscono i dati personali.

Il Legislatore europeo fa menzione della sola persona fisica, dovendosi escludere dal perimetro della nozione in esame le persone giuridiche, gli enti e le associazioni[203]. Tale esclusione, peraltro, implica unicamente che, in seguito a condotte di illecito trattamento di dati che abbiano cagionato un danno, le persone giuridiche non potranno esercitare i diritti previsti nel Regolamento, rimanendo integra, all'opposto, la possibilità di avvalersi pienamente dei mezzi di tutela offerti dalla normativa interna degli Stati. Analogamente, nella Convenzione n. 108/1981 del Consiglio d'Europa[204] è stato previsto come la protezione dei dati interessa, primariamente, la tutela delle persone fisiche, ferma la possibilità per le parti contraenti di estendere, nel rispettivo diritto nazionale, la protezione dei dati alle persone giuridiche, quali società e associazioni[205].

Quanto alla normativa italiana, il Codice in materia di protezione dei dati personali (d.legis.

---

[202] Il dettato normativo, comunque, si concentra sul concetto di consenso dell'interessato come "*qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento*".

[203] Così previsto dal *Considerando* 14, GDPR. Nel caso di imprese individuali possono costituire dati personali quelli che consentono l'identificazione di una persona fisica. Sul punto, si veda la sentenza della Corte di Giustizia, 9 marzo 2017 nella causa C-398/15, *Manni*.

[204] La Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (Convenzione n. 108) è stata ratificata dall'Italia con la legge 21 febbraio 1989, n. 98. L'ambito di applicazione di tale Convenzione si estende a tutti i trattamenti di dati personali effettuati sia nel settore privato che nel settore pubblico. Essa offre tutela rispetto ad eventuali abusi che possono derivare dal trattamento, specifica il principio del consenso informato, cerca di regolamentare il flusso transfrontaliero dei dati personali, individua i principi cardine di correttezza e liceità posti a presidio della raccolta e del trattamento automatizzato dei dati, individua come prioritaria l'indicazione degli scopi legittimi della raccolta e del trattamento dei dati stessi, che devono essere conservati non oltre il tempo necessario, in ragione della loro adeguatezza, pertinenza, non eccedenza (proporzionalità) nonché esattezza. La Convenzione vieta, inoltre, il trattamento dei dati sensibili come razza, opinioni politiche, salute, religione, orientamento sessuale o precedenti giudiziari di una persona fisica e continua ad essere lo standard internazionale condiviso sia dagli Stati membri che dagli Stati non membri e da alcuni paesi extraeuropei che vi hanno aderito.

[205] Il diritto alla protezione contro l'uso di dati delle persone giuridiche è stato valutato non tanto alla luce della violazione dell'art. 8 CEDU ma ancorato al rispetto del domicilio e della corrispondenza. Sul punto, si veda Corte EDU, *Bernh Larsen Holding AS e a. c. Norvegia*, n. 24117/08, 14.3.2013. Tuttavia, cfr. anche Corte EDU, *Liberty e a. c. Regno Unito*, n. 58243/00, 1.7.2008. La Corte di Giustizia dell'Unione Europea, nelle cause riunite C-92/09 e C-93/09, *Volker und Markus Schecke GbR* e *Hartmut Eifert c. Land Hessen*, 9.11.2010, punto 5353, ha confermato la piena libertà, per i legislatori nazionali, di esercitare la propria discrezionalità nel disciplinare tale materia.

30.6.2003, n. 196), prima degli interventi modificativi, dell'emanazione della normativa europea e del decreto interno di adeguamento, definiva, all'art. 4, comma 1, lett. i), l'«interessato» come "*la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali*". Dall'un lato, veniva omesso il richiamo alla qualifica di soggetto "identificato o identificabile" (esplicitato, invece, nella nozione di «dato personale»[206]), dall'altro, venivano inclusi, nel perimetro di tale nozione, soggetti, all'opposto, estromessi dal contesto in seguito inaugurato dal GDPR.

Trattasi, comunque, di definizione non più attuale. L'art. 4 del Codice della Privacy («*Definizioni*»), unitamente a molte altre disposizioni dello stesso, sono state definitivamente abrogate per effetto del d.lgs. n. 101/2018 volto all'adeguamento della normativa nazionale rispetto alle disposizioni europee.

Chiarito chi può rivestire la qualità di «interessato», sul versante della responsabilità civile per illecito trattamento dei dati personali e del risarcimento del danno il referente normativo è rappresentato dall'art. 82 del GDPR.

La norma si struttura tipizzando le figure soggettive che rilevano nello specifico contesto del trattamento dei dati personali – in specie, Titolare e Responsabile – e le relative condotte, ma intende, comunque, costruire la fattispecie attorno al soggetto debole di tale rapporto asimmetrico.

Con riferimento al soggetto titolare del rimedio risarcitorio, un primo orientamento ritiene che l'utilizzo del termine "chiunque"[207] è da intendersi nel senso che è all'interessato, se e in quanto anche danneggiato, che viene riconosciuto il diritto di azionare i mezzi per tutelare la propria sfera giuridica lesa da un'attività di trattamento illecito non conforme ai precetti conformativi protettivi del GDPR.

Una diversa tesi[208], invece, argomenta che l'utilizzo del termine "chiunque" permetta di estendere la tutela risarcitoria fino a comprendere, non solo le persone prossime all'interessato (ad esempio i familiari, su cu cui v. *infra* il par. seguente), ma anche terzi rispetto allo stesso, che pur non vantando un diritto alla protezione dei propri dati personali, subiscano un pregiudizio derivante dal trattamento illecito di dati personali altrui (ad esempio, il soggetto che abbia riposto un affidamento sulla correttezza di una banca dati creata dal titolare).

---

[206] La normativa del 2003 definisce «dato personale» "qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale".

[207] Tale espressione non è da intendersi come evocativa di un soggetto non qualificato, come quel «chiunque» ai sensi dell'art. 2043 c.c. che ponga in essere una condotta illecita contraria alle norme dell'ordinamento. All'opposto, identifica quel soggetto alla cui identità il dato personale oggetto di trattamento si riferisce, per tale motivo interessato, e che, in ragione dell'illegittimità di tale attività, subisca un danno materiale o immateriale e rivesta, pertanto, altresì la posizione di danneggiato. Così TOSI E., *Trattamento illecito dei dati personali, responsabilità oggettiva e danno non patrimoniale alla luce dell'art. 82 del GDPR UE,* in *Danno e resp.*, 2020, pp. 434 ss. Sulla responsabilità del «chiunque» ai sensi dell'art. 2043 c.c. si veda CASTRONOVO C., *La nuova responsabilità civile*, Milano, 2018, p. 180.

[208] M. GAMBINI, *op. cit.*, p. 47.

2.1. La tutela dei dati di defunti e nascituri

Posto che il diritto alla protezione dei dati costituisce specificazione ed ampliamento del diritto alla libertà e alla inviolabilità della vita privata[209], entrambi riferibili agli esseri umani, è dubbia l'applicabilità della normativa contenuta nel GDPR anche ai dati di defunti e nascituri.

Per la precisione, il *Considerando* 27 esclude l'applicazione della normativa GDPR ai dati delle persone decedute ma statuisce al contempo una clausola di salvaguardia che apre la possibilità per gli Stati membri di prevedere diversamente sul punto. Il d.lgs. 10.8.2018 n. 101, modificativo del previgente Codice italiano in materia di Privacy, ha, per l'appunto, espressamente esteso le tutele previste dal GDPR anche al trattamento dei dati dei soggetti deceduti.

A norma dell'art. 2-*terdecies*, comma 1°, del citato decreto, "*i diritti di cui agli articoli da 15 a 22 del Regolamento riferiti ai dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato, in qualità di suo mandatario, o per ragioni familiari meritevoli di protezione*". La norma ammette poi la possibilità, per l'interessato, tramite dichiarazione scritta, di vietare l'esercizio dei diritti di cui al comma 1°, di revocare o modificare il divieto precedentemente espresso, con la precisazione che "*in ogni caso, il divieto non può produrre effetti pregiudizievoli per l'esercizio da parte dei terzi dei diritti patrimoniali che derivano dalla morte dell'interessato nonché del diritto di difenderne in giudizio i propri interessi*".

Vengono individuati come legittimati a richiedere e ottenere l'accesso ai dati di un soggetto defunto coloro che siano titolari di un interesse proprio o che agiscano per finalità di tutela di questo in veste di mandatari o per ragioni familiari. È il caso, ad esempio, del legittimario pretermesso, di un coerede o legatario; dell'esecutore testamentario che ritenga lesa la dignità del defunto; dei soggetti che, in forza di un contratto *inter vivos*, hanno ricevuto l'incarico di compiere una determinata attività, ad esempio cancellare o consegnare i dati del mandante; del familiare che ritenga una pubblicazione presente su un *social network* lesiva degli interessi del proprio nucleo familiare.

Trattasi di soggetti che potrebbero o essere titolari di un diritto acquisito *mortis causa* o legittimati *iure proprio*[210].

Tale richiesta di accesso potrà investire i dati personali della persona deceduta, le finalità del trattamento, le categorie di dati, i destinatari o le categorie di destinatari a cui i dati sono o saranno comunicati, il periodo di conservazione dei dati o i criteri utilizzati per determinarlo, l'origine dei dati, l'esistenza di un processo decisionale automatizzato, compresa la profilazione o trasferimento

---

[209] F. PIZZETTI, *Privacy e Diritto europeo della protezione dei dati personali. Dalla Direttiva 95/46 al Nuovo Regolamento Europeo, I Diritti nella "rete" della rete,* Giappichelli, 2016, pp. 6-19; 23-35; 175-177, 182-196.

[210] G. RESTA, *La successione nei rapporti digitali e la tutela post mortale dei dati personali*, in *Contr. e impr*., 2019, p. 99.

dei propri dati fuori dall'Unione europea.

In realtà, comunque, nonostante il citato *Considerando* 27, il Regolamento 679/2016 si dimostra uno strumento giuridico essenziale onde ottenere copia dei beni digitali di appartenenza di un soggetto defunto e memorizzati all'interno di un *account* a quest'ultimo riferibile. Si ricordi, infatti, che la normativa europea è pienamente applicabile ai Titolari che risiedano al di fuori dell'Unione Europea ma che realizzino operazioni di trattamento dati appartenenti ad interessati che si collocano all'interno di questo spazio[211].

Si pensi ai fornitori di servizi della società dell'informazione con sede negli Stati Uniti. L'invocazione (esasperazione?) del principio di tutela della riservatezza del defunto (nonché delle controparti - c.d. *partner* - delle comunicazioni, nel caso di conversazioni private) dietro cui i fornitori si trincerano al fine di negare la possibilità, per gli eredi, di accedere ai dati digitali del *de cuius*, si rivela del tutto inconsistente.

In primo luogo, se è vero che il contratto atipico per la fornitura di un servizio (o di un bene digitale) si trasferisce *mortis causa* come ogni altro rapporto contrattuale, è altrettanto vero che, anche ai fini dell'effettivo subentro degli eredi nel contratto (e, quindi, nella gestione dell'*account*) il trattamento dei dati del defunto relativi all'*account* (ivi compreso il trattamento dei dati dei *partner* di comunicazione) da parte degli eredi deve considerarsi lecito ex art. 6, par. 1, lett. b) GDPR, prima ancora che necessario[212].

In secondo luogo, gli eredi sono quasi sempre portatori di un "interesse legittimo"[213] ad accedere agli *account* del defunto (è il caso, ad esempio, dell'interesse alla tutela di diritti derivanti dalla successione, alla loro difesa, ecc.) ragione per la quale, anche prescindendo dal subentro nel contratto, potrebbe essere invocato anche l'art. 6, par. lett. f) che renderebbe comunque lecita la comunicazione dei dati del defunto e il loro trattamento[214]. Il trattamento dei dati necessario per la tutela degli interessi legittimi degli eredi, infatti, deve prevalere rispetto agli interessi e ai diritti alla protezione

---

[211] Si veda l'art. 3, par. 2, Regolamento UE n. 679/2016 "2. Il presente regolamento si applica al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano: a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione".

[212] G. RESTA, *La successione nei rapporti digitali e la tutela post mortale dei dati personali*, cit., p. 99; La trasmissione e la messa a disposizione presso l'*account* del defunto di messaggi e contenuti condivisi del *partner* di comunicazione avviene anche in adempimento di un'obbligazione contrattuale principale, esistente nei confronti di costui: sul punto, V. MATTERA, *La successione nell'account digitale*. *Il caso tedesco*, in *Nuova giur. civ. comm.,* 4, 2019., p. 700.

[213] BGH, 12 luglio 2018, n. 183/17; La Corte di Cassazione tedesca afferma che nel novero degli interessi legittimi rientrano, oltre quelli *ex lege*, anche gli interessi di fatto, economici o ideali, con esclusione tuttavia dei meri interessi generali.

[214] G. RESTA, *La successione nei rapporti digitali e la tutela post mortale dei dati personali*, cit., p. 99.

dei dati personali e al rispetto della vita privata e familiare propri dei *partner* di corrispondenza[215].
Tornando a considerare la normativa italiana, questa – l'art. 2-*terdecies* del d.lgs. n. 196/2003, come modificato dal d.lgs. n. 101/2018 – qualora risulti applicabile, si rivela l'espediente più efficace per ottenere beni digitali ereditari[216].
In considerazione del richiamo operato dalla norma interna sopra citata all'art. 15 GDPR, il soggetto legittimato ad entrare in possesso dell'eredità digitale della persona deceduta potrà ottenere l'accesso non solo ai dati anagrafici del defunto ma altresì a tutte le informazioni allo stesso riconducibili memorizzate dal titolare del trattamento[217].
Le problematiche che sono sorte nel tempo attorno alla possibilità di accedere ai beni digitali riconducibili al *de cuius* si collegano necessariamente a quelle relative al subentro nel rapporto contrattuale, di cui era parte il *de cuius,* sotteso alla fruizione degli *account*. In applicazione del principio di universalità della successione, così come ogni altro rapporto contrattuale, anche gli *account* dovrebbero essere oggetto di devoluzione e di acquisto *mortis causa*.
Così argomentando non dovrebbe impedirsi agli eredi - in qualità di successori nell'integrità dei rapporti attivi e passivi del *de cuius* e non già di legittimati *iure proprio* – di subentrare nel contratto atipico di *social network* e ottenere, così, l'accesso ai dati contenuti nel relativo *account*[218].

---

[215] V. MATTERA, *La successione nell'account digitale. Il caso tedesco*, cit., p. 706.
[216] Così A. D'ARMONIO MONFORTE, *La successione nel patrimonio digitale*, Pacini, 2020.
[217] È il caso di foto digitali, video, conversazioni, registrazioni, podcast, file di testo. Sul punto, F.M. RICCI*, I diritti dell'interessato*, in AA.VV. *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Zanichelli, 2017, p. 185. Sempre in virtù del richiamo alla normativa europea, viene assicurato al richiedente non solo tale diritto – ed il correlativo obbligo in capo al titolare – ma anche quello di copia gratuita, sempre che l'esercizio di tale diritto non arrechi una lesione a diritti o libertà di altre persone fisiche. Sul punto, D'ARMONIO MONFORTE A., *La successione nel patrimonio digitale*, cit.
[218] G. RESTA, *La successione nei rapporti digitali e la tutela post mortale dei dati personali*, cit., p. 91; C. CAMARDI, *L'eredità digitale. Tra reale e virtuale*, in *Dir. inf. e inform*., 2018, p. 79; G. MARINO, *La successione digitale*, in *Oss. dir. civ. e comm*., 2018, p. 180. Tuttavia, si è anche rilevato come spesso, nella contrattazione di massa a distanza, vengano pattuite clausole di intrasmissibilità del rapporto contrattuale che consentono ai fornitori dei servizi di trattenere i dati degli utenti defunti e dunque impedir e il subentro nel relativo *account* da parte degli eredi, clausole previste e ritenute dai fornitori del tutto legittime ora invocando la natura *intuitu personae* del rapporto tra fornitore e utente defunto, ora perché imposte dal rispetto del dovere di riservatezza e tutela della privacy dello stesso. Invero, clausole di tal specie di frequente devono classificarsi come abusive poiché avvantaggiano unilateralmente una delle parti a sfavore dell'altra. Ritiene la giurisprudenza tedesca che tali clausole, così come quelle relative all'autorità giurisdizionale competente o alla legge applicabile, debbano essere considerate nulle perché frutto di un'illegittima asimmetria contrattuale e perché non garantiscono una distribuzione equa dei diritti tra le parti. Ad ogni modo, clausole di tal natura, anche fossero idonee ad impedire la successione nell'*account* del soggetto defunto, non potrebbero comunque mai impedire la trasmissione di diritti già cristallizzati nel patrimonio del *de cuius* (quali, tra gli altri, il diritto di accesso ai dati personali), perché contrarie a norme e principi inderogabili sia in materia di tutela del consumatore sia in materia di successioni. Sul punto, G. MARINO, *La successione digitale*, cit., pp. 181-182.

2.2. Forme di tutela "aggregata"

La dottrina sottolinea la necessità di distinguere le azioni a tutela di interessi superindividuali, che sovente vengono impropriamente fatte tutte coincidere con l'istituto della *class action*. Si deve distinguere tra[219]: 1) class action, in virtù della quale uno o più individui, nell'interesse anche di una pluralità di altri soggetti danneggiati in un medesimo diritto dal comportamento di un terzo, possono iniziare un'azione legale per conto proprio e, nel contempo, chiedere che la causa sia condotta «on behalf» di tutti i membri; 2) group action, ossia il meccanismo processuale applicato in Inghilterra che consente al giudice di trattare unitariamente controversie che presentino le medesime questioni di fatto e di diritto, così da realizzare una concentrazione delle domande, rispondente a esigenze anche di economia processuale; 3) azioni collettive, ossia azioni promosse da associazioni rappresentative di consumatori o utenti (c.d. enti esponenziali), che agiscono quali "centri di imputazione".

In Italia, la prima forma di tutela aggregata è stata quella introdotta all'articolo 140-*bis* del Codice del consumo, nonché i giudizi inibitori, ricompresi agli artt. 139 e 140 dello stesso, promuovibili da parte delle associazioni di consumatori[220].

Più di recente, la l. 31/2019 ha abrogato tali disposizioni e introdotto, all'art. 840-*bis* ss. c.p.c., un'azione di classe non più limitata ai soli consumatori. Tale legge, inoltre, ha predisposto una nuova "*azione inibitoria collettiva*" (840-*sexiesdecies* c.p.c.), anch'essa di carattere comune, finalizzata ad ottenere l'ordine di cessazione o il divieto di reiterazione di atti e comportamenti posti in essere in pregiudizio di una pluralità di individui o enti.

Nell'ambito del Codice del consumo, all'art. 37, permane quale strumento di appannaggio esclusivo dei consumatori l'azione "*inibitoria collettiva*", esercitabile a fronte della violazione del divieto di utilizzare condizioni generali di contratto contenti clausole vessatorie ai sensi degli artt. 33 ss. Cod. consumo.

Una specifica forma di tutela aggregata per l'esercizio dei diritti contemplati dal Regolamento è prevista all'art. 80 GDPR, rubricato "*rappresentanza degli interessati*".

Sulla scorta di tale disposizione, l'interessato ha il diritto di dare mandato a "*un organismo, un'organizzazione o un'associazione senza scopo di lucro, che siano debitamente costituiti secondo il diritto di uno Stato membro, i cui obiettivi statutari siano di pubblico interesse e che siano attivi*

---

[219] G. SCARCHILLO, *Responsabilità e tutela dei diritti. Percorsi di diritto privato comparato*, Jovene, 2018, pp. 95 ss. Si v. anche L. SERAFINELLI, *Ancora sulla tutela del consumatore, anche in chiave collettiva*, in *Nuova giur. civ. comm.*, 2019, p. 612.

[220] Sull'azione di classe, si v. C. SCOGNAMIGLIO, *La Cassazione delinea presupposti e limiti di risarcibilità del danno non patrimoniale contrattuale nell'azione di classe*, in *Nuova giur. civ. comm.*, 2019, pp. 993 ss.; L. P. COMOGLIO, *L'azione di classe italiana: valutazioni ed efficienza*, in *Dir. pubbl. comp. eur.*, 2012, pp. 1114 ss.; C. CONSOLO-B. ZUFFI, *L'azione di classe ex art. 140-bis cod. cons. Lineamenti processuali*, Cedam, 2012; R. DONZELLI, *Art. 140 bis c. cons.*, in *Commentario breve al diritto dei consumatori*, a cura di G. DE CRISTOFARO-A. ZACCARIA, Cedam 2013, p. 1039; A. GIUSSANI, *L'azione di classe: aspetti processuali*, in *Riv. trim. dir. proc. civ.*, 2013, pp. 341 ss.;

nel settore della protezione dei diritti e delle libertà degli interessati con riguardo alla protezione dei dati personali", affinché il mandatario proponga reclamo per suo conto o eserciti per suo conto i diritti di cui agli art. 77, 78, 79, nonché il diritto di ottenere il risarcimento di cui all'art. 82 "*se previsto dal diritto degli Stati membri*".

La stessa norma sancisce, inoltre, al successivo par. 2, che gli Stati membri possono prevedere che un organismo, un'organizzazione o un'associazione (quelle di cui al par. 1), indipendentemente dal mandato conferito dall'interessato, abbia il diritto/potere di proporre, in tale Stato membro, un reclamo all'Autorità di controllo competente, e di esercitare i diritti di cui agli articoli 78 e 79, qualora ritenga che i diritti riconosciuti dal GDPR stesso ad un interessato siano stati violati in seguito al trattamento[221].

L'introduzione di queste forme aggregate di tutela rende certamente più efficiente la tutela privatistica presente nel Regolamento.

Come verrà analizzato *infra*, la violazione del diritto alla protezione dei dati determina la lesione di un diritto della personalità e la produzione di un danno di natura principalmente non patrimoniale. In relazione a questi ultimi, originano problematiche sia sul versante della loro quantificazione, sia su quello relativo alla prova della loro sussistenza. Si tratta, pur sempre, di riconoscere un equivalente monetario per un pregiudizio di tipo immateriale, "spirituale", con le ovvie criticità che questo comporta in termini di liquidazione.

A questa difficoltà di monetizzazione dei danni non patrimoniali conseguenti alla lesione di diritti della personalità, va ad aggiungersi l'evidente circostanza che, anche laddove la quantificazione e la prova del danno risultino semplici, si tratta, nella maggior parte dei casi, di importi risarcitori di scarsa rilevanza.

Tali elementi ingenerano certamente un forte senso di scoraggiamento al singolo utente, con il rischio che questi, con molta probabilità, deciderà di astenersi dal proporre un'azione per il risarcimento dei danni patiti.

Dal loro lato, gli operatori commerciali, consapevoli di tale condizione ricorrente, ben potrebbero realizzare in maniera sistematica violazioni della disciplina, confidando sullo scarso e limitato risarcimento che potrebbe essere, eventualmente, riconosciuto al singolo individuo.

Di fronte a tale scenario, un primo passo verso una maggiore effettività della tutela riconosciuta

---

[221] Nell'ambito del diritto dei dati, il noto caso Schrems v. FB Vol. II (Corte giust. UE, 16.7.2020, causa C-311/18), è riconducibile proprio ad un'azione di classe, in quanto il ricorrente Schrems agiva per sé stesso e quale rappresentante di altri soggetti. Come osservato, "*non essendovi in Austria alcuna disciplina specifica per l'azione di classe, la concentrazione delle domande è stata realizzata mediante la cessione del credito litigioso. Come rilevato anche da un recente report della Commissione Europea – di cui si parlerà nel prosieguo – la cessione del credito litigioso è lo schema tipico mediante il quale vengono instaurate le azioni collettive presso le giurisdizioni austriache, stante l'assenza di una specifica disciplina in tal senso*" (L. SERAFINELLI, *op. cit.*).

normativamente agli individui danneggiati può certo essere rinvenuto nell'introduzione di forme aggregate di tutela collettiva.

Se è vero che la previsione di tali mezzi costituisce un forte strumento di prevenzione e (potenzialmente) di repressione, è, tuttavia, necessario attendere gli esiti della loro utilizzazione, così da individuare gli inevitabili limiti applicativi che tale tutela aggregata incontra.

3. Il titolare del trattamento: dalla disciplina previgente al GDPR

La l. n. 675/1996, che aveva attuato la dir. 95/46/CE[222], tipizzava tre figure soggettive rilevanti nel trattamento dei dati: il titolare del trattamento (art. 1, comma 2°, lett. d) [223], il responsabile del trattamento (art. 1, comma 2°, lett. e) e l'incaricato (art. 19); tali figure sono state successivamente trasposte anche nel d.lgs. n. 196/2003[224].

È sin dalla Convenzione 108 del Consiglio d'Europa che l'individuazione del soggetto titolare del trattamento dei dati avviene nella persona fisica o giuridica, o nel soggetto pubblico, che si trova nella posizione di decidere le finalità e modalità del trattamento medesimo[225].

Il GDPR non ha modificato la definizione di "titolare del trattamento" che, tuttora, viene definito come "*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che,*

---

[222] Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24.10.1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

[223] Il "*data controller*", divenuto, nella normativa nazionale di attuazione, il "titolare del trattamento". Va evidenziato che il testo comunitario in lingua italiana della direttiva aveva tradotto "*data controller*" come "responsabile del trattamento", traduzione che portava il rischio di forte confusione nell'utilizzo dei termini. Tuttavia, il testo nazionale di recepimento della direttiva ha correttamente tradotto tale termine con "titolare del trattamento".

[224] S. RODOTÀ, *Tra diritti fondamentali ed elasticità della normativa: il nuovo codice della privacy*, in *Eur. e dir. priv.*, 2004, pp. 1 ss.

[225] Sulle figure soggettive del trattamento dei dati la letteratura è amplissima; si v. in particolare E. TOSI, *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale*, Giuffrè, 2020, pp. 61 ss.; A. D'OTTAVIO, *Ruoli e funzioni* privacy *principali ai sensi del regolamento*, in *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, a cura di R. PANETTA, Giuffrè, 2019, pp. 143 ss.; L. GRECO, *L'organigramma privacy: i soggetti del trattamento*, in *La protezione dei dati personali in Italia*, a cura di G. FINOCCHIARO, Zanichelli, 2019, pp. 321 ss.; V. RICCIUTO, *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, in *Dir. inf. e inform.*, 2018, pp. 689 ss.; G.M. RICCIO-G. SCORZA-E. BELISARIO, *GDPR e normativa privacy*, Cedam, 2018, pp. 596 ss.; L. BOLOGNINI-E. PELINO-C. BISTOLFI, *Il Regolamento Privacy Europeo. Commentario alla nuova disciplina sulla protezione dei dati personali,* Giuffrè, 2016; G. G. CASSANO-V: COLAROCCO-G.B. GALLUS-F.P. MICOZZI, *Il processo di adeguamento al GDPR aggiornato al D.Lgs. 10 agosto 2018, n. 101*, Giuffrè, 2018; E. LUCCHINI GUASTALLA, *Il nuovo Regolamento Europeo sul trattamento dei dati personali: i principi ispiratori*, in *Contratto e impresa*, 2018, pp. 106 ss.; V. CUFFARO, *Il diritto europeo sul trattamento dei dati personali*, in *Contratto e impresa*, 2018, pp. 1098 ss.; F. PIRAINO, *Il regolamento generale sulla protezione dei dati ed i diritti dell'interessato*, in *Nuove leggi civ. comm.*, 2017, pp. 369 ss.; A. MANTELERO, *Responsabilità e rischio nel Regolamento UE 2016/679*, in *Nuove leggi civ. comm.*, 2017, pp. 144 ss.; ID., *Gli autori del trattamento dati: titolare e responsabile*, in *Giur. it*., 2019, pp. 2777 M. G. STANZIONE, *Il regolamento europeo sulla privacy: origine e ambito di applicazione*, in *Eur. e dir. priv.*, 2016, pp. 1249 ss.; S. SICA-V. D'ANTONIO-G. M. RICCIO, *La nuova disciplina europea della privacy*, Cedam, 2016; F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati,* Giappichelli, 2016.

singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri" (art. 4, n. 7), GDPR).

La scelta di individuare quale responsabile del trattamento il soggetto che ne decide le finalità, assolve a due scopi, fondanti la disciplina dei dati personali[226]:

- trasparenza: sapere chi tratta i dati personali e ha il potere di conformare il trattamento permette agli interessati di conoscere l'identità del soggetto che è in grado di esercitare un potere su questo attributo della personalità;
- gestione del rischio: l'individuazione del titolare risulta funzionale ad un'allocazione della responsabilità[227]. Al potere di controllare finalità e modalità del trattamento corrispondono gli obblighi e le responsabilità in capo al soggetto che tale potere esercita. Tali obblighi, come vedremo *infra*, consistono, in particolare, nel rispetto dei principi in materia di trattamento (art. 5 GDPR), il cui inadempimento determina il sorgere della responsabilità civile sintetizzata nell'art. 82 GDPR: inoltre, il mancato adeguamento del titolare al GDPR può comportare responsabilità di tipo penale e amministrativo.

Il Garante per la protezione dei dati personali, nel Provvedimento del 9.12.1997[228], ha chiarito che il "titolare" del trattamento è da individuarsi, in caso di organizzazione collettiva, nell'ente medesimo e complessivamente considerato. Infatti, afferma il Garante che "*qualora il trattamento sia effettuato nell'ambito di una persona giuridica, di una pubblica amministrazione o di un altro organismo, il "titolare" è l'entità nel suo complesso (ad esempio, la società, il ministero, l'ente pubblico, l'associazione, ecc.), anziché taluna delle persone fisiche che operano nella relativa struttura e che concorrono, in concreto, ad esprimerne la volontà o che sono legittimati a manifestare all'esterno (ad esempio, l'amministratore delegato, il ministro, il direttore generale, il presidente, il legale rappresentante, ecc.). In molti casi, tali soggetti potrebbero assumere, semmai, la qualifica di "responsabile""*.

L'art. 24 GDPR (rubricato "responsabilità del titolare") prevede che il titolare del trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché

---

[226] M. RENNA, *Sicurezza e gestione del rischio nel trattamento dei dati personali*, in *Resp. civ. e prev.*, 2020, pp. 1343 ss. A. MANTELERO, *Gli autori del trattamento dati: titolare e responsabile*, in *Giur. it,* 2019; F. BRAVO, *Sulla figura del responsabile "interno" del trattamento dei dati personali*, in *Dir. inf. e inform.*, 2019, pp. 951 ss.; D. FARACE, *Le persone autorizzate al trattamento dei dati personali*, in *Riv. trim. dir. e proc. civ.*, 2021, pp. 423 ss.

[227] A. MANTELERO, *op. cit.*

[228] Provvedimento intitolato "*Titolare, responsabile, incaricato — Precisazioni sulla figura del "titolare""*, concernente la "*Circolare del Ministero delle Finanze n. 291/S del 13 novembre 1997 recante direttive in materia di protezione dei dati personali*".

dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al GDPR stesso. Il titolare è tenuto specificamente a riesaminare ed aggiornare tali misure, qualora necessario. È previsto, inoltre, l'obbligo di attuare "*politiche adeguate in materia di protezione dei dati*", se ciò è proporzionato rispetto alle attività di trattamento (art. 24.2 GDPR).

Va considerato che il GDPR 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. 1, lett. c), GDPR) e, infatti, il considerando n. 18 GDPR prevede che il regolamento "*non si applica al trattamento di dati personali effettuato da una persona fisica nell'ambito di attività a carattere esclusivamente personale o domestico e quindi senza una connessione con un'attività commerciale o professionale. Le attività a carattere personale o domestico potrebbero comprendere la corrispondenza e gli indirizzari, o l'uso dei social network e attività online intraprese nel quadro di tali attività. Tuttavia, il presente regolamento si applica ai titolari del trattamento o ai responsabili del trattamento che forniscono i mezzi per trattare dati personali nell'ambito di tali attività a carattere personale o domestico*".

Dunque, nella prospettiva del legislatore europeo il titolare è l'imprenditore, che effettua il trattamento di dati personali in connessione e per lo svolgimento della propria attività commerciale o professionale: il GDPR tutela la circolazione dei dati personali all'interno di questo perimetro di applicazione.

È questo il soggetto a cui il GDPR imputa la responsabilità civile nel caso dell'illecito trattamento dei dati personali.

Il GDPR prevede, tuttavia, che il titolare possa ricorrere ad un responsabile per l'esecuzione di un trattamento o di una parte del trattamento: tuttavia, in base al principio di responsabilizzazione del titolare, quest'ultimo deve ricorrere unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti dell'interessato (art. 28 GDPR). Dunque, laddove il danno per l'interessato sia stato determinato dalla condotta negligente di un responsabile esterno a cui è stata affidata una parte del trattamento, la responsabilità potrà essere ascritta anche al titolare per l'inadempimento dell'obbligo ex art. 28 GDPR di avvalersi di responsabili qualificati: una responsabilità che può essere qualificata, secondo le categorie tradizionali, come *culpa in eligendo.* A questa responsabilità si aggiunge quella per *culpa in vigilando*, in tutte quelle ipotesi in cui il titolare sia venuto meno ai propri doveri di controllo e monitoraggio effettivo sull'attività del responsabile.

Infatti, la prospettiva della "gestione del rischio", che pervade il GDPR (su questo aspetto, v. *infra* Cap. IV), impone al titolare di verificare costantemente i rischi che derivano dall'aver esternalizzato parti del trattamento, nonché di assumere le iniziative per mitigarli. Ciò significa, ad esempio, che il titolare dovrebbe garantirsi la possibilità, attraverso il contratto con il responsabile, di ricevere un flusso di informazioni costante sulle modalità con cui quest'ultimo effettua il trattamento affidatogli; in determinate ipotesi, il titolare dovrebbe garantirsi, inoltre, la possibilità di svolgere specifici *audit* sull'attività del responsabile, per verificare se questi ha effettivamente messo in atto adeguate misure di sicurezza per il trattamento di dati personali.

È interessante evidenziare che le recenti Linee Guida del Gruppo di Lavoro Articolo 29 precisano che i concetti di titolare e responsabile sono concetti "funzionali", nel senso che mirano ad allocare le responsabilità secondo i ruoli effettivi delle parti. Ciò implica che lo status giuridico come "titolare" o "responsabile del trattamento" deve, in linea di principio, essere determinato dalle sue "attività effettive" in uno specifico contesto, piuttosto che sulla designazione formale utilizzata dalle parti contrattuali: ciò significa che la suddivisione dei ruoli deve derivare da un'analisi degli elementi di fatto o delle circostanze del caso e come tale non è negoziabile dalle parti[229].

4. Il responsabile del trattamento

Mentre la definizione di "titolare del trattamento" è rimasta invariata rispetto al passato, il GDPR introduce una nuova definizione di "responsabile" del trattamento dei dati personali.

Ora il responsabile non è più individuato nel soggetto "*preposto*" dal titolare al trattamento di dati personali[230], come prevedeva l'art. 4, co. 1, lett. g) Codice privacy; il responsabile è colui il quale, persona fisica o giuridica, autorità pubblica, servizio o altro organismo, "tratta dati personali *per conto* del titolare del trattamento" (art. 4, n. 8), GDPR).

Inoltre, il GDPR incrementa notevolmente gli adempimenti, e la conseguente sfera di responsabilità, a carico del responsabile del trattamento, con l'intento di aumentare gli *standard* di protezione in tema di *data protection* e di assicurare una più efficace *compliance* normativa[231].

Come precisato al paragrafo precedente, il titolare può affidare al responsabile l'esecuzione di uno o più trattamenti, attraverso un contratto che deve disciplinare modalità, durata, natura e finalità del

---

[229] EDPB, *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*, 7.7.2021.

[230] Com'è noto, la disciplina nazionale anteriore al GDPR prevedeva la duplice figura del "responsabile interno" e "responsabile esterno": sugli effetti di tale distinzione al fine della responsabilità civile da illecito trattamento, si tornerà *infra*.

[231] B. VAN ALSENOY, *Data Protection Law in the UE: Roles, Responsibilities and Liability*, Cambridge, 2019, p. 47; per ulteriori considerazioni sul saggio di Van Alsenoy, si v. D. KAMARINOU, *Brendan Van Alsenoy, Data Protection Law in the EU: Roles, Responsibilities and Liability* in *International Data Privacy Law,* Vol. 10, No. 4, 2020*,* pp. 395-398.

trattamento, tipo di dati personali, categorie di interessati, obblighi e diritti del titolare e del responsabile.

L'art. 28, par. 3, GDPR stabilisce il contenuto minimo essenziale di tale contratto, il quale deve prevedere che il responsabile:

a) tratti i dati personali soltanto su istruzione documentata del titolare del trattamento;

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 di sicurezza richieste dall'art. 32 GDPR;

d) rispetti le condizioni previste dal GDPR per la nomina di eventuali sub-responsabili (su cui v. *infra*);

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

f) assista il titolare del trattamento nel garantire il rispetto degli obblighi di sicurezza e di notifica delle violazioni di *data breach*, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;

g) su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti;

h) metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi del GDPR e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzate dal titolare del trattamento o da un altro soggetto da questi incaricato.

Sul responsabile grava, inoltre, l'obbligo di informare immediatamente il titolare del trattamento qualora, a suo parere, un'istruzione violi il regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati: viene così ulteriormente responsabilizzato anche il responsabile del trattamento, che non potrà andare esente da responsabilità deducendo di essersi attenuto meramente alle istruzioni del titolare. Egli dovrà dimostrare, semmai, di aver manifestato il proprio dissenso e di essere stato indotto ad eseguire tali istruzioni, quale *nudus minister*, per le insistenze del titolare.

Il GDPR disciplina l'ipotesi in cui il responsabile voglia ricorrere, per l'esecuzione di un trattamento affidatogli dal titolare, ad un ulteriore responsabile, ossia il "*sub-responsabile*". Tale nomina sarà legittima solo con la preventiva autorizzazione scritta, specifica o generale, da parte del titolare del trattamento. Qualora l'autorizzazione sia generale, il responsabile del trattamento deve informare il titolare del trattamento di eventuali modifiche riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche. Questo perché il titolare, per il principio di *accountability*, rimane sempre obbligato nei

confronti del danneggiato anche per l'inadempimento posto in essere dal responsabile e dal sub-responsabile: il titolare deve sempre garantire che il sub-responsabile sia soggetto qualificato e adeguato a eseguire la parte di trattamento che gli viene affidata.

Viene, inoltre, prevista l'obbligatoria "contrattualizzazione formale" anche del rapporto tra responsabile e sub-responsabile. Infatti, quando un responsabile del trattamento ricorre ad altro responsabile per l'esecuzione di specifiche attività di trattamento su tale soggetto ricadono, mediante un contratto, gli stessi obblighi in materia di protezione dei dati contenuti nel contratto tra il titolare del trattamento e il responsabile del trattamento. Allo stesso modo è previsto che anche il contratto tra responsabile e sub-responsabile debba prevedere garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR.

Come detto, dal punto di vista della responsabilità per illecito trattamento dei dati personali, il GDPR prevede che, in ogni caso, nei confronti del titolare del trattamento il responsabile iniziale resti obbligato per l'intero, qualora il sub-responsabile abbia omesso di adempiere agli obblighi del GDPR.

Inoltre, l'ultimo paragrafo dell'art. 28 GDPR prevede l'ipotesi in cui il responsabile non si sia attenuto al contratto e alle istruzioni fornite dal titolare e abbia, così, determinato le finalità e i mezzi del trattamento. In questo caso, il responsabile viene considerato titolare del trattamento in questione ed assume tutti gli obblighi connessi a tale qualifica. Il Regolamento supera, infatti, il dato formale della designazione a responsabile qualora, in sostanza, questi abbia assunto, anche contrariamente a quanto previsto contrattualmente, il potere di controllo sul dato che spetterebbe al titolare del trattamento.

Il responsabile diviene a tutti gli effetti "titolare del trattamento", assumendo i medesimi doveri di *accountability* e, conseguentemente, egli incorre nella medesima responsabilità del titolare ex art. 82 nei confronti del danneggiato.

5. La contitolarità nel trattamento ex art. 26 GDPR

La possibilità che il titolare del trattamento operi "*da solo o insieme ad altri*" non figurava nella Convenzione 108; nel procedimento di adozione della Direttiva 46/95, il Parlamento ha previsto tale ipotesi, introducendo un emendamento specifico al testo della Direttiva.

Nel parere sugli emendamenti del Parlamento Europeo, la Commissione afferma che "*per uno stesso trattamento, possono esservi più corresponsabili che determinano assieme la finalità del trattamento e gli strumenti da utilizzare per effettuarlo",* e di conseguenza che, in tal caso, *"ciascuno dei corresponsabili deve considerarsi tenuto al rispetto delle obbligazioni poste dalla presente direttiva al fine di proteggere le persone fisiche i dati delle quali sono trattati*"[232].

[232] GRUPPO DI LAVORO ARTICOLO 29, *op. cit.*

La Direttiva 46/95/CE prevedeva, dunque, che il titolare del trattamento potesse determinare modalità e finalità del trattamento "*da solo o insieme ad altri*" (art. 2, lett. d); tuttavia, a parte questo richiamo formale, il fenomeno della contitolarità non era disciplinato specificamente dalla Direttiva.

La contitolarità viene ora espressamente disciplinata dall'art. 28 GDPR, secondo cui è la determinazione "*congiunta*" delle finalità e delle modalità del trattamento che determina l'applicazione della disciplina in tema di contitolarità; tuttavia, il concetto di contitolarità è più ampio di quello considerato dalla Direttiva.

Infatti, nel parere 1/2020, il Gruppo di Lavoro Articolo 29 osserva che "*il parere della Commissione non rispecchia del tutto la complessità della realtà attuale in materia di protezione dei dati, poiché riguarda solo il caso in cui tutti i responsabili del trattamento determinano in uguale misura uno stesso trattamento e in uguale misura ne rispondono. La realtà mostra invece che questo è solo uno dei vari tipi di "responsabilità plurima" che possono esistere. In tale ottica, l'espressione "insieme a" deve essere interpretata come se significasse "non da solo", in varie forme e combinazioni*".

Da ciò si ricava che, nell'interpretazione del Gruppo di Lavoro Articolo 29, il fenomeno della contitolarità può riguardare anche quei casi in cui uno dei titolari coinvolti decida solo in minima parte sulle finalità del trattamento. Sul tema della contitolarità anche la giurisprudenza europea ha assunto una posizione particolarmente estensiva del concetto di "titolare".

Con la sentenza 5.6.2018, n. 210[233], la Corte di Giustizia UE ha affermato che dev'essere considerato contitolare del trattamento l'amministratore di una *fanpage* messa a disposizione da Facebook. In particolare, nel caso di specie, Facebook aveva installato un *cookie* sul dispositivo di ciascun utente, che poteva essere impostato secondo parametri diversi per individuare e selezionare specifici dati personali (es. età anagrafica, luogo, sesso) degli utenti che accedevano alla *fanpage*; questi dati venivano elaborati per fornire statistiche al gestore della *fanpage* stessa, il quale, per l'appunto, riceveva dati "anonimi" degli utenti, perché in forma meramente statistica, restando i dati personali da cui le statistiche erano ricavate nella sola disponibilità di Facebook.

La Corte di Giustizia afferma che "*la creazione di una fanpage su Facebook implica da parte del suo amministratore un'azione d'impostazione dei parametri in base, segnatamente, al suo pubblico destinatario nonché agli obiettivi di gestione o di promozione delle sue attività, che influisce sul trattamento di dati personali ai fini della creazione di statistiche stabilite a partire dalle visite della fanpage. Tale amministratore può, tramite filtri messi a disposizione da Facebook, definire i criteri a partire dai quali si devono stabilire tali statistiche e designare perfino le categorie di persone i cui dati personali saranno oggetto di utilizzo da parte di Facebook*".

---

[233] CORTE GIUST. UE, 5.6.2018, causa C-210/16, in *Nuova giur. civ. comm.,*, 2018, pp. 1805 ss., con nota di G.M. RICCIO, *Titolarità e contitolarità nel trattamento dei dati personali tra Corte di Giustizia e Regolamento privacy*.

Da ciò si ricava, secondo la Corte, che l'amministratore della *fanpage* è contitolare perché "*contribuisce al trattamento dei dati personali dei visitatori della sua pagina*" (par. 36 sentenza), poiché "*in ogni caso, la direttiva 95/46 non impone che, qualora vi sia una responsabilità congiunta di più operatori per un medesimo trattamento, ciascuno abbia accesso ai dati personali interessati*" (par. 38 sentenza). Dunque, anche la gestione di "dati anonimi" può comportare l'assunzione della qualifica di "titolare del trattamento" e l'applicazione della disciplina sulla protezione dei dati personali.

Nel caso di specie, il titolare ha solo impostato i parametri di base per il trattamento e ha trattato dati esclusivamente in forma anonima; il trattamento dei dati personali veri e propri è stato eseguito esclusivamente dal responsabile (sulla base dei parametri pre-impostati).

Si evidenzia, dunque, che la qualifica di titolare, cui consegue l'applicazione della relativa disciplina (si ricorda, ancora una volta, la necessità di adempiere all'obbligo di *accountability*), viene assunta sulla base del potere di "controllo" sul trattamento e non sull'esecuzione materiale dello stesso.

I contitolari sono obbligati, ex art. 26, a stipulare un accordo interno che disciplini le rispettive responsabilità in ordine all'adempimento degli obblighi derivanti dal Regolamento, con particolare riferimento all'esercizio dei diritti degli interessati; tale accordo deve disciplinare le "*funzioni di comunicazione delle informazioni di cui agli artt. 13 e 14*", ossia deve indicare le modalità di rilascio delle informative, che dovranno dare atto, in modo chiaro e trasparente, della contitolarità stessa.

L'accordo, che viene obbligatoriamente messo a disposizione dell'interessato, deve riflettere "*adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati*" (art. 26, par. 2). È evidente che, per tornare al caso sopra esposto del *social network* Facebook, in queste fattispecie la contitolarità si sviluppa attraverso contratti per adesione predisposti dal *social network* medesimo, a cui i gestori delle pagine non posso che aderire in via formale.

La disposizione di chiusura dell'art. 26 (par. 3), prevede quanto segue: "*l'interessato può esercitare i propri diritti ai sensi del presente regolamento nei confronti di e contro ciascun titolare del trattamento*"[234]. Ciascun titolare è perciò solidalmente responsabile, nei confronti dell'interessato, per i danni cagionati dal trattamento illecito *complessivamente* considerato, anche se, in base all'accordo stesso, l'illecito che cagiona il danno si riferisce all'esecuzione di una parte del

[234] G. M. RICCIO, *op. cit.*, critica la posizione assunta dalla Corte di Giustizia UE sul fenomeno della contitolarità per diverse ragioni. Una di queste è proprio l'impossibilità in cui versa talvolta uno dei contitolari – nell'espressione estensiva accolta dalla giurisprudenza europea – di dar seguito efficacemente alle richieste degli interessati di esercizio dei diritti. Ad esempio, laddove l'utente Facebook chiedesse al gestore della pagina di cancellare tutti i propri dati personali, l'amministratore della *fanpage* non potrebbe far altro che inoltrare la richiesta al *social network* e confidare sull'adempimento da parte di questi: tuttavia, nel caso di danni verificatisi per il ritardo o il mancato adempimento da parte di Facebook, l'amministratore della *fanpage* resterebbe, comunque, solidalmente obbligato nei confronti dell'interessato per il risarcimento.

trattamento che avviene sotto il controllo di un diverso titolare.

6. Il responsabile "interno": inammissibilità della figura

Nella normativa nazionale previgente al GDPR era prevista, accanto alla figura del titolare e del responsabile *esterno*, anche la figura del responsabile *interno*.

La creazione di questa "figura privacy", aggiuntiva rispetto ai ruoli descritti dalla normativa europea, aveva fatto sorgere un dibattito nella dottrina italiana in merito alla conformità della stessa legislazione nazionale rispetto alla Direttiva europea.

È opportuno soffermarsi brevemente su tale figura per verificare se essa sia compatibile con il GDPR e, in caso positivo, per valutarne gli effetti sulla responsabilità per illecito trattamento dei dati personali.

La normativa comunitaria anteriore al GDPR prevedeva la figura del "*data processor*"[235] definita come "la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che elabora dati personali per conto del responsabile del trattamento"[236]. Il *data processor* era dunque deputato alla "elaborazione" dei dati personali, ossia al compimento di operazioni di trattamento per conto del titolare.

Nella figura "europea" del *data processor* confluivano, in realtà, due distinte figure previste dal legislatore italiano, il "responsabile" (esterno all'organizzazione del titolare) e l'"incaricato" (interno all'organizzazione del titolare).

Infatti, l'art. 4, comma 1°, lett. *g)*, d.lgs. n. 196/2003, definiva il responsabile come "la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo *preposti* dal titolare al trattamento di dati personali".

Il responsabile (*data processor*) non era colui che compiva operazioni *per conto* del titolare, come previsto dalla formulazione letterale della Direttiva, ma era il soggetto "*preposto*" dal titolare al trattamento dei dati, ovvero il soggetto *esterno* o *interno* all'organizzazione del titolare, che gestiva il trattamento o una porzione di esso su *preposizione* del titolare, che lo aveva a ciò designato.

E infatti, il legislatore italiano, in sede di recepimento della direttiva, aveva tipizzato espressamente l'ulteriore figura dell'"incaricato del trattamento", non prevista dalla disciplina europea (che solo in alcuni passaggi faceva riferimento ai soggetti che trattano dati perché *autorizzati* dal titolare).

Gli incaricati erano indicati, all'art. 4, comma 1°, lett. *h*), d.lgs. n. 196/2003, come "*le persone fisiche*

---

[235] Il testo comunitario in lingua italiana della direttiva traduceva tale formulazione con "incaricato del trattamento": il testo nazionale di recepimento aveva invece correttamente trasposto la figura con l'espressione di "responsabile del trattamento".

[236] L'indicazione deve essere tradotta, in realtà, con l'espressione "per conto del *titolare* del trattamento", secondo le espressioni utilizzate dalla normativa nazionale di recepimento.

autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile": la definizione portava, dunque, ad una parziale sovrapposizione con la definizione europea di *data processor*, individuato in colui che "compie operazioni di trattamento". Si era così giunti a considerare "responsabili" del trattamento sia i soggetti che operavano all'interno dell'organizzazione del titolare del trattamento, che venivano definiti responsabili "*interni*", sia i soggetti che operavano all'esterno dell'organizzazione del titolare, definiti responsabili "*esterni*".

Nella prassi, le aziende italiane erano solite designare formalmente quali "responsabili interni" quelle figure apicali, di livello dirigenziale, che sovrintendevano una determinata area aziendale, al cui interno si eseguivano processi di trattamento dei dati, o parti di essi. È facile intuire, tuttavia, che tale designazione si scontrava nella frequente carenza di conoscenza, in capo a tali soggetti, della normativa privacy, nonché delle misure organizzative e di sicurezza che gli stessi erano chiamati ad attuare nell'ambito delle rispettive aree di competenza.

L'ammissibilità di tale figura non può ritenersi più compatibile con il GDPR[237]: la struttura del rapporto tra titolare e responsabile, come delineata dall'art. 28, richiede necessariamente la terzietà del soggetto-responsabile, che deve essere un soggetto giuridico esterno e terzo rispetto al titolare[238].

Il titolare potrebbe, comunque, al fine di rendere più efficiente la gestione del trattamento dei dati, delegare specifici compiti di controllo e supervisione ai soggetti dirigenziali delle diverse aree di competenza. Si tratta di una scelta che avviene nella prassi, proprio al fine di attuare il principio di responsabilizzazione, che impone al titolare di organizzare la propria struttura interna, anche in termini di controllo e supervisione dei processi, per garantire la sicurezza dei dati. Tuttavia, laddove si verificasse un trattamento illecito, perché il *preposto* non ha adempiuto ai propri compiti, il titolare resterebbe l'unico responsabile *ex* art. 82 nei confronti del danneggiato. Secondo le categorie della dottrina tradizionale, si può affermare che il titolare è responsabile nei confronti del danneggiato a titolo di *culpa in eligendo* o di *culpa in vigilando*: nel primo caso se avesse nominato un soggetto privo di caratteristiche adeguate, nel secondo se avesse omesso di controllare l'adempimento del preposto alle istruzioni ricevute.

Ma il titolare andrebbe anche incontro ad una responsabilità per colpa più pregnante e diretta, in quanto si tratterebbe di inadempimento diretto all'obbligo di approntare una struttura organizzativa adeguata al trattamento di dati personali: è, dunque, un obbligo di *accountability* che supera la

---

[237] Va evidenziato che la Relazione illustrativa del d.l. 18/1018 prevede espressamente la possibilità di "*mantenere le funzioni e i compiti assegnati a figure* interne *all'organizzazione che, ai sensi del previgente codice in materia di protezione dei dai personali* ma in contrasto con il regolamento*, potevano essere definiti, a seconda dei casi, responsabili o incaricati* ".

[238] Tale soluzione è in linea anche con l'interpretazione fornita dal Gruppo di Lavoro Articolo 29, che nel parere n.1/2010 ha posto l'accento sul carattere di "terzietà" del responsabile rispetto al titolare.

responsabilità per *culpa in eligendo* o *in vigilando* e che costituisce un autonomo titolo di responsabilità.

7. Il DPO ex art. 37 GDPR

Il GDPR introduce, all'art. 37, la nuova figura soggettiva del responsabile della protezione dei dati, che deve essere nominato dal titolare e dal responsabile ogniqualvolta:

> 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;
>
> 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.

I gruppi imprenditoriali possono nominare un unico responsabile della protezione dei dati, a condizione che il responsabile sia facilmente raggiungibile da ciascuno stabilimento[239].

Si tratta di un soggetto che: i) dev'essere dotato di competenze specialistiche in ambito privacy; ii) dev'essere dotato di autonomia decisionale nell'ambito dell'organizzazione del titolare, anche con autonomia di risorse; iii) deve esercitare le proprie funzioni in modo indipendente e in assenza di conflitti di interesse con l'organizzazione in cui è inserito; iv) deve fungere da punto di contatto tra il titolare, dall'un lato, e gli interessati o l'Autorità di controllo, dall'altro lato.

Nell'analisi della figura del responsabile, gli aspetti più rilevanti per le conseguenze sul tema della responsabilità civile per illecito trattamento dei dati, riguardano i compiti del responsabile e la posizione che lo stesso deve avere rispetto all'organizzazione dell'azienda o ente che lo hanno designato.

Con riferimento ai compiti, il GDPR prescrive che il responsabile dev'essere incaricato *almeno* delle seguenti funzioni (art. 39):

> a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento[240], nonché ai dipendenti che eseguono il trattamento, in merito agli obblighi

[239] Qualora il titolare del trattamento o il responsabile del trattamento sia un'autorità pubblica o un organismo pubblico, un unico responsabile della protezione dei dati può essere designato per più autorità pubbliche o organismi pubblici, tenuto conto della loro struttura organizzativa e dimensione (art. 37, par. 3).

[240] L'art. 38 prevede che titolare del trattamento e il responsabile del trattamento devono assicurarsi che il responsabile della protezione dei dati sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.

derivanti dal GDPR stesso (nonché da altre disposizioni dell'UE o degli Stati membri relative alla protezione dei dati);

b) sorvegliare sull'osservanza del GDPR (nonché di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati), nonché sulle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;

c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35[241];

d) cooperare con l'autorità di controllo;

e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento (tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione) [242].

Inoltre, la disposizione di chiusura dell'art. 39 (par. 2) impone, in linea generale e di principio che, nell'eseguire i propri compiti, il responsabile della protezione dei dati debba considerare debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

Con riferimento alle *competenze* e alla *posizione* del Responsabile della protezione, il GDPR prescrive, innanzitutto, che egli è designato "*in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39*" (art. 37, par. 5); inoltre il titolare e il responsabile devono fornire al DPO le "risorse necessarie" affinché egli mantenga la propria conoscenza specialistica: ad esempio, nel caso in cui venga nominato un dipendente, dovrà essere previsto un apposito budget aziendale per permettere al DPO di seguire corsi di formazione per aggiornare le proprie competenze.

Dunque, il responsabile della protezione dei dati può essere un dipendente del titolare del trattamento o del responsabile del trattamento; tale funzione può, alternativamente, essere esternalizzata, tramite

---

[241] L'art. 35 GDPR (rubricato "*valutazione d'impatto sulla protezione dei dati*") prevede che quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali.

[242] Il titolare del trattamento o il responsabile del trattamento deve pubblicare i dati di contatto del responsabile della protezione dei dati e comunicarli all'autorità di controllo; l'art. 38, par. 4, prevede infatti che "*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*".

un accordo scritto.

In ogni caso, deve essere assicurata l'indipendenza, la terzietà e l'assenza di conflitto di interessi tra il DPO e il titolare o responsabile.

L'art. 38 prevede, infatti, che il titolare e il responsabile del trattamento "*sostengono il responsabile della protezione dei dati nell'esecuzione dei compiti di cui all'articolo 39 fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti*". Ciò significa che, come avviene per le altre funzioni di controllo interno (*compliance*, *internal audit*, *risk management*), l'ente o l'azienda devono prevedere specifici *budget* per l'adeguamento e i controlli interni in ambito *privacy*; *budget* il cui utilizzo dev'essere rimesso alla discrezionalità del DPO stesso.

Il profilo dell'indipendenza del DPO risulta evidente all'art. 38, il quale impone che il titolare del trattamento e il responsabile del trattamento debbano assicurarsi che il responsabile della protezione dei dati "*non riceva alcuna istruzione*" per l'esecuzione dei compiti affidatigli dalla legge o dal contratto, nel caso in cui la funzione sia esternalizzata. Inoltre, il responsabile della protezione dei dati non può essere "*rimosso o penalizzato*" dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti.

Si tratta, dunque, di una figura di controllo e supervisione che deve caratterizzarsi per la piena indipendenza. Egli deve riferire sui compiti e responsabilità che gli sono affidati, direttamente al "*vertice gerarchico*" del titolare del trattamento o del responsabile del trattamento.

Pertanto, se dall'un lato è previsto che il responsabile della protezione dei dati possa svolgere altri compiti e funzioni (art. 38, par. 6), dall'altro è previsto che il titolare o il responsabile debbano assicurarsi che tali compiti e funzioni non diano adito a conflitto di interessi.

Come vedremo *infra*, il responsabile svolge un ruolo di supporto fondamentale per il titolare, nell'adempimento all'obbligo di *accountability* e nella gestione del rischio privacy. Sin dalle fasi di individuazione dei trattamenti che possono comportare rischi per i diritti e le libertà degli interessati, il titolare può fare affidamento sulla competenza specialistica del DPO, il quale dovrà essere opportunamente coinvolto, a tutti i livelli dell'organizzazione dell'impresa, per la corretta gestione dei trattamenti di dati. Egli monitora che gli addetti interni all'organizzazione siano adeguatamente formati sulle misure di sicurezza da adottare nel trattamento dei dati e che adempiano alle proprie mansioni rispettando le prescrizioni della disciplina di protezione dei dati. Inoltre, il responsabile per la protezione monitora costantemente il rispetto delle misure di sicurezza adottate, che deve rivalutare costantemente, e svolge un ruolo di supporto e consulenza fondamentale nella valutazione d'impatto e nel rispetto dei principi di *privacy by design* e *by default* (su cui v. infra). È essenziale, infatti, che in tutte le fasi di progettazione dell'attività interna e dei nuovi prodotti, gli incaricati interni consultino e collaborino costantemente con il DPO, che potrà consigliare così, per ciascuna fase di creazione e

sviluppo dei nuovi prodotti/servizi, le misure più opportune per garantire il rispetto dei principi del GDPR. La nomina del responsabile per la protezione dei dati è dunque uno dei presidi fondamentali per la gestione dei rischi inerenti le attività di trattamento e, dunque, costituisce un presidio fondamentale per il titolare per dimostrare la propria responsabilizzazione.

Il responsabile per la protezione dei dati non compare tra i soggetti che, a norma dell'art. 82 GDPR, sono tenuti al risarcimento dei danni per il caso di trattamento illecito, con la conseguenza che l'eventuale soggetto danneggiato potrebbe rivalersi nei suoi confronti solo attraverso il regime ordinario di cui all'art. 2043 c.c.: si tratta di un'ipotesi assai remota, poiché nella pratica sarà molto più conveniente per il danneggiato agire nei confronti del titolare che, molto probabilmente, sarà un soggetto più solvibile. In ogni caso, laddove agisse anche nei confronti del responsabile per la protezione, il danneggiato non potrebbe godere del regime probatorio più vantaggioso previsto dall'art. 82 GDPR.

8. Presupposti e modalità del trattamento dei dati: premessa

Analizzate le figure soggettive coinvolte nel trattamento dei dati, è opportuno soffermarsi sull'analisi dei principi di legittimità del trattamento, in quanto la responsabilità ex art. 82 GDPR sorge evidentemente solo in presenza di trattamento "illecito": se da quest'ultimo deriva, secondo un nesso di causalità, un danno per l'interessato cui si riferiscono i dati, sorge il regime di responsabilità speciale previsto dal GDPR. Sul rapporto tra l'art. 82 GDPR e l'art. 2043 c.c. ci si soffermerà nel prossimo capitolo; tuttavia, è opportuno evidenziare sin d'ora che l'inapplicabilità dell'art. 82, in una fattispecie concreta, non vale ad escludere l'eventuale responsabilità civile, ai sensi dell'art. 2043 c.c., per i danni causati da illecito utilizzo di dati personali.

Il Reg. UE 2016/679 ripropone all'art. 6, con formulazione quasi invariata, i principi di "liceità del trattamento" che erano contenuti all'art. 7 Dir. 95/46/CE.

Nello specifico, prevede l'art. 6 GDPR che il trattamento è lecito solo se, e nella misura in cui, ricorre almeno una delle seguenti condizioni: a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità; b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso; c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento; d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica; e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento; f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà

fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

È, dunque, necessario, prima di tutto, che sussista una delle sopra elencate condizioni affinché il trattamento possa essere effettuato: si tratta di *presupposti* imprescindibili[243] che devono sussistere *ex ante*, ma che nulla dicono sulle *modalità* con cui tale trattamento dovrà essere svolto.

È l'art. 5 GDPR, rubricato "*principi applicabili al trattamento*", che indica, invece, le caratteristiche che rendono lecite le *modalità* del trattamento. Infatti, la lett. a), par. 1, di tale disposizione, prevede che i dati personali debbano essere "*trattati in modo lecito, corretto e trasparente nei confronti dell'interessato*", così affermando i tre principi della liceità, della correttezza e della trasparenza del trattamento dei dati personali.

Questi principi, che formano la base del trattamento eseguito "con modalità legittime", erano già espressi dal precedente Codice sul trattamento dei dati personali: infatti, tutti i principi sul trattamento previsti dal d.lgs. n. 196/2003 sono confluiti nel nuovo Reg. UE 2016/679, il quale, come vedremo, ha previsto ulteriori principi per la tutela del trattamento dei dati.

Si tratta, in particolare, dei seguenti principi:

- principio di limitazione delle finalità (art. 5, par. 1, lett. b), secondo cui i dati personali sono raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in un modo che non sia incompatibile con tali finalità[244];
- principio di minimizzazione dei dati (art. 5, par. 1, lett. c), secondo cui i dati personali devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
- principio di esattezza (art. 5, par. 1, lett. d), secondo cui i dati devono essere esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;
- principio di limitazione della conservazione (art. 5, par. 1, lett. e), secondo cui i dati personali devono 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[245];

---

[243] Si v. D. POLETTI, *Le condizioni di liceità del trattamento dei dati personali*, in *Giur. it.*, 2019, pp. 2777 ss., che qualifica i principi di cui all'art. 6 GDPR come "condizioni" di legittimità del trattamento, così sottolineando il fatto che esse si collocano in una fase *ex ante* del trattamento.

[244] La norma precisa che un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali.

[245] La disposizione aggiunge che i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici,

- principio di sicurezza del trattamento (art. 5, par. 1, lett. f) e art. 32), secondo cui i dati personali devono essere trattati in maniera da garantire un'adeguata sicurezza, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali;
- principio della *privacy by design* (art. 25, par. 1) e *by default* (art. 25, par.), secondo cui il titolare deve mettere in atto le misure tecniche e organizzative adeguate "sia al *momento* di determinare i mezzi del trattamento sia all'*atto* del trattamento"[246] e queste misure devono garantire che siano trattati "per impostazione predefinita" solo i dati personali necessari per ogni specifica finalità del trattamento;
- principio dell'informativa del trattamento (artt. 13 e 14), il quale attua la stessa "trasparenza" del trattamento. Il principio di informativa impone al titolare di fornire all'interessato un'informazione chiara, precisa e trasparente sulle condizioni e sulla modalità effettive del trattamento, nonché degli eventuali soggetti coinvolti che lo pongono in essere o che, comunque, possono venire a conoscenza dei dati dell'interessato.

A questi principi (che, come detto, erano già espressi nel precedente Codice privacy), il nuovo Regolamento aggiunge:

- principio del divieto di decisioni basate su trattamenti esclusivamente automatizzati (art. 22), secondo cui l'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona;
- principio di oblio dei dati, che impone al titolare, nelle ipotesi determinate dall'art. 17 GDPR, di cancellare senza ingiustificato ritardo i dati personali.

Questa "architettura" si regge ed è conformata dal nuovo principio di *accountability*, attorno al quale ruota il sistema di tutela dei dati personali del Regolamento.

L'analisi delle condizioni di liceità del trattamento dei dati personali[247] è, dunque, essenziale per

---

conformemente all'articolo 89, par. 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato

[246] Più nello specifico, l'art. 25, par. 1, prevede che la *privacy by design* e *by default* vadano attuata "tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento".

[247] Sui principi del trattamento la dottrina è molto ampia. Si. v. G. FINOCCHIARO, *Il principio di* accountability*,* in *Giur. it.*, 2019, pp. 2777; D. POLETTI, *Le condizioni di liceità del trattamento dei dati personali*, in *Giur. it.*, 2019, pp. 2777; G. ALPA, *L'identità digitale e la tutela della persona. Spunti di riflessione*, op. cit., pp. 723; L. LIONELLO, *La creazione del mercato europeo dei dati: sfide e prospettive*, in *Dir. comm. int.*, 2021, pp. 65; L. TORMEN, *La linea dura della Cassazione in materia di responsabilità dell'*Hosting Provider *(attivo e passivo)*, in *Nuova giur. civ. comm.*, 2019, pp. 1039, nota a

determinare quando si verifica un'ipotesi di responsabilità ex art. 82 GDPR, che obbliga al risarcimento del danno "…*causato da una violazione del presente Regolamento*".

Come già precisato, l'art. 6 GDPR sulle condizioni di liceità del trattamento sembra riproporre interamente il contenuto dell'art. 7 della Dir. 95/46/CE, che apriva la sezione dedicata ai principi relativi alla legittimazione del trattamento. Tuttavia, anche laddove i principi del trattamento vengono descritti con analoghe formulazioni lessicali, essi vanno interpretato nella diversa prospettiva del Regolamento, che sposta l'attenzione dai diritti dell'interessato agli obblighi del titolare, in particolare l'obbligo di responsabilizzazione.

L'analisi dei presupposti del trattamento ex art. 6 GDPR deve essere svolta congiuntamente all'analisi dei principi del trattamento ex art. 5 GDPR: è evidente, infatti, che anche la legittimità della "base giuridica" del trattamento ex art. 6 deve essere valutata alla luce dei principi di cui all'art. 5.

9. Il principio di liceità

Il principio di liceità del trattamento si fonda, ancor prima del Regolamento, sulla Carta dei diritti UE, che all'art. 52, par. 1, afferma che "*eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla presente Carta devono essere previste dalla legge e rispettare il contenuto essenziale di detti diritti e libertà. Nel rispetto del principio di proporzionalità, possono essere apportate limitazioni solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui*". Peraltro, va ricordato che la protezione offerta dalla Carta dei diritti UE deve essere coordinata con la CEDU[248],

---

Cass. 19.3.2019, n. 7708; M. G. STANZIONE, *Il regolamento europeo sulla privacy: origini e ambito di applicazione*, in *Eur. e dir. priv.*, 2016, pp. 1249; D. BARBIERATO, *Trattamento dei dati personali e nuova responsabilità civile*, in *Resp. civ. e prev.*, 2019, pp. 2151 ss.; A. RICCI, *Trattamento di dati sensibili e principio di responsabilizzazione*, in *Giur. it.*, 2018, pp. 2639.

Nella dottrina transazionale, si v. D. WRIGHT, K. WADHWA, M. LAGAZIO, C. RAAB, E. CHARIKANE, *Integrating privacy impact assessment in risk management in Data Privacy Law,* Vol. 4, No. 2, 2014, pp. 155-170; E. RAMIREZ, J. BRILL, M. K. OHLHAUSEN, J. D. WRIGHT, T. MCSWEENY, *Data Brokers. A Call for Transparency and Accountability*, Federal Trade Commission, 2014, pp. 1-58; I.S RUBINSTEIN, N. GOOD, *The trouble with Article 25 (and how to fix it): the future of data protection by design and default in International Data Privacy Law,* Vol. 10, No. 1, 2020, pp. 37-56.

In particolare si v. l'interessante analisi di D. WRIGHT (*A framework for the ethical impact assessment of information technology* in *Ethics and Information Technology,* 2011, pp. 199-226), che analizza in modo approfondito i principi del trattamento dei dati, il cui rispetto è fondamentale per lo sviluppo di un "*ethical impact assessment of information technology that could used by those developing new technologies, services, project, policies or programmes as a way to ensure that their ethical implications are adequately examined by stakeholders before possible deployment and so that mitigating measures can be taken as necessary*"; al contempo, l'autore evidenzia la necessità di considerare maggiormente, nello sviluppo di una *data protection* più efficace, i rischi etici e sociali derivanti dall'utilizzo dei dati. Interessante, inoltre, il fatto che l'autore proponga una *check-list* di domande, per ciascun principio del trattamento, che il titolare dovrebbe porsi per verificare se il trattamento di dati è conforme a quel dato principio.

[248] L'art. 52, par. 3, Carta dir. UE prevede che "*Laddove la presente Carta contenga diritti corrispondenti a quelli*

che prevede, all'art. 8, par. 2, che "*non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto* [al rispetto della vita privata e familiare] *a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui*". Da questo quadro normativo emerge, innanzitutto, che eventuali limitazioni al diritto alla protezione dei dati possono essere poste esclusivamente dalla legge (riserva assoluta di legge). In secondo luogo, il trattamento dei dati deve sempre essere compatibile con una società democratica e perseguire uno scopo legittimo, ossia assicurare interessi pubblici o di altri soggetti, ma che siano riconosciuti come rilevanti e leciti dall'ordinamento UE.

Dal combinato disposto delle due norme sopra citate emergono due ulteriori principi fondamentali del diritto alla protezione dati, ossia il principio di proporzionalità del trattamento e il principio di necessità. Sul punto, il Gruppo di Lavoro Articolo 29 ha precisato che "*le limitazioni ai diritti fondamentali devono essere interpretate restrittivamente, conformemente alla giurisprudenza della Corte europea dei diritti dell'uomo e della Corte di giustizia dell'Unione europea. Ciò implica che tutte le ingerenze devono essere necessarie e proporzionate alla finalità perseguita. Si deve inoltre tenere presente che non esiste una presunzione automatica dell'effettiva esistenza e validità delle giustificazioni di sicurezza nazionale avanzate da un'autorità nazionale: devono essere dimostrate*"[249]. Dunque, deve esservi una stretta proporzionalità e necessità nelle misure di limitazione dei diritti relativi alla protezione dei dati personali, come ribadito più volte, per altro, dalla Corte di Giustizia UE, secondo cui "*l'art. 52, n. 1, della Carta riconosce che possano essere apportate limitazioni all'esercizio di diritti come quelli sanciti dagli artt. 7 e 8 della medesima, purché tali limitazioni siano previste dalla legge, rispettino il contenuto essenziale di detti diritti e libertà e, nel rispetto del principio di proporzionalità, siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui*"[250].

Il principio di proporzionalità è, dunque, sovraordinato rispetto allo stesso Regolamento UE

---

garantiti dalla Convenzione europea per la salvaguardia dei Diritti dell'Uomo e delle Libertà fondamentali, il significato e la portata degli stessi sono uguali a quelli conferiti dalla suddetta convenzione. La presente disposizione non preclude che il diritto dell'Unione conceda una protezione più estesa".

[249] GRUPPO DI LAVORO ARTICOLO 29, *Parere 04/2014 sulla sorveglianza delle comunicazioni elettroniche a fini di intelligence e sicurezza nazionale*, all'indirizzo https://www.garanteprivacy.it/documents/10160/3815091/WP+215+Parere+042014+sorveglianza+comunicazioni+elettroniche.pdf.

[250] CORTE GIUST. UE, 9.11.2010, cause riunite C-92/09 e C-93/09, *Volker und Markus Schecke Gbr e Hartmut Eifert c. Land Hessen*.

2016/679; ma è da quest'ultimo ribadito sin dai Considerando introduttivi, ove si legge che se "*il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali"*, in ogni caso tale limitazione deve avvenire "…*in ossequio al principio di proporzionalità*" (Considerando n. 4).

Il principio di proporzionalità (e necessità) del trattamento è dunque essenziale per verificare la legittimità delle limitazioni poste dalle legislazioni nazionali al diritto alla protezione dei dati[251]; nella prospettiva della responsabilità del titolare, che qui interessa, la proporzionalità è la prima condizione perché il trattamento possa essere considerato lecito, in particolare in quelle ipotesi, di cui all'art. 52 Carta dir. UE, in cui il legislatore abbia consentito una "tutela affievolita" dei dati personali[252].

10. Il principio di necessità

Rispetto alla disciplina di cui alla Dir. 95/46/CE, con il Regolamento il legislatore europeo dimostra la scelta di favorire la circolazione dei dati personali: afferma l'art. 1, par. 3, GDPR che "*la libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali*".

Il legislatore prende atto della necessità della circolazione dei dati personali per lo sviluppo del mercato unico digitale, sicché l'uso dei dati deve essere consentito; dunque, lo spazio riservato all'autodeterminazione del singolo risulta eroso, tanto che al consenso sono affiancate ulteriori condizione di legittimità del trattamento. Al contempo, è necessario garantire che tali trattamenti avvengano in sicurezza e secondo modalità di correttezza e trasparenza, di modo da incrementare

---

[251] L'articolo 23 GDPR prevede che il diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o il responsabile del trattamento può limitare, mediante misure legislative, la portata degli obblighi e dei diritti di cui agli articoli da 12 a 22 e 34, nonché all'articolo 5, nella misura in cui le disposizioni ivi contenute corrispondano ai diritti e agli obblighi di cui agli articoli da 12 a 22, e purché vengano rispettate due condizioni: 1) la limitazione rispetti l'essenza dei diritti e delle libertà fondamentali; 2) la limitazione *"…sia una misura necessaria e proporzionata in una società democratica.."* e sia finalizzata a tutelare interessi specifici, elencati dallo stesso art. 23 GDPR. Su questo tema, in data 13.10.2021 l'EDPB ha approvato le *Guidelines 10/2020 on restrictions under Article 23 GDPR* (consultabili all'indirizzo https://edpb.europa.eu/system/files/2021-10/edpb_guidelines202010_on_art23_adopted_after_consultation_en.pdf), ove viene precisato che l'esercizio di un diritto può essere ritardato nel tempo, oppure esercitato parzialmente o circoscritto a determinate categorie di dati, ovvero ancora che un diritto venga esercitato indirettamente attraverso un'autorità di controllo indipendente. Tuttavia, restrizioni estese e invadenti che annullassero un diritto fondamentale del suo contenuto fondamentale, non sono giustificate. Né, in ogni caso, possono i titolari del trattamento comprimere i diritti degli interessati invocando direttamente i motivi di cui all'articolo 23, par. 1, GDPR. Per bilanciare le limitazioni con i diritti fondamentali del soggetto interessato e, quindi, rispettare l'art. 23 GDPR (e, ancor prima, l'art. 52 Carta Dir. UE), i legislatori nazionali devono effettuare un test di proporzionalità e necessità della misura da adottare. In particolare, dapprima deve essere verificata la necessità della misura, in secondo luogo la proporzionalità della stessa rispetto alla finalità da raggiungere. Affinché la misura possa essere considerata proporzionata, deve essere idonea a conseguire la finalità senza eccedere i limiti di quanto è appropriato e necessario per il raggiungimento di tale obbiettivo.

[252] F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati*, cit., p. 246.

anche la fiducia degli utenti nello sviluppo del mercato.

Come detto, ciò si evince chiaramente dal fatto che è il legislatore stesso, prima dell'interessato, ad effettuare il bilanciamento tra contrapposti interessi per individuare condizioni di legittimità del trattamento equipollenti rispetto al consenso.

Con il consenso, l'interessato verifica egli stesso i rischi del trattamento e valuta se sia opportuno iniziare o proseguire il trattamento[253], così bilanciando il proprio interesse con quelli coinvolti dal trattamento; nelle altre condizioni di legittimità, questo bilanciamento è stato svolto dal legislatore.

All'art. 6 GDPR è previsto, dunque, che il trattamento è lecito se fondato, alternativamente, sul consenso (par. 1, lett. a), oppure se esso è "necessario" a raggiungere una delle seguenti finalità: b) l'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso; c) l'adempimento di un obbligo legale al quale è soggetto il titolare del trattamento; d) la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica; e) l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento; f) il 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.

Dunque, il GDPR prevede che anche ulteriori interessi, portati da terzi, possano prevalere su quello dell'interessato: ciò si evince, in particolare, dalla lett. f) dell'art. 6, in cui vi è la retrocessione totale dell'autodeterminazione, venendo demandato al titolare il compito di effettuare il bilanciamento tra i diritti e le libertà degli individui e la "necessità" che il trattamento sia essenziale 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* […]". Eseguito positivamente il giudizio di necessità, il trattamento può, dunque, essere effettuato lecitamente dal titolare.

Il principio di necessità del trattamento per il perseguimento di interessi specifici connota, dunque, tutte le altre condizioni di legittimità del trattamento espresse dall'art. 6, tranne quella del consenso: in questo caso la sussistenza di un assenso manifestato validamente dall'interessato supera e assorbe l'opportunità di verificare la necessità del trattamento, dovendosi solo verificare che le finalità dello stesso siano state evidenziate con trasparenza all'individuo. Ma per le altre condizioni di legittimità

[253] La "base giuridica" costituita dal consenso suppone, dunque, che l'interessato sia effettivamente in grado di operare un coscienzioso bilanciamento tra benefici e rischi del trattamento. Tuttavia, come si dirà *infra,* in alcune circostanze è impossibile per l'interessato operare con successo questo bilanciamento. Questo dipende dalla complessità di funzionamento delle nuove tecnologie, nonché dall'elevatissimo uso di dati che ciascuna tecnologia e che possono potenzialmente essere aggregati con i dati raccolti in precedenza da dispositivi diversi.

deve verificarsi in modo rigoroso se è necessario l'utilizzo dei dati personali: laddove sia possibile raggiungere le finalità indicate nelle altre condizioni dell'art. 6 GDPR con modalità che non involgano l'uso di dati personali, sarà necessario scegliere tali modalità alternative.

Il principio di necessità del trattamento deve essere interpretato in modo alquanto rigoroso, come precisato dal Gruppo di Lavoro Articolo 29, nel "*Parere 6/2014 sul concetto di interesse legittimo del responsabile del trattamento ai sensi dell'articolo 7 della Direttiva 95/46/CE*"[254], ove si afferma che "*il criterio dell'interesse legittimo, insieme agli altri fondamenti giuridici ad esclusione del consenso, prevede l'esecuzione di un test di "necessità" che limita rigorosamente il contesto in cui ciascuno di essi può essere applicato*".

Svolto positivamente il giudizio di necessità, è necessario verificare, inoltre, che il trattamento sia proporzionato: il principio di minimizzazione dei dati impone, infatti, di scegliere quelle modalità di esecuzione del trattamento che comportano l'utilizzo del numero più ridotto di dati.

È il titolare stesso, sulla base del principio di *accountability*, che è tenuto a svolgere queste valutazioni per verificare che il trattamento posto in essere sia conforme al GDPR. Dunque, l'obbligo di *accountability* emerge già nella fase antecedente al trattamento, in cui il titolare del trattamento è tenuto a verificare quale sia la "base giuridica" del trattamento, al fine di fornirne idonea evidenza all'interessato con l'informativa[255].

11. Analisi delle condizioni di liceità ex art. 6 alla luce dei principi di liceità ex art. 5

Occorre ribadire che la legittimità della "base giuridica" che, ai sensi dell'art. 6 GDPR, rende legittimo il trattamento, deve essere valutata alla luce dei principi del trattamento di cui all'art. 5.

Le seguenti condizioni di legittimità del trattamento presenta profili di interesse per la presente analisi:

- il consenso, per il problema della sua libertà in relazione alla complessità dell'attuale società digitale;

---

[254] Parere 6/2014 sul concetto di interesse legittimo del responsabile del trattamento ai sensi dell'articolo 7 della Direttiva 95/46/CE, pubblicato il 9.4.2014, reperibile all'indirizzo https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_it.pdf.

[255] Sul punto, infatti, il Garante ha precisato che qualsiasi titolare che intenda effettuare un trattamento di dati personali fondato sul legittimo interesse, sia che i dati siano raccolti direttamente presso l'interessato sia che vengano ottenuti da altre fonti, "*dovrà fornire un'informativa che evidenzi opportunamente - specie qualora il trattamento preveda l'uso di nuove tecnologie o strumenti automatizzati - agli interessati la circostanza che sta trattando i dati che li riguardano sulla base di tale presupposto, nonché esplicitare quale sia il legittimo interesse in concreto perseguito, che andrà quindi opportunamente evidenziato come tale, a beneficio dell'interessato (artt. 13, par. 1, lett. d, e 14, par. 2, lett. b, del Regolamento)*" (Provvedimento del 22.2.2018, *Indicazioni preliminari di cui in motivazione volte a favorire la corretta applicazione delle disposizioni del Regolamento (UE) 2016/679*, consultabile all'indirizzo https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/8080493).

- l'esecuzione di un contratto, per il problema del rispetto dei principi di necessità e finalità;
- il legittimo interesse del titolare, per il problema del bilanciamento con i diritti e le libertà degli interessati, nonché per l'interpretazione di questa base giuridica alla luce del nuovo principio di *accountability*.

È opportuno, dunque, soffermarsi brevemente sull'analisi di tali presupposti legittimanti il trattamento.

12. Il consenso come condizione di liceità

Come anticipato, il consenso è condizione di liceità del trattamento che esclude il giudizio di necessità. Si tratta, evidentemente, di una condizione che, sebbene equipollente rispetto alle altre (ai fini del Regolamento tutte le basi giuridiche hanno uguale valore), ha connotati del tutto particolare. Il diritto alla protezione dei dati personali ha autorizzato la circolazione dei dati personali e il loro utilizzo a prescindere da una manifestazione di volontà, in una visuale nella quale il consenso esprimeva il potere decisionale dell'interessato nel campo dei diritti della personalità.

Tuttavia, se il mancato consenso non preclude il trattamento in presenza di differenti condizioni di liceità, esso rappresenta una condizione peculiare, che vede al centro lo stesso interessato[256].

Il consenso è definito dall'art. 4 GDPR come "*qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento*".

L'art. 7 ne detta una specifica disciplina. Con riferimento alle modalità di espressione del consenso nella fase pre-contrattuale, è previsto che se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso "*è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro*" (par. 2) e, inoltre, "…*prima di prestare il proprio consenso, l'interessato è informato di ciò*" (par. 3), con ciò evidenziandosi l'importanza del rispetto del principio di trasparenza. Il par. 2 prevede, come sanzione, che "...*nessuna parte di una tale dichiarazione che costituisca una violazione del presente regolamento è vincolante*".

Nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che "*l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto*".

---

[256] D. POLETTI, *Le condizioni di liceità del trattamento dei dati personali*, in *Giur. it.*, 2019, p. 2777;

Inoltre, il GDPR dispone che il consenso può essere revocato in qualsiasi momento dall'interessato e la revoca deve avvenire con la stessa facilità con cui era stato accordato, con ciò impedendo che vengano previsti costi, oneri o spese aggiuntivi. Il par. 4 precisa che la revoca non pregiudica la liceità del trattamento eseguito prima della revoca. La possibilità di revoca del consenso impedisce dunque la prosecuzione del trattamento che su di esso si fondava, a meno che il titolare non individui una condizione di liceità differente.

Il par. 1 pone, inoltre, un obbligo di *accountability* per il titolare, laddove prevede che qualora il trattamento sia basato sul consenso "*il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali*".

Sul punto, va inoltre evidenziato che, secondo il Considerando n. 32 del GDPR, il consenso dovrebbe essere espresso mediante un atto positivo inequivocabile con il quale l'interessato manifesta "*l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano, ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale. Ciò potrebbe comprendere la selezione di un'apposita casella in un sito web, la scelta di impostazioni tecniche per servizi della società dell'informazione o qualsiasi altra dichiarazione o qualsiasi altro comportamento che indichi chiaramente in tale contesto che l'interessato accetta il trattamento proposto*". Questo esclude, ad esempio, che sia lecita la preselezione di caselle, ossia un consenso fornito per "inattività" dell'utente. Se il consenso dell'interessato è richiesto attraverso mezzi elettronici, "*la richiesta deve essere chiara, concisa e non interferire immotivatamente con il servizio per il quale il consenso è espresso*" (Considerando n. 32).

12.1. (segue) La libertà del consenso

L'art. 7 prevede che, per verificare la libertà del consenso, è necessario tenere in considerazione se l'esecuzione di un contratto è condizionata alla prestazione del consenso, non necessario, al trattamento di dati personali.

È il caso in cui l'utente, per poter utilizzare o fruire di un servizio del titolare, è obbligato ad acconsentire al trattamento di dati che non sarebbero necessari per il servizio stesso; nel caso in cui l'utente si rifiutasse, non potrebbe accedere a tale servizio. Tale situazione si presenta frequentemente nell'utilizzo di *social network*: a fronte dell'utilizzo apparentemente gratuito di Facebook, gli utenti consentono l'utilizzo dei loro dati personali, sicché evidentemente è questo stesso utilizzo che diviene il corrispettivo per poter accedere al servizio.

Viene, dunque, introdotta una sorta di presunzione, nel senso che il legislatore presume che in tale situazione il consenso non sia effettivamente prestato con libertà, stante il forte condizionamento

subito dall'interessato che vuole accedere al servizio fornito dal titolare.

Il criterio per verificare, dunque, se il consenso sia, o meno, stato prestato in libertà, è costituito dalla natura e dalle caratteristiche stesse del consenso.

Evidentemente, laddove si trattasse di un servizio non essenziale, in quanto ad esempio ludico o reperibile presso altri titolari, non vi sarebbe alcuna coartazione nei confronti del soggetto, in quanto quest'ultimo potrebbe semplicemente rinunciare al servizio, oppure rivolgersi ad altri fornitori che non chiedono di utilizzare i dati personali.

Al contrario, laddove si trattasse di un servizio indispensabile, o un servizio a cui l'utente è obbligato per legge a fruire, allora non potrebbe dirsi libera la prestazione del consenso, proprio perché l'utente deve necessariamente concludere quel contratto. Sul punto, autorevole dottrina osserva, infatti, che "*il problema pratico più rilevante* [*omissis*] *riguarda le ipotesi in cui alla prestazione del consenso venga subordinata dalla controparte la conclusione del contratto o la prosecuzione del rapporto. Da un lato, infatti, sarebbe agevole affermare che non può considerarsi libero il consenso prestato da chi non poteva fare a meno del bene o del servizio offerto dalla controparte. Dall'altro, non sembra ipotizzabile un obbligo a contrarre in capo a chi ritiene indispensabile per lo svolgimento della propria attività il trattamento dei dati dei partner contrattuali*"[257].

Dunque, la libertà del consenso dovrà escludersi quando il servizio sia indispensabile per l'utente; sarà da considerarsi libero quando "*sussista un nesso di strumentalità fra trattamento dei dati e servizio offerto dal gestore: ove tale collegamento sia ravvisabile e si presenti solido, non potrà dubitarsi della legittimità della condotta negoziale del gestore, il quale condizioni l'erogazione del servizio al rilascio, da parte dell'utente, dei propri dati di registrazione e del consenso al relativo trattamento*"[258].

Anche la Cassazione ha confermato, in tema di consenso al trattamento dei dati personali[259], che "*la previsione dell'art. 23 del Codice della privacy, nello stabilire che il consenso è validamente prestato solo se espresso liberamente e specificamente in riferimento ad un trattamento chiaramente individuato, consente al gestore di un sito Internet, il quale somministri un servizio fungibile, cui l'utente possa rinunciare senza gravoso sacrificio (nella specie servizio di newsletter su tematiche legate alla finanza, al fisco, al diritto e al lavoro), di condizionare la fornitura del servizio al trattamento dei dati per finalità pubblicitarie, sempre che il consenso sia singolarmente ed*

---

[257] S. PATTI, *Il consenso dell'interessato al trattamento dei dati personali*, in *Riv. dir. civ*., 1999, pp. 455 ss.

[258] E. LUCCHINI GUASTALLA, *Il nuovo regolamento europeo sul trattamenti dei dati personali: i principi ispiratori,* in *Contr. e impr.,* 2018, p. 106.

[259] La pronuncia si riferisce al previgente art. 23 Codice privacy ma i principi in essa esposti sono certamente attuali anche alla luce della nuova disciplina.

inequivocabilmente prestato in riferimento a tale effetto"[260].

12.2. (segue) Il consenso e l'attività di marketing *attraverso profilazione*

Un ulteriore problema, in tema di consenso, è l'attività promozionale posta in essere dai *social network* attraverso le attività di profilazione degli utenti: i dati personali vengono utilizzati in modo automatizzato per individuare aspetti e caratteristiche personali dell'interessato, per analizzarne e prevederne il comportamento, al fine di offrire servizi o beni personalizzati e indurre il soggetto all'acquisto.

Sul punto, il Garante per la protezione dei dati personali ha affermato, in data 4.7.2013, che il "*consenso del contraente per l´attività promozionale deve intendersi libero quando non è preimpostato e non risulta -anche solo implicitamente in via di fatto- obbligatorio per poter fruire del prodotto o servizio fornito dal titolare del trattamento*" [261], precisando che "*non è libero il consenso prestato quando la società condiziona la registrazione al suo sito web da parte degli utenti e, conseguentemente, anche la fruizione dei suoi servizi, al rilascio del consenso al trattamento per la finalità promozionale. In quest'ottica, il Garante ha già espressamente affermato che non può definirsi "libero", e risulta indebitamente necessitato, il consenso a ulteriori trattamenti di dati personali che l'interessato "debba" prestare quale condizione per conseguire una prestazione richiesta*".

Inoltre, va ricordato, dall'un lato, l'art. 22 GDPR, che pone limitazioni all'attività di profilazione, laddove prescrive che "*l'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona*", dall'altro l'art. 122 Codice privacy[262], che disciplina le "*Informazioni raccolte nei riguardi del contraente o*

---

[260] CASS., 2.7.2018, n. 17278.

[261] AUTORITÀ GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Linee guida in materia di attività promozionale e contrasto allo spam*, consultabili all'indirizzo https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/2542348.

[262] Questa disposizione prevede che "l'*archiviazione delle informazioni nell'apparecchio terminale di un contraente o di un utente o l'accesso a informazioni già archiviate sono consentiti unicamente a condizione che il contraente o l'utente abbia espresso il proprio consenso dopo essere stato informato con modalità semplificate. Ciò non vieta l'eventuale archiviazione tecnica o l'accesso alle informazioni già archiviate se finalizzati unicamente ad effettuare la trasmissione di una comunicazione su una rete di comunicazione elettronica, o nella misura strettamente necessaria al fornitore di un servizio della società dell'informazione esplicitamente richiesto dal contraente o dall'utente a erogare tale servizio. Ai fini della determinazione delle modalità semplificate di cui al primo periodo il Garante tiene anche conto delle proposte formulate dalle associazioni maggiormente rappresentative a livello nazionale dei consumatori e delle categorie economiche coinvolte, anche allo scopo di garantire l'utilizzo di metodologie che assicurino l'effettiva consapevolezza del contraente o dell'utente*".

dell'utente", introdotto a seguito della direttiva ePrivacy[263].

Diviene, dunque, necessario coordinare il GDPR con la direttiva ePrivacy per verificare la legittimità di tale attività promozionale, svolta con l'utilizzo dei dati personali raccolti attraverso i cookies.

In particolare, se è nella direttiva ePrivacy che, nei casi previsti, si rinviene l'obbligo di acquisizione del consenso all'impiego di cookie e altri strumenti di tracciamento, andranno invece ricercate nel GDPR le specifiche caratteristiche di quel consenso ai fini della sua validità e conformità alla disciplina generale. Ed infatti, nelle recenti *Linee guida cookie e altri strumenti di tracciamento*, approvate il 10.6.2021, il Garante ha affermato che la disciplina della direttiva ePrivacy "*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. In nessun caso sarà pertanto possibile invocare ad esempio, come è stato invece osservato nel corso delle verifiche effettuate su diversi siti web, la scriminante del legittimo interesse del titolare per giustificare il ricorso a cookie o altri strumenti di tracciamento*"[264]. Da ciò emerge che affinché il consenso risulti acquisito legittimamente, il titolare dovrà far sì che le modalità di raccolta siano realizzate in modo tale da rendere inequivoco anche per l'utente l'effetto della propria azione, equivalente alla manifestazione del consenso stesso. Ciò allo scopo di limitare l'incidenza dei c.d. "falsi positivi", ossia di erronee interpretazioni di azioni casuali come espressioni consapevoli della volontà dell'utente. Qualora invece, nel caso concreto, "*all'azione dell'utente non corrisponda alcun evento informatico inequivoco, documentabile e dotato delle menzionate caratteristiche anche sotto il profilo della consapevolezza per lo stesso utente, allora in nessun modo sarà possibile attribuire a tale azione la validità del consenso ai sensi della normativa vigente*".

12.3. (segue) Il problema del consenso nell'attuale società tecnologica

Sono i più recenti sviluppi delle tecnologie della comunicazione e il diffuso uso dei *social media* che pongono interrogativi sulla concezione tradizionale del consenso per l'utilizzo dei dati personali. Ed infatti, si è recentemente sviluppato un dibattito, in dottrina e giurisprudenza, sulla reale natura del consenso e sulla natura dei dati personali. Questo perché nella realtà del mercato digitale attuale, il consenso viene ad acquisire sovente natura negoziale vera e propria e i dati personali divengono essi stessi oggetto del contratto e prezzo per il servizio offerto, circostanze che ne fanno emergere la natura

[263] Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12.7.2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche.

[264] Consultabili all'indirizzo https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9677876

economico-negoziale accanto alla loro natura personalistica[265].

Inoltre, come dimostrato anche da recenti indagini comportamentali[266], all'aumentare delle reiterate richieste di consenso sul web l'utente riduce la propria soglia di attenzione, anche per l'informativa, con conseguente "*debolezza cognitiva e compromissione del processo decisionale*". Ed infatti, la dottrina ha evidenziato il paradosso del sistema basato sul consenso, il quale diviene non tanto strumento di salvaguardia dell'interesso, quanto strumento di garanzia per il titolare per dimostrare di aver adempiuto agli obblighi di *accountability*, poiché gli utenti si limitano distrattamente a prestare un mero assenso al trattamento, senza effettivamente verificare le modalità e finalità dello stesso, pur di accedere a qualsiasi servizio offerto dal titolare.

A ciò va aggiunta l'impossibilità per l'utente, anche informato e razionale, di svolgere un adeguato bilanciamento tra i costi e i benefici, quando i dati confluiscono all'interno dei *Big Data*[267].

È praticamente impossibile per l'individuo verificare quale sia il rischio conseguente all'aggregazione dei dati[268]. I dati vengono raccolti da una molteplicità di titolari, attraverso i sensori più differenti[269], e vengono successivamente trasferiti per essere aggregati con dati già raccolti in precedenza. Dall'analisi di queste informazioni esistenti possono ricavarsi previsioni più o meno precise, sino a giungere alla conoscenza di elementi particolarmente complessi e intimi dell'individuo.

Dunque, per esprimere un consenso veramente libero ed informato ad un trattamento di dati, l'interessato dovrebbe poter comprendere tutti i rischi che conseguono dall'aggregazione di quel dato, con tutti gli altri dati di cui ha già autorizzato, in qualche forma, il trattamento. In queste ipotesi, infatti, il rischio deriva proprio dall'aggregazione, e si tratta evidentemente di un rischio non calcolabile e quantificabile dal singolo utente[270].

L'evolversi della tecnologia dei *Big Data* e degli strumenti predittivi dimostra l'inefficienza del

---

[265] G. VERSACI, *La contrattualizzazione dei dati personali dei consumatori*, Esi, 2020.

[266] D. POLETTI, *op. cit.*; P. PASSAGLIA-D. POLETTI, *Nodi virtuali, legami informali. Internet alla ricerca di regole,* Pisa University Press, 2017.

[267] D. J. SOLOVE, *Introduction: privacy self-management and the consent dilemma*, in *Harward Law Review*, 2013, Vol. 126: 1934, pp. 1880-1903.

[268] Sui meccanismi di aggregazione dei dati si veda il report sui *Data Brokers* della Federal Trade Commission (2014), ove si osserva che "*in general, the data brokers collect information about consumers from a wide variety of commercial, government, and other publicly available sources. In developing their products, the data brokers use not only the raw data they obtain from these sources, such as a person's name, address, home ownership status, or age, but also certain derived data, which they infer about consumers. For example, a data broker might infer that an individual with a boating license has an interest in boating, that a consumer has a technology interest based on the purchase of a "Wired" magazine subscription, or that a consumer who has bought two Ford cars has loyalty to that brand. The data brokers use this actual and derived data to create three main kinds of products for clients in a wide variety of industries: marketing products, risk mitigation products, and people search products*". Così E. RAMIREZ-J. BRILL-M. K. OHLHAUSEN-J. D. WRIGHT-T. MCSWEENY, *Data Brokers. A Call for Transparency and Accountability*, op. cit., pp. 1-58.

[269] Sull'incorporazione dei sensori e degli strumenti di controllo nella tecnologia, v. G. ZICCARDI, *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica*, Raffaello Cortina Editore, 2015, pp. 115 ss.

[270] D. J. SOLOVE, *op. cit.*

sistema di tutela basato sul solo consenso.
Il GDPR si fonda anche sulla consapevolezza che il baricentro della disciplina deve essere spostato dall'autodeterminazione del singolo, attraverso il consenso, ad un sistema di obblighi per il titolare, attraverso la responsabilizzazione. Tuttavia, questa "rivoluzione" è solo incompleta.
Il consenso riveste un ruolo ancora fondamentale come base giuridica del trattamento e, soprattutto, gli strumenti rimediali sono affidati principalmente all'individuo. Inoltre, come si vedrà nel capitolo successivo, il sistema di tutela della responsabilità civile di cui all'art. 82 presenta seri problemi di effettività, soprattutto per la difficoltà di accertare e quantificare i danni conseguenti al trattamento illecito.
A ciò va aggiunto che il sistema di gestione del rischio disegnato dal GDPR (v. capitolo successivo) risulta incompleto perché non considera anche i rischi collettivi, come quelli etici e sociali, derivanti dal trattamento.

13. Il trattamento necessario per l'esecuzione dei contratti per i servizi digitali

L'art. 6 GDPR prevede, alla lett. b), che il trattamento di dati personali è lecito se necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso.
Si tratta dunque di una condizione di liceità alternativa al consenso, che merita particolare attenzione perché, nell'attuale società in cui sovente i dati personali sono l'oggetto del contratto (o, comunque, la controprestazione rispetto al servizio offerto dal titolare)[271], queste due basi giuridiche per il trattamento possono venire a sovrapporsi o confondersi.
Ed infatti, in data 8.10.2019 il Comitato europeo di protezione dei dati (EDPB) ha dedicato all'analisi di questa base giuridica le *Linea 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*[272], dove si evidenzia che proprio l'attuale complessità dei servizi offerti tramite Internet e il problema contratti in cui il trattamento dei dati costituisce il corrispettivo per il servizio; afferma l'EDPB che "*la diffusione di Internet sempre attivo sui dispositivi mobili e l'ampia disponibilità di dispositivi connessi hanno consentito lo sviluppo di servizi online in settori quali i social media, il commercio elettronico, la ricerca su Internet, la comunicazione e i viaggi. Mentre taluni di questi servizi sono finanziati dai pagamenti degli utenti,*

[271] Nell'attuale società digitale è comune la pratica dello scambio di dati personali contro l'acquisto di servizi online; a tali contratti fa espresso riferimento la Dir. UE 2019/770, che si applica anche quando, in cambio di un contenuto o di un servizio digitale, il consumatore "*fornisce o si impegna a fornire dati personali all'operatore economico*".
[272] Consultabili all'indirizzo https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_it.pdf .

altri sono forniti senza un corrispettivo monetario da parte del consumatore essendo invece finanziati dalla vendita di servizi pubblicitari online che permettono di rivolgersi in maniera mirata agli interessati. Il tracciamento del comportamento degli utenti ai fini di tale pubblicità è di frequente effettuato secondo modalità ignote all'utente; inoltre, tale attività può non essere immediatamente evidente in ragione della natura del servizio fornito, circostanza questa che rende praticamente impossibile all'interessato l'esercizio di una scelta informata sull'utilizzo dei propri dati".

La (seconda) ipotesi del trattamento necessario all'esecuzione di misure precontrattuali fa riferimento a quei casi in cui l'interessato abbia, su propria iniziativa, contattato il titolare per ricevere un'offerta o preventivo di spesa relativamente all'acquisto di un prodotto o servizio. In queste ipotesi il titolare avrà diritto al trattamento dei dati all'esclusivo fine di adempiere alla richiesta dell'interessato: il trattamento evidentemente potrà involgere anche la conservazione successiva dei dati, ma solo per finalità specifiche e per un congruo tempo.

Nell'altra ipotesi descritta dalla lett. b), l'interessato comunica i propri dati personali proprio perché essi sono funzionali all'accordo contrattuale, che non può essere attuato senza il trattamento dei dati. Dunque, il consenso all'accordo negoziale assorbe la necessità di un consenso specifico all'utilizzo dei dati personali, perché evidentemente lo postula.

Viene, dunque, consentito al titolare, in genere fornitore di servizi, ma potrebbe essere fornitore di un prodotto, di trattare i dati personali così da adempiere all'accordo negoziale concluso con la persona fisica.

Come tutte le condizioni legittimanti il trattamento, è fondamentale il rispetto del principio di necessità: dunque, il titolare può ricorrere a tale base giuridica solo laddove il trattamento sia strettamente necessario e funzionale all'adempimento degli obblighi contrattuali, non potendo attuare trattamenti con finalità differente rispetto all'esecuzione del contratto. Ad esempio, non potrebbero essere utilizzati i dati dell'interessato per svolgere attività ulteriore di *marketing* non autorizzata. Pertanto, tali ulteriori attività di trattamento potrebbero essere svolte dal titolare solo individuando una differente e valida base giuridica, come potrebbe essere – ove opportunamente bilanciato – il proprio legittimo interesse.

Anche l'EDBP ha evidenziato l'importanza del rispetto del principio di necessità, affermando che nella valutazione della liceità del trattamento basato sulla lett. b) si dovrebbe tener conto dello scopo, della finalità o dell'obiettivo specifico/a del servizio. In particolare, l'EDBP ha affermato che "*è necessario che il trattamento sia oggettivamente necessario per una finalità che è parte integrante della prestazione di tale servizio contrattuale all'interessato. Il trattamento dei dati relativi al pagamento ai fini dell'addebito del servizio non è escluso da tale contesto. Il titolare del trattamento dovrebbe essere in grado di dimostrare in che modo l'oggetto principale del contratto specifico*

stipulato con l'interessato non sia di fatto realizzabile senza lo specifico trattamento dei dati personali in questione. Essenziale in questo contesto è il nesso tra i dati personali e i trattamenti in questione, nonché l'esecuzione o meno del servizio reso ai sensi del contratto". Di conseguenza, un contratto non può ampliare artificiosamente le categorie di dati personali o le tipologie di trattamenti che il titolare necessita di effettuare per l'esecuzione del contratto ai sensi dell'articolo 6, paragrafo 1, lettera b)[273].

Come sopra precisato, questa base giuridica pone notevoli problemi applicativi nella odierna realtà dei contratti per i servizi digitali, dove può sorgere una confusione applicativa con la differente base giuridica costituita dal consenso, di cui alla lett. a) art. 6.

L'EDPB sottolinea infatti che "*a seconda delle circostanze, gli interessati possono erroneamente avere l'impressione di esprimere un consenso in linea con l'articolo 6, paragrafo 1, lettera a), firmando un contratto o accettando condizioni di servizio. Al tempo stesso, un titolare del trattamento potrebbe erroneamente presumere che la firma di un contratto corrisponda a una manifestazione di consenso ai sensi dell'articolo 6, paragrafo 1, lettera a)*". Tuttavia, sono concetti assolutamente differenti, sicché è essenziale distinguere l'ipotesi dell'accettazione delle condizioni di servizio ai fini dell'esecuzione del contratto di cui alla lett. b) art. 6, dalla diversa ipotesi del consenso al trattamento di dati di cui alla lett. a) art. 6.

Ecco, perciò, che il contratto che ad oggetto il trattamento dei dati personali come corrispettivo (prezzo) di un servizio solleva notevoli problematiche interpretative, come dimostra l'attuale dibattito della dottrina attorno a questi accordi negoziali.

In particolare, si è ormai riconosciuta la natura anche "commerciale" dei dati, accanto alla natura personale, accettando quegli scambi negoziali che hanno ad oggetto proprio i dati personali. Ciò comporta anche una tutela ampliata per l'interessato, che può far valere nei confronti del titolare non solo la disciplina di cui al regolamento per la protezione dei dati personali, che si fonda principalmente sulla natura individualistica dei dati, ma anche su forme di tutela alternative proprie del diritto dei contratti e delle obbligazioni, tra cui la disciplina per la tutela del consumatore[274].

---

[273] Se il contratto è costituito da più servizi distinti o da più elementi di un servizio distinti che di fatto possono essere svolti separatamente l'uno dall'altro, si pone la questione circa la misura in cui l'articolo 6, paragrafo 1, lettera b), possa fungere da base giuridica. Per il rispetto del principio di necessità, l'applicabilità dell'articolo 6, paragrafo 1, lettera b), dovrebbe essere valutata nel contesto di ciascuno di tali servizi separatamente, considerando ciò che è oggettivamente necessario per ciascuno dei singoli servizi che l'interessato ha attivamente richiesto o sottoscritto. Di conseguenza, potrebbe accadere che l'esecuzione del contratto funga da base giuridica solo per determinati trattamenti, mentre l'esecuzione di alcuni trattamenti sia necessaria, ad esempio, per il legittimo interesse del titolare. Tali basi giuridiche andranno, dunque, separatamente individuate ed evidenziate con precisione e trasparenza all'interessato.

[274] M. DELL'UTRI, *Principi generali e condizioni di liceità del trattamento dei dati personali*, in *I dati personali nel diritto*

Ciò comporta anche il sorgere di responsabilità ulteriori per il titolare[275], che è tenuto nei confronti dell'interessato anche alla responsabilità contrattuale conseguente alla stipulazione dell'accordo con il consumatore, con la conseguenza che l'interessato potrà contare anche su rimedi ulteriori[276].

14. Il legittimo interesse del titolare

La lett. f) dell'art. 6 GDPR prevede, appunto, che il trattamento è legittimo se necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, interesse che deve essere bilanciato con 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).

Questa base giuridica è piena espressione del principio di *accountability* e dimostra il cambio di prospettiva rispetto al sistema previgente, basato sul sistema autorizzatorio. Nell'ambito della lett. f), al titolare è demandato il compito di operare il bilanciamento del proprio interesse, per verificare se esso prevale sui diritti e le libertà degli interessati.

---

europeo, a cura di V. CUFFARO-R. D'ORAZIO-V. RICCIUTO, Giappichelli, 2019.

Sulla complementarietà tra la disciplina per la protezione dei dati, il diritto dei consumatori e la disciplina per la libera concorrenza del mercato, si v. I. GRAEF, D. CLIFFORD, P. VALCKE, *Fairness and enforcement: bridging competition, data protection and consumer law* in *International Data Privacy Law,* Vol. 8, No. 3, 2018, pp. 200-223. Gli autori evidenziano che il diritto per la protezione dei dati concorre a rendere maggiormente incisive ed effettive le tutele per i consumatori e la disciplina sulla concorrenza; osservano che "*the three areas of law complement each other and protect different dimensions of consumer welfare. While data protection law aims to protect autonomous decision-making by data subjects but also more broadly includes the safeguarding of a secure and fair personal data processing environment, consumer protection law empowers individuals to make well-informed autonomous choices. Therefore, although consumer protection and data protection clearly overlap, as data protection applies whenever personal data are processed, it is distinct since it is not solely connected to the protection of an individual's decision-making capacity and choices. Competition law, for its part, aims to keep markets competitive so to ensure that consumers have such choices. As such, competition enforcement is vital to protect consumers against distortions of competition but a precondition for the existence of a wellfunctioning market is that individuals are able to exercise a genuine and informed choice. To that end, the effective implementation and enforcement of information requirements in consumer protection law and conditions for valid consent in data protection law in particular, are key. Competition law thus aims to ensure the availability of choice whereas data protection and consumer protection law aim at effectively empowering individuals exercise such a choice. Hence, competition, data protection and consumer law have to go hand in hand in order to adequately protect consumer interests*".

[275] La commercializzazione dei dati personali comporta, inoltre, la possibilità d'intervento dell'Autorità garante della concorrenza e del mercato e la possibilità per gli utenti di far valere la disciplina in tema di protezione della concorrenza, con i rimedi conseguenti alle pratiche commerciali sleali. Sul punto, si veda infatti AGCM, 11.5.2017, con il commento di G. CODIGLIONE, *I dati personali come corrispettivo della fruizione di un servizio di comunicazione elettronica e la "commercializzazione" della privacy*, in *Dir. inf. e inform*., 2017, pp. 418 ss.

[276] Sul cumulo dei rimedi inibitori, risarcitori, satisfattivi e ablativi, si v. l'approfondita analisi di G. VERSACI, *La contrattualizzazione dei dati personali dei consumatori*, Esi, 2020, spec. pp. 196 ss., il quale evidenzia che il medesimo fatto illecito (la violazione del GDPR) può determinare l'attivazione di differenti tipi di tutele: "*una* tutela invalidante*, la nullità di protezione, qualora la violazione sia fatta oggetto di una clausola negoziale; una* tutela satisfattiva*, il ripristino della conformità del bene, contenuto o servizio digitale, oppure* reintegratoria-demolitoria*, la riduzione del prezzo o la risoluzione del contratto, laddove la violazione della* data protection *assurga a difetto di conformità; una* tutela inibitoria*, la cancellazione dei dati personali o la limitazione del trattamento, prevista in caso di trattamento illecito; una* tutela riparatoria-compensatoria*, il risarcimento dei datti subiti a causa dell'illiceità commessa*".

Per evitare sovrapposizioni con la base giuridica costituita dall'art. e), che consente il trattamento quando 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*", l'art. 6, par. 2, prevede che la base giuridica del legittimo interesse non possa essere invocata per considerare leciti i trattamenti effettuati dalle autorità pubbliche nell'esecuzione dei loro compiti.

La disciplina anteriore prevedeva la possibilità che i trattamenti fossero effettuati se necessario al perseguimento del legittimo interesse del titolare, tuttavia era previsto un meccanismo autorizzatorio, nel quale era il Garante a valutare preventivamente la prevalenza rispetto ai diritti degli interessati[277]: ora il bilanciamento deve essere effettuato dal titolare, che si assume la responsabilità di effettuare questo giudizio.

Il GDPR individua alcuni casi esemplificativi di "legittimo interesse del titolare":

- potrebbero sussistere tali legittimi interessi quando sussiste una relazione tra l'interessato e il titolare del trattamento, ad esempio quando l'interessato è un cliente o è alle dipendenze del titolare del trattamento (Considerando n. 47)[278].
- costituisce legittimo interesse del titolare del trattamento interessato trattare dati personali strettamente necessari a fini di prevenzione delle frodi (Considerando n. 47).
- può essere considerato legittimo interesse trattare dati personali per finalità di marketing diretto (Considerando n. 47);
- i titolari del trattamento facenti parte di un gruppo imprenditoriale o di enti collegati a un organismo centrale possono avere un interesse legittimo "*a trasmettere dati personali all'interno del gruppo imprenditoriale a fini amministrativi interni, compreso il trattamento di dati personali dei clienti o dei dipendenti*" (Considerando n. 48)[279].
- costituisce legittimo interesse del titolare del trattamento interessato trattare dati personali relativi al traffico, in misura strettamente necessaria e proporzionata "*per garantire la sicurezza delle reti e dell'informazione, vale a dire la capacità di una rete o di un sistema d'informazione di resistere, a un dato livello di sicurezza, a eventi imprevisti o atti illeciti o*

---

[277] Questa base giuridica era prevista sin dalla l. n. 675/1996. Tuttavia, l'applicabilità era stata notevolmente ridotta con il d.lgs. n. 467/2001, che aveva disposto che in assenza di consenso il trattamento era consentito per il legittimo interesse del titolare solo "*nei casi individuati dal Garante sulla base dei principi sanciti dalla legge*" e aveva, altresì, previsto che il legittimo interesse dovesse essere bilanciato non solo con i "*i diritti e libertà fondamentali dell'interessato*", ma anche con "*la dignità o un legittimo interesse dell'interessato*" (art. 12, lett. h-*bis*).

[278] Il Considerando n. 47 precisa che "*in ogni caso, l'esistenza di legittimi interessi richiede un'attenta valutazione anche in merito all'eventualità che l'interessato, al momento e nell'ambito della raccolta dei dati personali, possa ragionevolmente attendersi che abbia luogo un trattamento a tal fine*".

[279] Il Considerando n. 48 precisa che "*sono fatti salvi i principi generali per il trasferimento di dati personali, all'interno di un gruppo imprenditoriale, verso un'impresa situata in un paese terzo*".

dolosi che compromettano la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati personali conservati o trasmessi e la sicurezza dei relativi servizi offerti o resi accessibili tramite tali reti e sistemi da autorità pubbliche, organismi di intervento in caso di emergenza informatica (CERT), gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRT), fornitori di reti e servizi di comunicazione elettronica e fornitori di tecnologie e servizi di sicurezza" (Considerando n. 49)[280].

- Ulteriori casi esemplificativi sono raccolti nel *Parere 6/2014 sul concetto di interesse legittimo del responsabile del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE"*:
- esercizio del diritto alla libertà di espressione e d'informazione, anche nei mezzi di comunicazione e di espressione artistica;
- commercializzazione diretta tradizionale e altre forme di commercializzazione o pubblicità;
- messaggi indesiderati non commerciali, anche a fini di campagne politiche o di raccolta fondi per scopi benefici;
- esercizio di un diritto in via giudiziale, compreso il recupero del credito tramite
- procedure extragiudiziali;
- prevenzione di frodi, uso improprio dei servizi o riciclaggio di denaro;
- controllo del personale a fini di sicurezza o gestione;
- procedure per la denuncia delle irregolarità;
- sicurezza fisica, sicurezza informatica e sicurezza della rete;
- trattamento di dati a scopi statistici o di ricerca storica o scientifica;
- trattamento a scopi di ricerca (compresa la ricerca a fini commerciali.

Si tratta di ipotesi in cui "*potrebbe*" sussistere il legittimo interesse del titolare, ma evidentemente il giudizio di bilanciamento deve sempre essere svolto in concreto, valutando tutte le circostanze specifiche del caso.

Il *Parere 6/2014* detta, inoltre, alcune indicazioni che il titolare del trattamento può adottare per svolgere adeguatamente il test di bilanciamento, onde verificare se il proprio interesse può considerarsi legittimo: si tratta di mere indicazioni che, tuttavia, il titolare è tenuto a seguire, in un'ottica di *accountability* e deve dare la prova di aver seguito in sede di eventuale controllo successivo.

Innanzitutto, è necessario individuare e valutare correttamente l'interesse legittimo del titolare. Esso può essere valutato come preminente, ad esempio, se corrisponde all'esercizio di un diritto

[280] Ciò include, ad esempio, le misure atte a impedire l'accesso non autorizzato a reti di comunicazioni elettroniche e la diffusione di codici maligni, e a porre termine agli attacchi da blocco di servizio e ai danni ai sistemi informatici e di comunicazione elettronica (Considerando n. 49).

fondamentale riconosciuto dalla Carta dei diritti fondamentali dell'UE o dalla Convenzione europea dei diritti dell'uomo, oppure potrebbe corrispondere ad un interesse della collettività (ad esempio, un ente senza scopo di lucro potrebbe trattare dati personali per campagne di sensibilizzazione di interessi della collettività).

Dopo aver individuato questo interesse, il Parere 6/2014 detta alcuni orientamenti per agevolare il titolare nella valutazione dell'impatto del trattamento sui diritti degli interessati, sottolineando che è fondamentale comprendere che "l'impatto" di cui trattasi è concetto più ampio rispetto al nocumento o al danno che possono essere arrecati a uno o più interessati predeterminati. Nello specifico, il termine "impatto" "…*comprende tutte le possibili (potenziali o effettive) conseguenze del trattamento dei dati"*; inoltre, questo concetto "*non è correlato alla nozione di violazione dei dati ed è molto più ampio rispetto alle conseguenze che potrebbero derivare da una violazione dei dati. Il concetto di impatto quale utilizzato nel presente parere, invece, contempla i vari modi in cui il trattamento dei dati personali potrebbe incidere, positivamente o negativamente, su un interessato*".

Nella valutazione dell'impatto sugli interessati devono essere tenuti in considerazioni diversi fattori, come la natura dei dati trattati, le modalità del trattamento, le ragionevoli aspettative dell'interessato riguardo all'utilizzo e alla comunicazione dei dati, lo status del titolare del trattamento e lo status dell'interessato. Successivamente, il titolare effettuerà un bilanciamento "provvisorio", che andrà svolto tenendo in considerazione anche le misure adottare dal titolare per assolvere agli obblighi generali di cui al GDPR. Il rispetto degli obblighi generali potrebbe, tuttavia, non essere di per sé sufficiente: potrebbe dunque rivelarsi necessario svolgere un'ulteriore valutazione nei casi in cui, sulla base dell'analisi preliminare e provvisoria, non è chiaro in quale modo deve essere operato il bilanciamento.

Il Parere spiega, dunque, che in questa fase il responsabile del trattamento potrebbe valutare la possibilità di introdurre misure supplementari, che vadano oltre il rispetto delle disposizioni che impongono gli obblighi generali, per contribuire a ridurre l'impatto negativo del trattamento sugli interessati. Viene posto l'accento sulla necessità di svolgere un test "*meticoloso ed effettivo*", che deve essere basato "*sulle specifiche circostanze del caso, anziché operare in maniera astratta, tenendo altresì conto delle ragionevoli aspettative degli interessati"*, e come norma di *accountability*, *"l'esecuzione di questo test deve essere documentata in maniera sufficientemente dettagliata e trasparente da permettere di verificare la completa e corretta applicazione del test, se del caso, da parte dei soggetti pertinenti, tra cui gli interessati e le autorità di protezione dei dati nonché, in ultima analisi, dei tribunali competenti*".

15. Il principio di correttezza e trasparenza (alla luce della liceità)

L'art. 5, lett. a), prevede che i dati devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato.

I concetti di correttezza e liceità sono intrinsecamente connessi, tuttavia autorevole dottrina ha tentato di individuarne una distinzione. Secondo questo orientamento, correttezza significa, in particolare, il rispetto dei doveri del titolare nei confronti dell'interessato e nei rapporti con le Autorità di controllo, con la conseguenza che potrebbero esservi violazioni del principio di correttezza che non determinino immediatamente anche violazioni alla liceità del trattamento, mentre, al contrario, difficilmente una violazione del principio di liceità non comporta anche violazione alla correttezza.

Tuttavia, la distinzione non è agevole e, al contrario, sembrerebbe comunque plausibile affermare che la liceità è principio sovraordinato rispetto agli altri e riguarda sia la sussistenza di una valida base giuridica del trattamento, sia il rispetto di tutti gli obblighi relativi alla fase concreta in cui il trattamento è effettivamente posto in essere, sicché la correttezza sembrerebbe costituire, semmai, un particolare "profilo" della liceità, un modo d'essere della stessa.

La trasparenza è concetto che caratterizza l'intera disciplina della protezione dei dati personali[281]. La Sezione prima del GDPR è intitolata "*Trasparenza e modalità*" e l'art. 12 (rubricato "*Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato"*), detta una procedimentalizzazione delle modalità comunicative delle informazioni finalizzato proprio a garantire la trasparenza delle stesse, in quanto prevede che tutte le comunicazioni e informative relative al trattamento debbano essere rese "*in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori. Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici*"[282].

---

[281] Il Considerando n. 30 del GDPR descrive compiutamente il contenuto del principio di trasparenza, laddove prevede che "*dovrebbero essere trasparenti per le persone fisiche le modalità con cui sono raccolti, utilizzati, consultati o altrimenti trattati dati personali che li riguardano nonché la misura in cui i dati personali sono o saranno trattati*". Tale principio impone *"che le informazioni e le comunicazioni relative al trattamento di tali dati personali siano facilmente accessibili e comprensibili e che sia utilizzato un linguaggio semplice e chiaro*" e riguarda *l'informazione degli interessati sull'identità del titolare del trattamento e sulle finalità del trattamento e ulteriori informazioni per assicurare un trattamento corretto e trasparente con riguardo alle persone fisiche interessate".* Esso impone una forte collaborazione e responsabilizzazione del titolare, che è tenuto a spiegare esattamente agli interessi i rischi che potrebbero derivare dal trattamento*;* inoltre, la trasparenza impone di precisare ed evidenziare, in maniera esplicita, le finalità del trattamento (Considerando n. 30).

[282] Nel report del 2014 sui *Data Brokers*, la Federal Trade Commission sottolinea l'importanza del rispetto del principio di trasparenza, proponendo "*for example, it proposed exploring the idea of a centralized website where data brokers that compile and sell data for marketing purposes could identify themselves to consumers, describe how they collect consumer information, disclose the types of companies to which they sell the information, and explain the access rights and other choices they offer consumers. The Commission's recommendations regarding data brokers built on almost two decades of work on these issues—indeed, decades marked by an expansion in the number of data brokers and the richness of data*

Inoltre, la trasparenza riguarda anche i diritti degli interessati, nel senso che il titolare del trattamento è tenuto ad agevolare l'interessato nell'esercizio dei propri diritti (art. 12, par. 2)[283], anche nel diritto di accesso. Ed è fondamentale evidenziare che questa prescrizione si riferisce non solo alle ipotesi in cui il trattamento viene effettuato sulla base del consenso dell'interessato, ma riguarda tutti i tipi di trattamento.

Per garantire la piena trasparenza, chi intende effettuare un trattamento di dati personali deve, dunque, fornire all'interessato le informative di cui agli artt. 13 e 14 GDPR prima di effettuare il trattamento, ossia prima della raccolta dei dati, se questa avviene presso l'interessato (art. 13), oppure entro un termine ragionevole, comunque non superiore al mese (art. 14).

Fatte salve alcune eccezioni, chi intende effettuare un trattamento di dati personali deve fornire all'interessato alcune informazioni anche per metterlo nelle condizioni di esercitare i propri diritti (articoli 15-22 del Regolamento medesimo).

Gli artt. 13 e 14 elencano in modo tassativo i contenuti minimi di questa informativa[284], ossia: a) l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante; b) i dati di contatto del responsabile della protezione dei dati, se nominato; c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento; d) qualora il trattamento si fondi sul legittimo interesse perseguiti dal titolare del trattamento o da terzi, esso deve essere indicato; e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali; f) l'eventuale intenzione del titolare del trattamento di trasferire[285] dati personali a un paese terzo o a

---

they collect, but little progress in providing transparency and choices to consumers about their practices. While the Commission recognizes the benefits that data brokers offer, it continues to support legislation to provide consumers with more information and meaningful choices about data broker practices".

[283] L'art. 12 detta una disciplina precisa e specifica delle modalità di accesso e di esercizio dei diritti dell'interessato. Il par. 2 precisa, ad esempio, che il titolare può rifiutare l'esercizio dei diritti solo quando non sia in grado di identificare l'interessato.

Il titolare è tenuto a rispondere alla richiesta senza ritardo e, comunque, entro un mese, termine che può essere prorogato di due mesi in base alla complessità e al numero delle richieste; in ogni caso, della proroga è necessario informare gli interessi, indicando i motivi del ritardo.

[284] L'art. 13, par. 2, indica ulteriori informazioni che vanno rese "*nel momento in cui i dati sono stati raccolti*", ossia: a) il periodo di conservazione dei dati personali b) l'esistenza del diritto dell'interessato nonché degli altri diritti relativi ai dati; c) le informazioni relative al diritto di revoca, quando sussistente; d) il diritto di proporre reclamo a un'autorità di controllo; e) se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati; f) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

[285] E, in questo caso, l'informativa deve indicare "*l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, paragrafo 1, secondo comma, il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali garanzie o il luogo dove sono state rese disponibili*".

un'organizzazione internazionale.

16. Il principio di finalità

Il principio di finalità è da sempre[286] al centro delle discipline per la protezione dei dati personali[287], ed è previsto dalla lett. b) dell'art. 6 GDPR, secondo cui i dati personali devono essere "*raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità*".

Il principio ha due componenti:

- il titolare del trattamento deve raccogliere i dati solo per finalità determinate, esplicite e legittime;
- i dati una volta raccolti non devono essere ulteriormente trattati in modo incompatibile con quegli scopi.

Come osservato dal Gruppo di Lavoro Articolo 29 nell' *Opinion 03/2013 on purpose limitation*, quando le persone condividono dati personali con altri, hanno una legittima aspettativa sulle finalità per cui i dati saranno utilizzati. È necessario rispettare queste aspettative e preservare la fiducia e la certezza degli utenti: questo è il motivo per cui la limitazione delle finalità è così importante, in quanto inibisce ai titolari l'utilizzo dei dati personali al di là delle finalità per le quali sono stati inizialmente raccolti.

È evidente che i dati già raccolti potrebbero essere realmente utili per altre finalità, non specificate inizialmente: essi possono generare un valore importante e fondamentale nell'attuale realtà digitale, per lo sviluppo delle attività di *data analytics*. Pertanto, c'è un valore, riconosciuto dal GDPR, nel consentire un certo grado di utilizzo aggiuntivo dei dati già raccolti, all'interno di limiti accuratamente bilanciati. Infatti, il divieto di "incompatibilità" nelle finalità, di cui all'art. 6, lett. b), non esclude del tutto usi nuovi e diversi dei dati, a condizione che ciò avvenga entro il parametro della compatibilità.

Il principio di finalità implica, innanzitutto, che i dati devono essere raccolti per finalità, specifiche, ossia sufficientemente definite per consentirne l'attuazione di tutte le necessarie garanzie di protezione dei dati e per delimitare l'ambito dell'operazione di trattamento. Prima del trattamento, il

---

[286] L'art. 5 Convenzione 108 prevede che i dati personali debbano essere "*registrati per fini determinati e legittimi e non devono essere utilizzati in modo incompatibile con tali fini*" (par. 1, lett. b) e la Dir. 95/46 ribadisce questo principio affermando che i dati devono essere "*rilevati per finalità determinate, esplicite e legittime, e successivamente trattati in modo non incompatibile con tali finalità. Il trattamento successivo dei dati per scopi storici, statistici o scientifici non è ritenuto incompatibile, purché gli Stati membri forniscano garanzie appropriate*".
Inoltre, l'art. 8, par. 2, Carta dir. UE, afferma che i dati personali devono essere "*trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge*".

[287] GRUPPO DI LAVORO ARTICOLO 29, *Opinion 03/2013 on purpose limitation*, 2.4.2013.

titolare deve determinare per quale scopo o finalità i dati personali verranno utilizzati; ciò comporta anche che non devono essere raccolti dati personali che non sono necessari o pertinenti rispetto alla finalità perseguita. La specificazione dello scopo è al centro della disciplina per la protezione dei dati: per poter determinare se il trattamento dei dati è conforme alla legge (e per stabilire l'ampiezza delle garanzie di protezione che dovrebbero essere applicate), è necessario identificare le finalità specifiche per le quali è effettuata la raccolta dei dati personali. L'individuazione della finalità richiede una valutazione interna e preventiva da parte del titolare del trattamento ed è condizione necessaria in un'ottica di *accountability* del titolare, in quanto è il primo passo che il titolare deve seguire per garantire il rispetto della normativa applicabile in materia di protezione dei dati (e per dimostrare di avervi adempiuto).

In secondo luogo, il principio di finalità (e di trasparenza) impone che le finalità stesse siano sufficientemente inequivocabili ed espresse chiaramente.

Le finalità della raccolta dei dati devono essere chiaramente rivelate ed espresse all'interessato, in forma intelligibile, senza vaghezza o ambiguità quanto al loro significato. Ciò che si intende deve essere chiaro e non deve lasciare dubbi o difficoltà di comprensione, all'Autorità di controllo e agli interessati. Il requisito che le finalità siano specificate "esplicitamente" contribuisce al rispetto del principio di trasparenza del trattamento, consentendo di individuare con evidenza i limiti entro cui il titolare del trattamento può effettuare l'attività e, conseguentemente, si riduce il rischio che le aspettative degli interessati differiscano dalle aspettative del titolare.

Infine, le finalità devono essere legittime, con ciò intendendosi non solo che deve sussistere una base giuridica valida, ma anche che il trattamento deve avere uno scopo lecito. Il requisito di legittimità sta, dunque, a significare che le finalità dell'operazione di trattamento devono essere "conformi al diritto" e ciò comporta che la legittimità di un determinato scopo può anche cambiare nel tempo, a seconda della scienza e sviluppi tecnologici, cambiamenti nella società e atteggiamenti culturali[288].

Il requisito della "non incompatibilità" delle finalità viene approfonditamente analizzato dal Gruppo di Lavoro Articolo 29, che individua i criteri che devono essere considerati per svolgere il "*compatibility assesment*":

- il rapporto tra le finalità per le quali i dati sono stati raccolti e la finalità dell'ulteriore trattamento;
- il contesto in cui i dati sono stati raccolti e le ragionevoli aspettative degli interessati sugli usi ulteriori degli stessi;
- la natura dei dati raccolti e l'impatto del loro utilizzo ulteriore sugli interessati;

[288] GRUPPO DI LAVORO ARTICOLO 29, *op. cit.*, p. 20.

- le misure adottate dal titolare per assicurare trattamenti ulteriori "leali" e prevenire impatti negativi di questi sugli interessati.

Nell'*Opinion* il Gruppo di Lavoro Articolo 29 richiama, inoltre, l'attenzione su alcune delle sfide nell'applicazione del test di compatibilità ai *big data* e agli *open data*[289], in quanto "*here, perhaps even more so than elsewhere, there is a need for a rigorous but balanced and flexible application of the compatibility test to ensure it can be applied in our modern, networked society*", con ciò dimostrando la necessità di consentire, pur all'interno di specifici limiti, usi ulteriori dei dati già raccolti.

17. Il principio della qualità dei dati

Le lett. c), d), e), dell'art. 5 GDPR pongono tre principi ulteriori.

- principio di minimizzazione, secondo cui i dati sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
- principio di esattezza, secondo cui i dati sono esatti e, se necessario, aggiornati;
- principio di limitazione della conservazione, secondo cui i dati sono 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.

Secondo dottrina autorevole[290], le suddette prescrizioni sono, in realtà, tre profili distinti dell'unico principio della necessaria "qualità" dei dati.

Infatti, tali disposizioni descrivono caratteristiche intrinseche che i dati devono possedere affinché il loro trattamento possa considerarsi legittimo.

La necessaria adeguatezza, pertinenza e limitazione è strettamente correlata al principio di finalità dei dati: solo individuando correttamente lo scopo del trattamento, è possibile verificare se i dati che sono stati raccolti sono sufficienti e non eccedenti. Questa analisi, peraltro, incontra talune difficoltà quando, nel medesimo contesto, viene raccolto un ampio numero di dati per soddisfare differenti finalità: può, infatti, essere possibile che non tutti i dati siano pertinenti e adeguati rispetto a talune finalità di un medesimo trattamento; o, più ancora, il medesimo dato potrebbe essere adeguato o pertinente per talune finalità che riguardano un trattamento, ma eccedente rispetto alle finalità di un diverso trattamento. In ogni caso, il principio di trasparenza impone una chiara informativa (v. *supra*) sulla finalità di ciascun dato e sulla sua pertinenza rispetto a ciascun trattamento.

Anche l'esattezza dei dati e il termine di conservazione devono essere valutati in relazione alla finalità per cui gli stessi sono stati raccolti.

---

[289] Ai quali viene dedicata una specifica analisi nell'allegato 2 dell'*Opinion*.

[290] F. PIZZETTI, *op. cit.*

La lett. d) impone al titolare anche di cancellare o rettificare tempestivamente i dati inesatti, adottando "*tutte le misure ragionevoli*" per garantire l'esattezza degli stessi. Si tratta di un preciso obbligo di *accountability* del titolare, che può essere chiamato a dimostrare di aver approntato specifiche misure per monitorare e verificare l'eventuale inesattezza dei dati raccolti.

Allo stesso modo, il titolare deve adottare misure che monitorino l'utilità dei dati: una volta raggiunta la finalità per cui sono stati raccolti – salvo che non ricorrano le ulteriori ragioni precisate dalla lett. e)[291] – i dati personali perdono una loro qualità (l'essere "necessari") e devono essere cancellati dal titolare, oppure anonimizzati. Il titolare può infatti adottare tecniche di anonimizzazione dei dati, per non rendere più identificabili gli interessati, così che i dati perdono la loro qualifica di dati "personali" e possono essere utilizzati nuovamente dal titolare, ad esempio a fini statistici.

18. Il principio di *accountability*

La grande novità del GDPR consiste nell'avere introdotto il principio di *accountability*, la cui inosservanza è il presupposto principale della responsabilità per illecito trattamento di dati personali. Tale principio impone al titolare stesso di individuare e prevenire i rischi connessi ad uno specifico trattamento: è una prospettiva che segna un mutamento profondo nella disciplina per la protezione dei dati. Ed infatti, l'introduzione dell'*accountability* conferisce anche un nuovo contenuto a quei principi – ad es. di liceità, correttezza, trasparenza – che già erano espressi dalla previgente disciplina e che appaiono semplicemente riaffermati, con le medesime formulazioni linguistiche, dal GDPR[292].

Come osservato da autorevole dottrina, il principio di *accountability* è "*il nucleo della riforma europea e realizza un nuovo sistema normativo nel trattamento dei dati personali e nella protezione dei diritti della persona. Il principio di accountability comporta un cambio di paradigma e, anche nel caso in cui la lettera della norma resti invariata, richiede l'adozione di un metodo radicalmente diverso*"[293].

Gettando uno sguardo al sistema previgente, si osserva che nel Codice privacy si imponevano prescrizioni specifiche e di dettaglio a cui il titolare doveva ottemperare affinché il trattamento potesse considerarsi legittimo: ad esempio, l'all. B del d.lgs. n. 196/2003, intitolato "*Disciplinare tecnico in materia di misure minime di sicurezza*", imponeva al titolare di dotarsi di una serie di

---

[291] I dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, par. 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato.

[292] Sul tema si v., in ambito transazione, il contributo di V. MAYER-SCHÖNBERGER-Y. PADOVA, *Regime change? Enabling big data through Europe's new data protection regulation* in *The Columbia Science & technology law review*, 2016, Vol. XVII, pp. 315-335.

[293] G. FINOCCHIARO, *Il principio di accountability*, op. cit., pp. 2777 ss.

misure di sicurezza definitive "minime", la cui adozione era di per sé sufficiente, in determinate ipotesi, per escludere la responsabilità penale del titolare del trattamento. Ma questo modello, basato sull'imposizione di prescrizioni specifiche, era inadeguato a far fronte alle molteplici nuove sfide della tutela dei dati, che affiorano per il continuo evolversi delle nuove tecnologie, in quanto non consentiva adattamenti ai diversi casi concreti.

Invece, l'art. 32 GDPR impone al titolare di effettuare valutazioni variabili, a seconda dei casi concreti, per determinare le misure più adeguate e proporzionate, senza che queste siano predeterminate dalla legge: questa disposizione è chiara affermazione del principio di *accountability* e della nuova prospettiva da cui il legislatore europeo affronta il tema della protezione dei dati personali. Peraltro, il principio di *accountability* è strettamente correlato al concetto di gestione del rischio *privacy*, approccio che caratterizza l'intera disciplina per la protezione dei dati personali e che impone al titolare di eseguire valutazioni preventive per l'individuazione dei rischi che possono derivare dalle attività di trattamento, al fine di individuare le misure più adeguate per eliminare i rischi medesimi.

Questo principio verrà analizzato più specificamente nel capitolo 3, perché è proprio attraverso l'adempimento di tale obbligo che il titolare può andare esente da responsabilità, dimostrando che l'evento dannoso *non gli è in alcun modo imputabile*.

Il titolare dovrà, dunque, dare la prova di aver predisposto tutte le misure adeguate per prevenire e gestire i rischi da trattamenti illeciti, con ciò dimostrando che il rischio che si è realizzato era atipico e non prevedibile.

Con la conseguenza che l'introduzione della responsabilizzazione connota la stessa responsabilità ex art. 82 GDPR come una responsabilità d'impresa, relativa all'assetto organizzativo della stessa che deve essere predisposto in un'ottica di gestione e prevenzione dei rischi.

19. Riflessioni conclusive

Dall'analisi dei principi sulle modalità del trattamento emerge dunque il cambio totale di prospettiva della nuova disciplina.

Quelli che nella direttiva erano diritti dell'interessato, nel regolamento vengono valorizzati quali doveri del titolare: la disciplina non ruota più attorno al controllo sui dati da parte delle persone, ma piuttosto riconosce la centralità della figura del titolare e dei soggetti che prendono parte all'esecuzione del trattamento e attorno a questi soggetti costruisce un impianto ben delineato di obblighi e vincoli.

Il GDPR riconosce la necessità di responsabilizzare il titolare perché nel trattamento dei dati vi è insito un valore anche "sociale" e non solo un valore individuale per il soggetto a cui si riferiscono,

in quanto la società esige che i trattamenti siano eseguiti da un titolare responsabilizzato. Per tale ragione l'inadempimento all'obbligo di *accountability* comporta prima di tutto la possibilità per l'Autorità di controllo di irrogare la sanzione amministrativa e, solo in un secondo momento, diviene presupposto per il riconoscimento del danno di cui all'art. 82 GDPR. Tuttavia, il modello di *accountability* deve essere ulteriormente implementato, integrando maggiori obblighi di trasparenza e di controllo, ed imponendo di tenere in considerazione anche rischi sociali e collettivi e non esclusivamente individuali.

La responsabilità civile è dunque complementare ad un sistema di tutela più ampio dei dati personali e, infatti, la dottrina ha evidenziato il carattere anche "*sostanzialmente pubblicistico*" della responsabilità del titolare, come emerge con chiarezza dalla disciplina delle violazioni di dati personali, che prevede come obbligatoria la notifica all'Autorità di controllo, mentre come eventuale la comunicazione agli interessati[294].

[294] F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali*, cit., p. 282.

Capitolo IV

NATURA E DISCIPLINA DELLA RESPONSABILITÀ DA ILLECITO TRATTAMENTO DEI DATI PERSONALI

SOMMARIO: 1. Natura della responsabilità per illecito trattamento. - 2. Il trattamento illecito. - 3. La prova liberatoria: la gestione del rischio privacy. - 4. Il principio di responsabilizzazione. - 4.1. *Contrattualizzazione dei rapporti tra i "soggetti del trattamento".* - 4.2. *La solidarietà nel risarcimento dei danni.* - 5. Gestione del rischio privacy e accountability. - 6. La gestione del rischio nel GDPR. - 6.1. *Mappatura dei processi.* - 6.2. *Valutazione d'impatto: contenuto, finalità, modalità esecutive.* - 6.3. *(segue) Alcune osservazioni sulla valutazione d'impatto*. - 6.4. *Violazione di sicurezza.* - 7. Integrazione della gestione del rischio privacy nell'organizzazione. - 8. *Duty of care* e prova liberatoria negli altri Stati UE. - 9. Il danno materiale e immateriale. - 10. Art. 82 e filtro di risarcibilità. - 10.1. *La gravità della lesione.* - 10.2. *La serietà del danno.* - 11. Osservazioni critiche al doppio filtro di ammissibilità: prospettive ermeneutiche verso l'oggettivizzazione del danno. - 12. Onere della prova e quantificazione del danno non patrimoniale. - 13. I danni risarcibili negli altri Stati UE.

1. Natura della responsabilità per illecito trattamento

L'art. 82 GDPR afferma che "*chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento*".

La natura della responsabilità per illecito trattamento dei dati personali è questione dibattuta in dottrina sin dalla l. 31.12.1996, n. 675; successivamente, il contrasto si è spostato sull'analisi della disciplina prevista nel d.lgs. 39.6.2003, n. 196[295].

[295] Sul tema della responsabilità per illecito trattamento dei dati personali la dottrina è molto ampia; si v., tra gli altri: G. M. RICCIO-G. SCORZA-E. BELISARIO, *GDPR e Normativa Privacy*. *Commentato*, Ipsoa, 2018, pp. 596 ss.; M. RATTI, *La responsabilità da illecito trattamento dei dati personali nel nuovo Regolamento,* in *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, a cura di G. FINOCCHIARO, Zanichelli, 2019, pp. 615 ss.; G. BUTTARELLI, *Banche dati e tutela della riservatezza*, op. cit.; G. ALPA, *La disciplina dei dati personali*. *Note esegetiche sulla Legge 31 dicembre 1996, n. 675 e successive modifiche*, op. cit., 1998; E. GIANNANTONIO- M. G. LOSANO-V. ZENO-ZENCOVICH, *La tutela dei dati personali. Commentario alla L. 675/1996*, Cedam, 1999; V. CUFFARO-V. RICCIUTO, *Il trattamento dei dati personali*, Giappichelli, 1999; A. SCALISI, *Il diritto alla riservatezza*, Giuffrè, 2002; E. PELLECCHIA, *La responsabilità civile per trattamento dei dati personali*, in *Resp. civ. e prev*., 2005, pp. 232 ss.; R. PARDOLESI, *Diritto alla riservatezza e circolazione dei dati personali*, Giuffrè, 2003; R. PANETTA, *Libera circolazione e protezione dei dati personali*, Giuffrè, 2006; V. CUFFARO-R. D'ORAZIO-V. RICCIUTO, *Il codice del Trattamento dei dati personali*, Giappichelli, 2007; C. BIANCA-M. BUSNELLI, *La protezione dei dati personali*, Cedam, 2007; G. FINOCCHIARO, *Privacy*

Il dibattito sulla natura della responsabilità involge temi quali il contenuto della prova liberatoria, la quantificazione del danno non patrimoniale, l'applicabilità della soglia di risarcibilità ai danni conseguenti al trattamento illecito.

Va considerato che il GDPR si applica direttamente all'interno degli Stati europei: di conseguenza, in futuro i tribunali italiani dovranno fare riferimento al regolamento e tenere conto della giurisprudenza della Corte di giustizia UE sul tema del trattamento dei dati. Tale opera interpretativa riempirà di significato anche quei concetti elastici oggi tanto dibattuti in giurisprudenza e dottrina.

Il GDPR individua un punto di equilibrio tra la necessità di proteggere i diritti fondamentali della persona relativi ai dati personali e l'esigenza di consentire, comunque, la circolazione di tali beni e lo sviluppo delle tecnologie che ne fanno un utilizzo massiccio. Essenziale, dunque, ponderare i rischi che derivano ai soggetti da tali attività d'impresa, considerando che l'utilizzo illegittimo dei dati personali può ledere diversi interessi dell'individuo[296].

Il GDPR dispone espressamente che il risarcimento del danno è dovuto a seguito di una qualsiasi "*violazione del presente regolamento*", con ciò distinguendosi dall'ormai abrogato art. 15 cod. privacy che, in tema di responsabilità per illecito trattamento, richiamava l'applicazione dell'art. 2050 c.c.[297]. Diversamente, oggi, viene richiamata la contrarietà della condotta a qualsiasi obbligo del Regolamento, con il chiaro obbiettivo di estendere il più possibile l'efficacia, anche deterrente, del modello di responsabilità civile delineata dal GDPR.

---

e protezione dei dati personali. Disciplina e strumenti operativi, Zanichelli, 2012; G. M. RICCIO, *Diritto all'oblio e responsabilità dei motori di ricerca*, in *Dir. inform.*, 2014, pp. 753 ss.; F. DI CIOMMO , *Quello che il diritto non dice. Internet e oblio*, in *Danno e resp*., 2014, pp. 1101 ss.; G. RESTA-A. SALERNO, *La responsabilità civile per il trattamento dei dati personali*, in *La responsabilità d'impresa*, a cura di P. G. ALPA-G. CONTE, Giuffrè, 2015, p. 684; F. BRAVO, *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, Cedam, 2018; F. BRAVO, *Sul bilanciamento proporzionale dei diritti e delle libertà "fondamentali", tra mercato e persona: nuovi assetti dell'ordinamento europeo*?, in *Contr. e impr.*, 2018, pp. 190 ss.; S. SICA, *La libertà fragile. Pubblico e privato al tempo della rete*, Esi, 2014; P. PERLINGIERI, *Privacy digitale e protezione dei dati personali tra persona e mercato*, in *Foro Nap.,* 2018, pp. 481 ss.; S. THOBANI, *Il danno non patrimoniale da trattamento illecito dei dati personali*, in *Dir. inform*., 2017, pp. 427 ss.; F. BARRA CARACCIOLO, *La tutela della personalità in Internet*, in *Dir. inform*., 2018, pp. 201 ss.; P. MANES, *Il consenso al trattamento dei dati personali*, Cedam, 2001. Sulla responsabilità extracontrattuale in generale, si v.: G. ALPA, *La responsabilità del produttore*, Giuffrè, 2019; G. ALPA-M. BESSONE, *La responsabilità del produttore*, Giuffrè, 1999; F. D. BUSNELLI, voce "Illecito civile", in *Enciclopedia giuridica*, XV, Treccani, 1989, pp. 1 ss.; M. FRANZONI, *L'illecito*, nel *Trattato della Responsabilità civile*, Giuffrè, 2010, p. 941; P. TRIMARCHI, *Rischio e responsabilità oggettiva*, Giuffrè, 1961, p. 11; P. PERLINGIERI, *La responsabilità civile tra indennizzo e risarcimento*, in *Rass. dir. civ*., 2004, p. 1066; C. CASTRONOVO, *Responsabilità civile*, Giuffrè, 2018; E. LUCCHINI GUASTALLA, *Il nuovo regolamento europeo sul trattamento dei dati personali: i principi ispiratori*, op. cit., pp. 106 ss.; C. SALVI, *La responsabilità civile*, Giuffrè, 1998, pp. 110 ss.; G. ALPA-M. BESSONE, *I fatti illeciti*, in *Trattato di Diritto Privato*, diretto da P. RESCIGNO, XIV, Utet, 1982, pp. 295 ss.; C. M. BIANCA, *Diritto Civile, 5, La Responsabilità*, Giuffrè, pp. 575 ss.

[296] Non sembrano invece adeguatamente considerati dal GDPR i rischi collettivi, come quelli etici e sociali, derivanti in particolare dall'utilizzo dei *big data* e dell'intelligenza artificiale (su cui v. Cap. II).

[297] Il comma 1° dell'art. 15 così recitava: "*Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile*"

L'orientamento dominante della dottrina sviluppatosi attorno all'art. 15 cod. *privacy* qualificava la responsabilità da illecito trattamento dei dati personali come responsabilità di natura extracontrattuale[298] – sebbene con tratti di specialità rispetto alla disciplina generale di cui all'art. 2043 c.c. – assoggettandola, dunque, alla medesima disciplina[299].

Altra parte della dottrina ha evidenziato, invece, l'origine *ex lege* degli obblighi gravanti sui soggetti che effettuano il trattamento e ne ha delineato, pertanto, un'ipotesi di responsabilità da contatto sociale, da inadempimento di obbligazioni derivanti dalla legge[300].

2. Il trattamento illecito

L'art. 82, par. 1, descrive la condotta illecita che determina il risarcimento del danno nel modo più ampio possibile, riferendosi ad un'attività di trattamento eseguita in "*violazione del presente regolamento*", con ciò andando a comprendere anche gli atti delegati e gli atti di esecuzione adottati in conformità del Regolamento stesso, nonché le disposizioni adottate dagli Stati membri quali specificazioni delle norme regolamentari (come precisato nel Considerando n. 146).

La condotta rilevante non viene descritta nei suoi contenuti, optandosi, all'opposto, per un rinvio il più ampio possibile che ingloba in sé tutti gli obblighi previsti dalla disciplina per la protezione dei dati personali per l'attività del titolare.

Ad un'attività di trattamento di dati svolta in violazione di tali regole di condotta non potrà che conseguire l'insorgenza di una forma di responsabilità.

Quando un'attività di trattamento può dirsi (il)lecita?

Dovranno, innanzitutto, verificarsi i presupposti (ossia la base giuridica) del trattamento ex art. 6 (su cui v. Cap. precedente), nonché se esso sia stato posto in essere con modalità conformi ai principi del trattamento ex art. 5 (liceità, correttezza e trasparenza; limitazione della finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza).

Peraltro, è proprio per garantire il rispetto di tali principi che il legislatore ha stabilito la regola di cui

---

[298] In questo senso si v. G. RESTA-A. SALERNO, *La responsabilità civile per il trattamento dei dati personali*, cit., pp. 653 ss.; E. LUCCHINI GUASTALLA, *op. cit*., 2018, pp. 106 ss.; M. GAMBINI, *Principio di responsabilità e tutela aquiliana dei dati personali*, Esi, 2018; E. NAVARRETTA, *Commento all'art. 9*, in *Commentario alla L. 31 dicembre 1996, n. 675, Tutela della "privacy"*, a cura di C. M. BIANCA-F. D. BUSNELLI, cit., pp. 323 ss.; A. PINORI, *Internet e responsabilità civile per il trattamento dei dati personali*, in *Contr. e impr.*, 2007 pp. 1568 ss.

[299] In ambito europeo, si afferma che "*to hold a controller liable, the data subject must succeed in demonstrating three elements: namely (1) the performance of an "unlawful act" (i.e. an unlawful processing operation or other act incompatible with the national provisions adopted pursuant to the Directive); (2) the existence of damages; and (3) a causal relationship between the unlawful act and the damages incurred*" (B. VAN ALSENOY, *Liability under EU Data Protection Law. From Directive 95/46 to the General Data Protection Regulation*, JIPITEC, 2016, pp. 271-288).

[300] C. CASTRONOVO, *Situazioni soggettive e tutela nella legge sul trattamento delle informazioni personali*, in *Eur. e dir. priv*., 1998, I, pp. 677 ss. F. BRAVO, *Riflessioni critiche sulla natura della responsabilità da trattamento illecito dei dati personali*, in *Persona e mercato dei dati*, a cura di N. ZORZI-F. GALGANO, Giuffrè, 2019, pp. 383 ss.

all'art. 82, che chiude il sistema di protezione dei dati personali, conferendo efficacia deterrente all'intera disciplina.

In secondo luogo, la valutazione involgente l'osservanza di tali principi e delle specifiche regole di condotta andrà effettuata assumendo come parametro di valutazione, in particolare, il principio di *accountability.*

Il titolare (e ogni altro soggetto coinvolto nel trattamento) dovrà dimostrare il proprio atteggiamento prudente e responsabile nell'individuazione e gestione dei rischi legati al trattamento, dando evidenza di averli adeguatamente ponderati, eliminati o mitigati dotandosi di una struttura organizzativa che, a tutti i livelli, gestisce in modo efficace e *compliance* i dati personali trattati.

La stessa inosservanza di questo atteggiamento precauzionale, da parte del titolare, determina illiceità e ingiustizia del trattamento.

L'individuo affida i dati al titolare nella convinzione che quest'ultimo si comporti, in relazione agli stessi, secondo un'ottica di piena responsabilizzazione, tenendo costantemente conto dei rischi che possono derivare per i diritti e le libertà degli individui; per tale motivo, il GDPR sanziona la mancata assunzione di questo atteggiamento proattivo, finalizzato a custodire, gestire e trattare i dati in un'ottica prudenziale. Il titolare non deve far necessariamente prevalere il proprio interesse economico-individuale rispetto a quello degli interessati ed è responsabilizzato in tal senso: un comportamento difforme assume gli estremi della condotta illecita che può determinare danni risarcibili ex art. 82.

3. La prova liberatoria: la gestione del rischio *privacy*

L'art. 82 imputa automaticamente alla responsabilità del titolare i danni conseguenti al trattamento illecito, secondo una responsabilità di tipo "oggettivo" o, comunque, "aggravato".

Il par. 3 dell'art. 82 stabilisce il regime della "prova liberatoria" da responsabilità, prevedendo 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*".

Si tratta di una disposizione del tutto differente rispetto alla disciplina previgente, la quale, rinviando all'art. 2050 c.c., disponeva che la prova liberatoria per il titolare o il responsabile dovesse consistere nella dimostrazione "*di avere adottato tutte le misure idonee a evitare il danno*" (art. 2050 c.c.).

Tale rinvio, peraltro, aveva generato un dibattito sulla natura stessa dell'attività di trattamento dati personali: ci si chiedeva se tale attività fosse considerata "pericolosa" dal legislatore sotto ogni aspetto, oppure se il rinvio fosse teso semplicemente a richiamare la medesima disciplina prevista per le attività "pericolose".

Tale dibattito non comportava, comunque, particolari effetti applicativi ai fini della prova per

escludere l'imputazione della responsabilità.

Merita attenzione, piuttosto, il dibattito allora venutosi a creare attorno alla natura della responsabilità ex art. 2050 c.c.[301] che, conseguentemente, si rifletteva anche sulla ricostruzione della natura della responsabilità ex art. 15 cod. privacy.

In particolare, secondo un primo orientamento, la responsabilità ex art. 2050 c.c. e, dunque, quella per illecito trattamento di dati personali, doveva considerarsi come responsabilità di tipo oggettivo[302], con la conseguenza che il titolare (o il responsabile) del trattamento, per sottrarsi all'imputazione di tale responsabilità, era tenuto a dimostrare la forza maggiore o il caso fortuito, ossia una causa esterna atipica, al di fuori della sua sfera di controllo, che da sola si ponesse come evento dannoso idoneo a recidere il nesso di causa tra la condotta e il danno.

Un orientamento minoritario della dottrina – e, in questo senso, anche una parte della giurisprudenza[303] – qualificava tale responsabilità come per "colpa aggravata", sul presupposto che l'art. 2050 c.c. porrebbe un'inversione dell'onere della prova a favore del danneggiato obbligando, dunque, il danneggiante a dimostrare di aver adottato tutte le misure idonee a prevenire il danno. Tale ricostruzione si incentra sull'analisi del profilo soggettivo della colpa del titolare, al quale è richiesta la dimostrazione del massimo grado di diligenza pretendibile nella fattispecie concreta[304], nonché della predisposizione di misure e controlli finalizzati specificamente ad evitare l'evento dannoso[305].

---

[301] L'art. 2050 c.c. viene qualificato, dalla dottrina dominante, come un'ipotesi di responsabilità oggettiva; si v. in particolare G. ALPA-M. BESSONE, *La responsabilità del produttore*, cit.; M. FRANZONI, *Responsabilità per l'esercizio di attività pericolose*, in *La responsabilità civile*, II, 2, a cura di G. ALPA-M. BESSONE, Giappichelli, 1987, p. 462; P. TRIMARCHI*, Rischio e responsabilità oggettiva*, cit., p. 11.

[302] In questo senso G. RESTA-A. SALERNO, *op. cit.*, p. 670; M. FRANZONI, *Responsabilità derivante da trattamento dei dati personali*, in *Diritto dell'informatica*, a cura di G. FINOCCHIARO-F. DELFINI, Giuffrè, 2014, p. 831.

Il rinvio all'art. 2050 c.c. realizzerebbe, secondo altra parte della dottrina, una mera inversione dell'onere della prova in favore del danneggiato. Su questo punto, si v. inoltre E. PELLECCHIA, *op. cit.*, p. 221; V. COLONNA, *Il danno da lesione della privacy, in Danno e resp*., 1999, p. 18.

[303] Tra le sentenze della giurisprudenza di legittimità CASS., 14.5.2013, n. 11575, in *Guida al dir.,* 2013, pp. 33, 57; CASS., 17.12.2009, n. 26516, in *Mass. Giust. civ*., 2009, 12, p. 1704. Nella giurisprudenza di merito, si. v. APP. MILANO, 11.4.2017, n. 1519; TRIB. BARI, 23.7.2010, in *Resp. civ. prev*., 2010, p. 864; TRIB. TRENTO, 11.9.2015, n. 863; TRIB. PORDENONE, 16.4.2010, in *Danno e resp.*, 2011, p. 215.

[304] La Cassazione ha affermato che per vincere la presunzione di colpa posta a carico dell'esercente l'attività pericolosa, non rileva la semplice prova dell'imprevedibilità del danno, dovendosi, invece, dimostrare che esso non si sarebbe potuto evitare mediante l'adozione delle misure di prevenzione che le leggi dell'arte o la comune diligenza imponevano (CASS., 20.5.2016, n. 10422). Si v., inoltre, CASS., 5.2.2016, n. 2306, l'art. 15 cod. privacy "*prevede un'inversione dell'onere della prova a carico dell'autore del danno, tenuto a dimostrare di aver adottato tutte le misure idonee ad evitarlo. La presunzione iuris tantum riguarda, peraltro, l'elemento psicologico della colpa non certo, del fatto illecito, né del nesso eziologico tra fatto ed evento, che devono essere, invece, puntualmente provati dai danneggiati*". E si esprime in termini di responsabilità aggravata Cass., 25.1.2017, n. 1931, secondo cui "*erra il ricorrente nel porre l'accento sull'assunto secondo cui la responsabilità per attività pericolosa di cui all'art. 2050 c.c., alla luce della giurisprudenza di questa Corte, costituirebbe ipotesi di responsabilità oggettiva*".

[305] F. MACARIO, *La protezione dei dati personali nel diritto privato europeo*, in *Il trattamento dei dati personali*, a cura di V. CUFFARO-V. RICCIUTO, cit., pp. 48 ss., nt. 104 e 108.

Una diversa tesi intravede, invece, nell'art. 2050 c.c. un'ipotesi di responsabilità "da rischio", così intendendo che lo svolgimento di un certo tipo di attività, da considerarsi pericolosa, fa sorgere in capo al titolare che la pone in essere, e che da essa ricava un'utilità, la responsabilità per tutti i danni che da essa possano derivare a terzi.

Nella responsabilità da rischio l'imputazione si fonda su di un principio di solidarietà e di responsabilità sociale: nell'attuale società tecnologica è necessario consentire anche lo sviluppo di attività economiche ed imprenditoriali che possono generare danni a terzi, sicché devono anche ammettersi forme di responsabilità extracontrattuale che prescindono dalla colpa e che si fondano semplicemente su di un'allocazione ponderata dei rischi.

È il legislatore stesso che individua, dunque, il soggetto che subisce il rischio dei danni conseguenti a tali attività e, normalmente, esso viene individuato nel soggetto che trae beneficio e utilità dalla stessa.

Sulla scorta di tale tesi, tutte le ipotesi di responsabilità di cui agli artt. 2047 ss. c.c. si qualificherebbero, infatti, in quanto ipotesi in cui la responsabilità deriva dalla relazione che intercorre tra il soggetto individuato come responsabile e una particolare attività (come nell'art. 2050 c.c.), una cosa (artt. 2051, 2052, 2053, 2054 c.c..), una situazione (artt. 2047, 2048, 2049 c.c.). In questi casi, il legislatore ha ponderato e distribuito il rischio di tale relazione, il quale, in tema di danni conseguenti ad un trattamento illecito, viene imputato al soggetto titolare.

Infatti, come evidenziato, il GDPR dimostra di essere specificamente rivolto all'attività imprenditoriale ed economica e si sviluppa proprio come un modello di gestione dei rischi. Laddove questi rischi sfuggono al controllo del titolare e provochino danni a terzi, il principio di solidarietà sociale impone che tali danni vengano sopportati dal soggetto che trae beneficio/utilità dall'attività di trattamento dei dati e che la pone effettivamente in essere.

Nell'ambito di un trattamento dati, in virtù del principio di *accountability* il titolare è tenuto a considerare i rischi conseguenti a tale attività, risultando, in caso di inadempienza, responsabile per i danni che ne conseguono.

Trattasi, perciò, di una specifica ipotesi di responsabilità da rischio imprenditoriale, la cui prova liberatoria consiste nella dimostrazione di aver rispettato in concreto il principio di responsabilizzazione nell'esecuzione del trattamento. A tal proposito, il GDPR disciplina esclusivamente i trattamenti effettuati nell'esercizio dell'attività di impresa e professionale (intese in senso lato), tralasciando, invece, quei trattamenti effettuati da una persona fisica per esercizio di attività personali o domestiche. I principi di correttezza, trasparenza e liceità del trattamento devono informare di sé il contesto d'impresa e, alla luce della responsabilizzazione del titolare, indurre quest'ultimo a verificare con la massima diligenza i rischi correlati al trattamento, al fine di mitigarli.

In punto di responsabilità dell'imprenditore, la dottrina ha infatti affermato che "*la responsabilità dovrà essere attribuita a chi ha il controllo delle condizioni generali del rischio ed è in grado di tradurre il rischio in costo inserendolo armonicamente nel gioco dei profitti e delle perdite, con lo strumento dell'assicurazione o dell'autotassazione*"[306].

Se osserviamo la disciplina conformativa del GDPR, possiamo rilevare che le disposizioni rivolte al titolare possono essere raggruppate in due categorie: una costituita dalle disposizioni che prevedono un comportamento specifico a cui il titolare deve adeguarsi, un'altra, formata da tutti quei principi – tra cui quelli di responsabilizzazione – che non impongono uno specifico obbligo ma, piuttosto, indicano una finalità o uno scopo da perseguirsi nell'ambito di un'attività di trattamento.

Se con riferimento alla prima categoria può individuarsi un profilo di colpa certamente oggettivo per il titolare che abbia violato l'obbligo, con riferimento alla conformazione ai principi generali l'analisi è certamente più flessibile. In tale ultima ipotesi, dunque, la responsabilità si sposta verso un modello di "colpa aggravata" con inversione dell'onere della prova a carico del danneggiante. Secondo l'orientamento maggioritario, la verifica di tale profilo soggettivo della colpa dovrà fondarsi sul criterio della diligenza qualificata ex art. 1176 c.c.

Sul punto, tuttavia, va osservato che il parametro di cui all'art. 1176 c.c., all'interno della disciplina della protezione dei dati personali, risulta quasi assorbito dallo stesso criterio di responsabilizzazione. Quest'ultimo, infatti, permette di modellare il grado di diligenza e precauzione che deve essere osservato dal titolare in riferimento anche al settore specifico in cui viene esercitata l'attività, imponendo al contempo di tenere conto di tutte le altre circostanze del trattamento, tra cui i fattori di rischio nonché lo stato dell'arte della tecnica e dei costi di attuazione delle misure organizzative e di sicurezza.

4. Il principio di responsabilizzazione

Come precisato al capitolo 2, par. 15, il GDPR stabilisce un principio di responsabilizzazione del titolare: fissa gli obbiettivi e la finalità di tutela e impone al titolare del trattamento di raggiungerli, prevedendo che lo stesso valuti, di volta in volta, i rischi per i dati personali che possano derivare da una specifica attività di trattamento. Il titolare viene, in tal modo, responsabilizzato.

Il concetto di *accountability* deriva dal sistema anglosassone[307] (è tipico della disciplina dei mercati e

---

[306] P. TRIMARCHI, *La responsabilità civile: atti illeciti, rischio, danno*, Giuffrè, 2017, pp. 415 ss.; E. TOSI, *opp. citt*.

[307] Il termine inglese "*accountability*" (responsabilità) proviene dal mondo anglosassone, dove è di uso comune e dove il suo significato è ampiamente compreso e condiviso. Ciononostante, risulta complesso definire che cosa esattamente significhi "*accountability*" in pratica. In generale, comunque, l'accento è posto sulla dimostrazione di come viene esercitata la responsabilità e sulla sua verificabilità. Si veda GRUPPO DI LAVORO ARTICOLO 29, *Parere 3/2010 sul principio di responsabilità*, 13.7.2010.

sistemi finanziari) ed è un principio che mira ad evitare l'abuso nell'esercizio di un potere in un determinato settore.

È uno dei presidi necessari per garantire che, nell'ambito del mercato dei dati, i trattamenti siano effettuati in modo lecito, senza possibilità per gli attori coinvolti di abusare della propria posizione di controllo sui dati stessi: nel mondo anglosassone e dei mercati finanziari, l'*accountability* nasce come strumento che opera in sinergia con un esteso sistema di controlli e di supervisione da parte di autorità statali, nonché di vincoli e imperativi istituzionali[308].

L'*accountability* è un principio più ampio della responsabilità civile e, anzi, quest'ultima è solo uno degli strumenti residuali che concorrono a rendere la prima vincolante: la responsabilità civile, che consegue al trattamento illecito, unitamente all'obbligo di risarcire i danni causati agli interessati, si conforma come presidio di garanzia complementare al sistema di controllo (e sanzionatorio) affidato alle Autorità garanti nazionali.

In quest'ottica, un ruolo fondamentale dovrebbe essere assunto dai controlli istituzionali poiché, se correttamente svolti, potrebbero impedire il sorgere stesso della responsabilità civile. L'*accountability* rappresenta, dunque, una metodologia e una finalità.

Essa viene raggiunta attraverso tre fasi. In primo luogo, attraverso la predisposizione di limiti all'esercizio del potere di controllo del titolare, ossia il soggetto che deve raggiungere la finalità specifica. Nel contesto dei dati personali, si chiede al titolare di non pregiudicare i diritti e le libertà degli interessati. Può trattarsi di limiti esterni al titolare, dunque obblighi specifici di legge o stabiliti dall'Autorità di controllo che impongono al titolare di esercitare il proprio potere di controllo sui dati conformemente a determinati principi. Può trattarsi, all'opposto, di limiti interni ed auto-imposti, ovverosia la predisposizione da parte del titolare stesso di *policy* aziendali, linee guida interne, codici di condotta, adesione a sistemi di certificazione. Attraverso questi limiti, pertanto, l'ente impone alla sua stessa organizzazione di esercitare il potere secondo determinate modalità.

In secondo luogo, per porre in essere un efficiente sistema di tutela basato sull'*accountability*, è necessario che il titolare del trattamento eserciti un controllo sul modo in cui esercita il potere. Affinché il titolare possa "auto-controllarsi", deve dotarsi di una organizzazione adeguata e proporzionata per il raggiungimento dell'*accountability*. Il titolare dovrà formalizzare le procedure interne che implicano trattamento di dati, così da individuare e gestire i rischi *privacy*, minimizzandoli. Dovrà, in aggiunta, apprestare un'organizzazione di monitoraggio e controllo costante di questa stessa organizzazione nonché del rispetto delle procedure adottate.

---

[308] F. BILOTTA, *La responsabilità nel trattamento dei dati personali*, in *Circolazione e protezione dei dati personali, tra libertà e regole del mercato, Commentario al Regolamento UE n. 2016/679 (GDPR) e al novellato d.lgs. n. 196/2003 (Codice Privacy)*, a cura di R. PANETTA, Giuffrè, 2019, p. 460.

Da ultimo, i modelli di *accountability* prevedono che alla supervisione operata dal titolare stesso si affianchi il controllo istituzionale, attraverso il conferimento all'Autorità garante di poteri ispettivi e sanzionatori.

L'*accountability*, si ribadisce, non coincide con la responsabilità civile, essendo, invece, un presupposto della responsabilità: se tale obbligo è violato, il trattamento è considerato illecito e il titolare è tenuto al risarcimento dei danni conseguenti. Questa sorge laddove il titolare viene meno all'obbligo di predisporre, in modo trasparente e verificabile, tutte le misure tecniche, organizzative e giuridiche, atte a individuare, gestire ed eliminare i rischi per la sicurezza dei dati e per i diritti e le libertà degli interessati. Al titolare viene richiesto di assumere un ruolo proattivo nella predisposizione di tali misure e di considerare prudenzialmente tutti i rischi che, secondo le attuali conoscenze tecnologiche, potrebbero verificarsi.

L'introduzione del principio dell'*accountability*, dunque, rovescia completamente l'approccio del legislatore: si passa da un sistema fondato su istruzioni specifiche ad un impianto normativo che fissa le finalità di protezione di determinati diritti e responsabilizza, rispetto ad essi, il titolare del trattamento. Questi diviene il primo soggetto chiamato ad interessarsi della tutela di quei diritti fondamentali dell'uomo che la propria attività potrebbe pregiudicare. Tale responsabilizzazione consente di adeguare l'applicazione degli altri principi per il trattamento lecito, a seconda delle caratteristiche del titolare, nonché della natura del dato e delle modalità del trattamento che viene effettuato.

Il principio di *accountability* nell'ambito della protezione dei dati è stato oggetto di analisi da parte del Gruppo di Lavoro Articolo 29; nel parere n. 3/2010, adottato il 13.7.2010[309], viene descritto come meccanismo procedurale che opera su due piani, uno vincolante, l'altro volontario:

- il primo livello è costituito da un obbligo di base vincolante per tutti i responsabili del trattamento (con la possibilità, comunque, che siano previste, ad integrazione di questo, ulteriori disposizioni specifiche). Tale obbligo comprende due elementi: l'attuazione di misure e procedure di prevenzione e sicurezza, unitamente alla formalizzazione e

[309] Il principio dell'*accountability* è preso in esame anche nel Parere 7.7.2021 dell'EDBP, ove si evidenzia che "*Il GDPR, all'articolo 5, paragrafo 2, introduce esplicitamente il principio di responsabilità, il che significa che:*
I. il responsabile del trattamento è responsabile del rispetto dei principi di cui all'articolo 5, paragrafo 1 GDPR; e che
II. il titolare del trattamento è in grado di dimostrare il rispetto dei principi di cui all'articolo 5, paragrafo 1 GDPR".
Qui si evidenzia che l'obiettivo di incorporare il principio di responsabilità nel GDPR e renderlo un principio centrale era quello di sottolineare che i titolari del trattamento dei dati devono attuare misure appropriate ed efficaci, attuative dei principi sul trattamento descritti dal GDPR; inoltre, egli deve essere in grado di dimostrare, in ogni momento, che tali misure sono effettivamente conformi al GDPR. Tali misure devono essere riviste e aggiornate se necessario. Il principio di responsabilità si riflette anche nell'articolo 28, che stabilisce gli obblighi del titolare del trattamento in caso di assunzione di un responsabile del trattamento.

conservazione delle prove documentali di averle adottate;

- il secondo livello include sistemi di responsabilità di natura volontaria che eccedono il livello minimo previsto dalle norme di legge. In forza dei principi fondamentali propri del campo della protezione dei dati, è possibile apprestare garanzie più elevate di quelle prescritte dalla normativa vigente, oppure prevedere volontariamente modalità di attuazione delle misure e garanzie d'efficacia più protettive rispetto al livello minimo legale stabilito

L'*accountability* ha, infatti, lo scopo di "*promuovere l'adozione di misure concrete e pratiche, in quanto trasformerebbe i principi generali della protezione dei dati in politiche e procedure concrete definite al livello del responsabile del trattamento, nel rispetto delle leggi e dei regolamenti applicabili. Il responsabile del trattamento dovrebbe anche garantire l'efficacia delle misure adottate e dimostrare, su richiesta, di aver intrapreso tali azioni*"[310].

Il principio di responsabilizzazione si compone di due aspetti: a) la necessità che il titolare del trattamento adotti misure appropriate ed efficaci per attuare i principi di protezione dei dati; b) la necessità di dimostrare, su richiesta, che sono state adottate misure appropriate ed efficaci.

Il principio dell'*accountability* permea l'intera nuova disciplina e, lungi dall'essere sintetizzato in un'unica disposizione del GDPR, viene contemplato dai Considerando introduttivi, come da diverse previsioni.

L'*accountability* è descritta dal Considerando n. 74, secondo cui "*è opportuno stabilire la responsabilità generale del titolare del trattamento per qualsiasi trattamento di dati personali che quest'ultimo abbia effettuato direttamente o che altri abbiano effettuato per suo conto. In particolare, il titolare del trattamento dovrebbe essere tenuto a mettere in atto misure adeguate ed efficaci ed essere in grado di dimostrare la conformità delle attività di trattamento con il presente regolamento, compresa l'efficacia delle misure*".

Il Considerando n. 78, inoltre, afferma che la tutela dei diritti e delle libertà degli interessati del trattamento dei dati "*richiede l'adozione di misure tecniche e organizzative adeguate per garantire il rispetto delle disposizioni del presente regolamento*"; si fa preciso riferimento al tema della *privacy by design* e *by default*, temi strettamente correlati con la responsabilizzazione, affermando che "*al fine di poter dimostrare la conformità con il presente regolamento, il titolare del trattamento dovrebbe adottare politiche interne e attuare misure che soddisfino in particolare i principi della protezione dei dati fin dalla progettazione e della protezione dei dati di default*"[311].

---

[310] GRUPPO DI LAVORO ARTICOLO 29, *op. cit.*, par. 27.

[311] Il medesimo considerando detta, infine, prescrizioni specifiche sulle misure di sicurezza da adottare nell'ambito della *privacy by design* e *by default*, prevedendo che "*tali misure potrebbero consistere, tra l'altro, nel ridurre al minimo il*

Dal Considerando n. 84 emerge, ancora, la connessione tra *accountability* e gestione del rischio per la sicurezza del trattamento: il titolare è tenuto a verificare i potenziali rischi e a prevenirli e, qualora dagli stessi possa derivare un rischio elevato per i diritti e le libertà delle persone fisiche, a svolgere una valutazione d'impatto preventiva sulla protezione dei dati personali "*per determinare, in particolare, l'origine, la natura, la particolarità e la gravità di tale rischio*".

Il Considerando n. 82 si dedica specificamente al secondo aspetto dell'*accountability*, ossia la "dimostrazione" di aver adempiuto agli obblighi del GDPR: esso prevede che "*per dimostrare che si conforma al presente regolamento, il titolare del trattamento o il responsabile del trattamento dovrebbe tenere un registro delle attività di trattamento effettuate sotto la sua responsabilità*". Il registro delle attività di trattamento è strumento fondamentale per individuare e tracciare tutti i trattamenti di dati personali eseguiti all'interno della propria organizzazione: la sua regolare tenuta dimostra l'attenzione (in questo senso la "responsabilizzazione") prestata dal titolare al fine di garantire trattamenti conformi al GDPR.

A livello prescrittivo, le disposizioni del GDPR che esprimono il principio dell'*accountability* sono molteplici e dal loro combinato disposto emerge il generale obbligo per il titolare di tutelare, egli stesso, i dati personali di cui ha il controllo.

Referente normativo cardine è rappresentato dall'art. 24, secondo il quale, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, "*il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento*".

L'art. 5, dopo aver elencato al primo paragrafo i principi relativi al trattamento dei dati, prevede, al par. 2, che "*il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo*". Tale disposizione dall'un lato imputa al titolare la responsabilità di attivarsi e organizzarsi per impedire violazioni alla sicurezza dei dati, dall'altro lato esprime il profilo "probatorio" dell'*accountability.*

Espressione ulteriore del principio di *accountability* è rappresentata dalla disposizione di cui all'art.

---

trattamento dei dati personali, pseudonimizzare i dati personali il più presto possibile, offrire trasparenza per quanto riguarda le funzioni e il trattamento di dati personali, consentire all'interessato di controllare il trattamento dei dati e consentire al titolare del trattamento di creare e migliorare caratteristiche di sicurezza. In fase di sviluppo, progettazione, selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati personali o che trattano dati personali per svolgere le loro funzioni, i produttori dei prodotti, dei servizi e delle applicazioni dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati allorché sviluppano e progettano tali prodotti, servizi e applicazioni e, tenuto debito conto dello stato dell'arte, a far sì che i titolari del trattamento e i responsabili del trattamento possano adempiere ai loro obblighi di protezione dei dati".

33, par. 1, secondo cui è il titolare a dover valutare se la violazione dei dati costituisca un rischio per i diritti e le libertà delle persone fisiche, al fine di verificare se risulti necessario notificare tale violazione di sicurezza all'Autorità garante.

In via generale, alla "responsabilizzazione" concorrono poi tutte quelle disposizioni che lasciano al titolare il compito di eseguire una valutazione, un contemperamento di interessi, da effettuare con proporzionalità, senza perseguimento di propri interessi individuali, ma, all'opposto, preservando e bilanciando diritti e libertà degli utenti.

Risulta evidente, dunque, il totale mutamento di prospettiva rispetto al sistema previgente, basato sull'imposizione di specifici obblighi. Tale cambio di rotta dev'essere considerato anche nell'interpretazione di quei principi e di quelle regole che appaiono confluiti nel GDPR dalla precedente disciplina, con formulazioni letterali spesso simili, ma che ora acquisiscono nuovi significati.

Così è, ad esempio, per il sistema dell'informativa (artt. 13 e 14) e del consenso dell'interessato (art. 7), che ad un primo approccio appaiono semplicemente traslati dal Codice *privacy* al GDPR, il quale li definisce pure in modo sostanzialmente analogo.

Tuttavia, a ben vedere, se prima il titolare era chiamato all'obbligo specifico di documentare "per iscritto" di aver rilasciato l'informativa e di aver ottenuto il libero consenso dell'interessato, nel sistema attuale è il titolare che valuta quali sono le modalità più adeguate per raccogliere il consenso e per rendere informato l'interessato. In particolare, il titolare dovrà verificare di aver reso l'informazione in modo trasparente e corretto, nonché di aver assicurato all'interessato la possibilità di esercitare i diritti derivanti dal GDPR, come, ad esempio, la possibilità di opporsi al trattamento.

Se, dunque, tale valutazione e bilanciamento viene rimesso al titolare, quest'ultimo deve, al contempo, essere pronto ad una dimostrazione postuma sulla proporzionalità e ragionevolezza delle soluzioni adottate.

Nel Codice della *privacy,* il consenso dell'interessato costituiva la base giuridica principale per rendere il trattamento lecito: la disciplina si fondava sul principio di autodeterminazione degli interessati e sul presupposto – probabilmente non del tutto fondato – che gli utenti avessero il pieno controllo dei propri dati e fossero perfettamente in grado di valutare autonomamente i rischi conseguenti all'autorizzazione al trattamento dei propri dati personali.

Il sistema attuale prende atto dell'inadeguatezza di questa impostazione, alla luce della rapida evoluzione delle tecnologie esistenti: se gli utenti non possono individuare e quantificare autonomamente i rischi derivanti dal trattamento, tale valutazione deve essere eseguita "a monte" da parte soggetto che conosce perfettamente la tecnologia impiegata e le modalità di trattamento dei dati che tale tecnologia comporta, ossia il titolare.

Per questo motivo, l'attuale sistema rimette al titolare stesso l'individuazione della base giuridica del trattamento e, soprattutto, il bilanciamento tra il proprio legittimo interesse e quello degli interessati. L'art. 6, par. 1, lett. f), infatti, consente al titolare di effettuare il trattamento senza il consenso dell'interessato qualora, da una ponderazione effettuata dal titolare stesso, risulti prevalente il proprio legittimo interesse al trattamento rispetto agli interessi, ai diritti e alle libertà delle persone fisiche.

4.1. Contrattualizzazione dei rapporti tra i "soggetti del trattamento"

A presidio della liceità del trattamento, il GDPR prevede obbligatoriamente la formalizzazione dei rapporti contrattuali che si instaurano tra i soggetti che effettuano il trattamento, ossia titolare, contitolari, responsabili, sub-responsabili.

Stipulando specifici accordi con i soggetti che effettuano parti dell'attività di trattamento, il titolare adempie, al contempo, all'obbligo di *accountability*: egli è tenuto a conformare il contenuto contrattuale in modo che il responsabile tratti i dati personali con modalità adeguate, nel rispetto dei principi del Regolamento, nonché adottando tutte le misure di sicurezza necessarie.

Il titolare deve assicurarsi, inoltre, che il responsabile (e gli ulteriori soggetti coinvolti) adotti un corretto approccio della gestione del rischio per i diritti e le libertà degli interessati.

Per tale ragione, la contrattualizzazione dei rapporti è essa stessa una misura di sicurezza, di tipo giuridico, e come tale deve essere considerata dal titolare.

Analizzando la dinamica dei rapporti strutturata dal Regolamento, risulta un modello di gestione del trattamento in cui il titolare riveste una posizione apicale e assume compiti di natura gestoria nonché di controllo nei confronti del responsabile: a quest'ultimo, infatti, incarica di realizzare parti dell'attività, ovverosia singole e specifiche operazioni di trattamento che, in tal modo, vengono esternalizzate.

Questa struttura essenzialmente verticistica può ampliarsi nel caso in cui siano presenti anche un contitolare e un sub-responsabile: tuttavia, anche in tali ipotesi, la struttura delineata dal GDPR si fonda sul presupposto che il titolare mantenga costantemente un potere di controllo effettivo sull'attività trattamento nel suo complesso.

Si tratta di una prospettiva che nasce negli anni '70, inizialmente nel settore pubblico per poi diffondersi anche nel settore privato: la concentrazione delle tecnologie e del controllo dei dati nella disponibilità di una cerchia limitata di soggetti comportava, infatti, che generalmente il titolare effettuava per conto proprio l'intero trattamento e ricorreva in modo assai limitato all'esternalizzazione di parti del trattamento. Tale prospettiva, tuttavia, ben presto si scontra con la nuova realtà del mercato unico digitale: vengono a diffondersi modelli "reticolari" di gestione che prevedono la suddivisione del trattamento in sotto-operazioni, delegate ad una pluralità di

responsabili del trattamento che, a loro volta, ricorrono a sub-responsabili in tal modo frazionando ulteriormente la parte di attività di trattamento che sono chiamati ad effettuare.

Tale modalità di gestione del trattamento si è resa necessaria al fine di "stare al passo" con lo sviluppo tecnologico: il titolare si trova, sovente, nella condizione di dover necessariamente esternalizzare parti del trattamento, anche nei confronti di molteplici responsabili. Si tratta di una modalità quasi "obbligata" per il titolare, il quale, per non pregiudicare il proprio servizio, deve affidarsi a soggetti ulteriori (i responsabili, per l'appunto), dotati di competenza estremamente specializzata.

Si assiste, così, ad una sorta di scissione tra titolarità "formale" e titolarità "sostanziale" del trattamento: il titolare definisce le finalità del trattamento, ma solo in via approssimativa determina le modalità dello stesso, che, in concreto e nel dettaglio, vengono determinate da uno o più responsabili.

Questa criticità può essere osservata nei servizi di *cloud computing*[312], in cui viene lasciata ampia libertà al fornitore del servizio di scegliere le modalità di conservazione dei dati e le misure tecniche e organizzative di sicurezza da adottare[313]. In questo caso, il titolare del trattamento può solo decidere a quale fornitore rivolgersi, ma non ha alcun effettivo potere di verifica e controllo sul trattamento e, soprattutto, non ha un vero potere contrattuale per negoziare il contenuto dell'accordo con il fornitore, che nella quasi totalità dei casi è un contratto imposto dal fornitore stesso[314].

Sul punto, il Gruppo di Lavoro Articolo 29 osservava che "*nell'attuale scenario del cloud computing, i clienti di servizi di cloud computing potrebbero non avere margine di manovra nel negoziare i termini contrattuali dell'uso dei servizi cloud, che in molti casi sono caratterizzati da offerte standardizzate*"[315], che in considerazione della "…*posizione giuridica asimmetrica degli interessati*

---

[312] Il *cloud computing* consiste in una serie di tecnologie e modelli di servizio incentrati sull'uso e sulla fornitura di applicazioni informatiche, capacità di elaborazione e archiviazione e spazio di memoria basati su Internet. Il *cloud computing* può produrre importanti vantaggi economici, poiché su Internet è possibile configurare, espandere e accedere a risorse su richiesta con molta facilità. Oltre ai vantaggi economici, il *cloud computing* può anche offrire vantaggi in termini di sicurezza; le imprese, in particolare piccole e medie, possono acquistare ad un costo marginale tecnologie avanzate che altrimenti non sarebbero alla loro portata.

I servizi offerti dai fornitori di soluzioni di *cloud computing* sono molto diversificati e spaziano da sistemi elaborativi virtuali (che sostituiscono o si affiancano ai tradizionali server controllati direttamente dal responsabile del trattamento dei dati) a servizi di supporto allo sviluppo e per l'*hosting* evoluto delle applicazioni, sino a soluzioni *software* rese disponibili in modalità *web* che sono sostitutive delle tradizionali applicazioni installate sui computer degli utenti finali, quali ad esempio applicazioni per l'elaborazione dei testi, per la gestione di agende e calendari, cartelle per l'archiviazione dei documenti *on-line* e soluzioni esternalizzate di posta elettronica (definizione tratta da GRUPPO DI LAVORO ARTICOLO 29, *Parere 05/2012 - WP 196 sul cloud computing*, 1.7.2012).

[313] Sul tema si v. K. LINCKE-A. NOURBAKHSH*, An Analysis of the GDPR's Effects on the Future of Cloud Outsourcing. Winds of regulatory change threaten the ubiquity of the cloud,* in *Computer Law Review International*, 2017, pp. 179-184.

[314] A. MANTELERO, *op. cit.*

[315] GRUPPO DI LAVORO ARTICOLO 29, *op. cit.*

e degli utenti piccole imprese nei confronti dei grandi fornitori di servizi di cloud computing", raccomandava "…*un ruolo più proattivo delle organizzazioni di consumatori e imprese per negoziare termini e condizioni generali più equilibrati*"[316].

Il potere di controllo sul dato da parte del titolare si esaurisce nella possibilità di scegliere se esternalizzare una parte del trattamento e nell'individuazione del responsabile a cui delegare l'attività da svolgere. Ma nella larga parte dei casi il titolare non ha il potere di verificare le modalità organizzative attraverso cui il responsabile esegue l'attività, in particolare se risultano adeguate le misure di sicurezza e prevenzione messe in atto dal responsabile. Per di più, risulta in concreto difficile, se non impossibile, coinvolgere il responsabile nelle ipotesi in cui si verifichi un *data breach* o in cui l'interessato eserciti i propri diritti nei confronti del titolare, poiché quest'ultimo (sovente un'azienda di dimensioni e struttura enormemente più piccole del responsabile) non è dotato di strumenti giuridici efficaci per obbligare il responsabile a collaborare.

Il GDPR risolve solo in parte il problema, laddove, all'art. 28, prevede la necessaria "contrattualizzazione" del rapporto tra titolare e responsabile (e tra co-titolari e tra responsabile e sub-responsabile), fissando anche il contenuto minimo dell'accordo stesso. A ben vedere, però, tale soluzione non è soddisfacente né risolutiva, risultando spesso meramente formale: nella sostanza, si ribadisce, al titolare residua solo il potere di controllo sul patrimonio informativo del dato e sulla scelta di delegare parte dell'attività, non anche la possibilità di esercitare un reale potere di controllo sul trattamento[317].

4.2. La solidarietà nel risarcimento dei danni

Nell'ottica di proteggere il danneggiato e agevolare l'effettivo risarcimento del danno, l'art. 82, par. 4, pone una regola di solidarietà nella responsabilità tra tutti i soggetti coinvolti nel trattamento illecito, disponendo che "*qualora più titolari del trattamento o responsabili del trattamento oppure*

---

[316] Si veda sul punto anche l'esempio contenuto in EDPB, *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*, 7.7.2021: "*Un grande provider di cloud storage offre ai propri clienti la possibilità di archiviare grandi volumi di dati personali. Il servizio è completamente standardizzato, con i clienti che hanno poca o nessuna possibilità di personalizzare il servizio. I termini del contratto sono determinati e redatti unilateralmente dal servizio cloud fornitore, fornito al cliente su base "prendere o lasciare". La società X decide di avvalersi del provider cloud per memorizzare i dati personali relativi ai propri clienti. La società X sarà ancora presa in considerazione un titolare del trattamento, data la sua decisione di avvalersi di questo particolare fornitore di servizi cloud per elaborare dati personali per le sue finalità. Nella misura in cui il fornitore di servizi cloud non elabora i dati personali per i propri scopi e memorizza i dati esclusivamente per conto dei propri clienti e in conformità con istruzioni, il fornitore di servizi sarà considerato un responsabile del trattamento*".

[317] Per tali ragioni, è stato osservato che "*alla luce di questi orientamenti, più che il risultato di un'astratta ripartizione di ruoli, corrispondente in concreto ad un effettivo potere di gestione del trattamento, titolare e responsabile divengono qualificazioni utilizzate in maniera funzionale rispetto agli scopi perseguiti circa l'allocazione del potere di controllo sull'uso dei dati o delle responsabilità inerenti al trattamento*"; così A. MANTELERO, *op. cit.*

entrambi il titolare del trattamento e il responsabile del trattamento siano coinvolti nello stesso trattamento e siano, ai sensi dei paragrafi 2 e 3, responsabili dell'eventuale danno causato dal trattamento, ogni titolare del trattamento o responsabile del trattamento è responsabile in solido per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dell'interessato"[318].

La disposizione stabilisce, dunque, il cumulo di responsabilità tra titolare, contitolari, responsabili.

Solo i sub-responsabili vengono esclusi da tale regola: il DPO, inoltre, non viene richiamato come soggetto responsabile ai sensi dell'art. 82 GDPR, ma ciò non esclude che egli possa essere chiamato al risarcimento del danno sulla base della disciplina tradizionale di cui all'art. 2043 c.c. (ipotesi, tuttavia, di scarsa applicazione pratica), anche per il medesimo fatto illecito per cui il danneggiato agisce nei confronti del titolare ex art. 82 GDPR. Tuttavia, in tale evenienza, il danneggiato non beneficerà, nei confronti del DPO, del regime probatorio più favorevole che deriva dall'applicazione dell'art. 82 GDPR.

Perciò, tutti i soggetti coinvolti nel trattamento illecito sono responsabili nei confronti del danneggiato solidalmente: alla luce di ciò, il titolare dovrebbe assumere un atteggiamento particolarmente cauto nella scelta dei soggetti a cui affidare l'esecuzione di parti del trattamento.

Nei rapporti interni, rileverà, invece, lo specifico apporto causale di ciascun soggetto alla causazione del danno e, infatti, il par. 5 dell'art. 82 dispone che "*qualora un titolare del trattamento o un responsabile del trattamento abbia pagato, conformemente al paragrafo 4, l'intero risarcimento del danno, tale titolare del trattamento o responsabile del trattamento ha il diritto di reclamare dagli altri titolari del trattamento o responsabili del trattamento coinvolti nello stesso trattamento la parte del risarcimento corrispondente alla loro parte di responsabilità per il danno conformemente alle condizioni di cui al paragrafo 2*".

Nei rapporti interni, pertanto, il titolare o responsabile che abbia pagato l'intero risarcimento al danneggiato potrà agire in via di regresso e di surroga nei confronti degli altri soggetti coinvolti nel trattamento.

5. Gestione del rischio privacy e *accountability*

Si è in precedenza analizzato il valore "personale" e il valore "sociale" della *privacy*[319]. In particolare, tale secondo aspetto si sviluppa negli anni '60, quando viene riconosciuto il "rischio" sociale, ossia il pregiudizio collettivo alla società che può derivare dall'utilizzo di banche dati e di elaboratori

---

[318] La disposizione è applicazione della regola generale di cui all'art. 2055 c.c., secondo cui "*Se il fatto dannoso è imputabile a più persone, tutte sono obbligate in solido al risarcimento del danno. / Colui che ha risarcito il danno ha regresso contro ciascuno degli altri, nella misura determinata dalla gravità della rispettiva colpa e dall'entità delle conseguenze che ne sono derivate".*

[319] Sul tema si v. M. GAMBINI, *op. cit.*

elettronici, idonei, per l'appunto, alla schedatura di massa di tutti i cittadini. Queste tecnologie permettono di esercitare un controllo sociale degli individui attraverso la raccolta e l'elaborazione congiunta delle più diverse informazioni.

Dagli elaboratori elettronici deriva, dunque, un potere di controllo e "informativo", che assume la caratteristica d'essere occulto, sia perché sovente gli interessati non conoscono la stessa costituzione di questi archivi, sia perché non sono conosciute ai terzi le modalità di gestione di tali banche date, nonché le informazioni ulteriori che dalle stesse possono essere tratte[320].

Il legislatore introduce così le prime forme di disciplina sul trattamento dei dati, al fine di contemperare le contrapposte esigenze degli utenti, dall'un lato, degli enti pubblici e privati che detengono le banche dati, dall'altro.

In particolare, gli utenti sono portatori di un interesse alla trasparenza, ossia a conoscere le modalità di raccolta e gestione dei dati: il cittadino ambisce, inoltre, alla fissazione di un limite al potere degli enti pubblici e privati di poter incrociare le informazioni contenute nelle diverse banche dati, essendo questa un'attività che genera ulteriori informazioni e dunque un'intrusione nella sfera privata.

Dall'altra prospettiva, gli enti pubblici e privati detentori degli archivi hanno la necessità di utilizzare i dati personali per svolgere specifici controlli e verifiche di interesse pubblico (come quelle fiscali), oppure per sfruttare tali dati a fini commerciali.

Si sviluppano, così, le prime discipline degli Stati europei sul "trattamento dei dati personali", le quali tutte dimostrano un approccio specifico al tema della gestione del rischio – inteso come rischio "della collettività" – che deriva dalle tecniche informatizzate con cui i dati vengono trattati.

Tali legislazioni sono accomunate: 1) dal principio di trasparenza, che consente a chiunque di conoscere l'esistenza dell'archivio; 2) dalla predisposizione di vincoli istituzionali e controlli pubblici sulle banche dati; 3) dal diritto riconosciuto agli individui di essere informato sul trattamento dei suoi dati personali.

Va evidenziato che in queste prime elaborazioni, e così nella Convenzione n. 108 del Consiglio d'Europa, all'individuo viene riconosciuto un mero diritto di informazione, senza alcun accenno al diritto all'autodeterminazione in relazione ai dati personali (che sorgerà solo successivamente): l'individuo, in questa fase, non ha alcun potere di controllo.

Tuttavia, è fondamentale osservare che prima vi è stata l'emersione[321] di un'istanza sociale finalizzata a disciplinare il potere informatico e il potere informativo che ne deriva, solo successivamente,

---

[320] E. GIANNANTONIO, voce Dati personali (tutela dei), in *Enc Dir.*, Giuffrè, 1999, p. 483; G. B. FERRI, *Privacy e libertà informatica,* in *Le banche dati in Italia. Realtà normativa e progetti di regolamentazione*, a cura di V. ZENO-ZENCOVICH, Jovene, 1985, p. 59.

[321] A. MANTELERO, *Responsabilità e rischio nel Reg. UE 2016/679*, in *Nuove leggi civ. comm.*, 2017, p. 145; ID., *La gestione del rischio*, in *La protezione dei dati personali in Italia,* op. cit., p. 478.

invece, la disciplina sul trattamento dei dati è stata intesa in chiave individualista, dunque finalizzata alla tutela dei dati quale attributo della personalità, che diviene un diritto fondamentale dell'uomo.
Osserva autorevole dottrina che la disciplina sul trattamento dei dati nasce "*con l'intenzione di regolare i flussi di dati, disciplinarne le modalità – anche tecniche – di trattamento, guardando ai rischi legati alla sicurezza da intrusioni ed agli accessi illegittimi di dati*", aggiungendo che "*...manca invece, nelle prime generazioni di normative, un riferimento al ruolo dell'interessato in termini di pieno esercizio dell'autodeterminazione rispetto alle informazioni che lo riguardano*", con ciò evidenziando, dall'un lato, che l'istanza di tutela individuale segue e non precede l'idea che una disciplina dei dati sia innanzitutto necessaria per la tutela della collettività, dall'altro lato che la prospettiva della gestione del rischio è fondamentale sin dalle prime elaborazioni normative in materia.
Ci si rende conto, immediatamente, che a fronte dell'informatizzazione dei dati e dell'utilizzo di strumenti tecnologici avanzati e in continua evoluzione, risulta necessario porre dei vincoli istituzionali nonché elaborare principi di tutela che accompagnino l'intero trattamento: in tal modo, l'attività diviene procedimentalizzata e viene disposto l'utilizzo di specifiche misure di sicurezza che tutelino da accessi e trattamenti illegittimi.
Dunque, ben può affermarsi che la disciplina sul trattamento dei dati nasce come disciplina di controllo dei rischi derivanti dal trattamento, inizialmente intesi come rischi di sicurezza per la collettività e solo successivamente come intrusioni illecite nella sfera privata.
Tale momento coincide con il diffondersi, sul finire del secolo scorso, delle nuove tecnologie, che determinano sempre più l'entrata dei dati personali nel settore produttivo. Alla diffusione di Internet e delle nuove tecnologie consegue, infatti, un aumento esponenziale del flusso di dati nonché la circostanza che sempre più soggetti privati iniziano ad utilizzarli a fini economici.
Il potere economico generato dai dati, divenendo disponibile ad una cerchia sempre più ampia di attori privati, fa sì che, correlativamente, vengano riconosciuti poteri di controllo da parte degli individui stessi dei dati.
Si sviluppa, dunque, il modello di *data protection:* esso si basa principalmente sul meccanismo del consenso dell'interessato, assolutamente necessario per il trattamento. Con tale previsione, il legislatore dimostra la volontà di attribuire al singolo un potere maggiore di autodeterminazione rispetto ai propri dati: nel frattempo, il diritto alla protezione dei dati viene riconosciuto come un vero e proprio diritto fondamentale della personalità (si v. Dir. 95/46/CE e Codice *privacy* italiano).
Il consenso informato rappresenta, dunque, presupposto imprescindibile di un lecito trattamento. L'interessato deve essere informato con trasparenza sulle modalità di raccolta e conservazione dei dati, nonché sul soggetto che li raccoglie e sulle finalità e modalità del trattamento, così da trovarsi

nella condizione di valutare adeguatamente se concedere il consenso al trattamento.

Si può evidenziare, dunque, che nella prospettiva della Dir. 95/46/CE, la gestione del rischio per la sicurezza nei confronti dell'individuo viene affidata all'individuo stesso, proprio attraverso lo strumento del consenso. L'informativa rappresenta lo strumento essenziale per rendere edotto l'interessato circa i rischi potenziali del trattamento; tuttavia, nella fase successiva, ossia una volta che sia stato raccolto il consenso, l'impianto della Direttiva non può dirsi approntato su una logica di gestione dei rischi individuali.

In ogni caso, con la Dir. 95/46/CE, il modello della *data protection* si allarga sino alla tutela individualista, pur non esaurendosi in esso.

Permane, comunque, l'idea che la disciplina sulla protezione dei dati debba fronteggiare quei rischi per la sicurezza della collettività (come la discriminazione di gruppi etnici o razziali attraverso la schedatura dei cittadini) che avevano spinto all'elaborazione delle prime discipline. Ed infatti, l'impianto della previgente legislazione europea viene, in questo senso, ulteriormente potenziato.

Ora, inolttre, la *data protection* deve bilanciare gli interessi del singolo con la necessità di non frenare lo sviluppo del nuovo mercato digitale. Dunque, se è imprescindibile garantire la sicurezza dei diritti e delle libertà degli individui, parimenti è necessario garantire che i dati personali possano essere sfruttati del mercato economico dagli attori privati, che ricavano un valore enorme dall'utilizzo degli stessi.

Sono questi duplici e contrapposti interessi, quelli dell'individuo e quelli del mercato, che la disciplina europea (sia la Direttiva 95/46/CE, sia il Regolamento UE 2016/679) vuole preservare e bilanciare.

Nella Direttiva 95/46/CE, la logica della gestione del rischio viene declinata, innanzitutto, come necessità di garantire la "sicurezza dei dati", ossia la sicurezza informatica del trattamento. Così si evince dal Considerando n. 46, il quale espressamente afferma che la tutela dei diritti e delle libertà delle persone interessate relativamente al trattamento di dati personali richiede l'adozione di adeguate misure tecniche ed organizzative, sia al momento della progettazione che a quello dell'esecuzione del trattamento, "*in particolare per garantirne la sicurezza ed impedire in tal modo qualsiasi trattamento non autorizzato*", aggiungendo che tali misure devono "*assicurare un adeguato livello di sicurezza*". Gestione del rischio significa[322], nella prospettiva della Direttiva, garantire la sicurezza dei dati personali in particolare dai c.d. "rischi illeciti", ossia dalla distruzione accidentale o illecita, dalla

[322] In ambito europeo, si v. R. GELLERT, *Data protection: a risk regulation? Between the risk management of everything and the precautionary alternative*, in *International Data Privacy Law*, 2015, vol 5, n. 1, p. 3-14; ID., *Understanding data protection as risk regulation* in *Journal of Internet Law*, 2015, pp. 3-15; C. HOOD-H. ROTHSTEIN-R. BALDWIN, *The Government of Risk—Understanding Risk Regulation Regimes*, Oxford University Press, Oxford, 2001.

perdita accidentale o dall'alterazione, dalla diffusione o dall'accesso non autorizzati, come disposto espressamente dall'art. 17 (rubricato "sicurezza dei trattamenti").

Il concetto di "gestione del rischio" è strettamente connesso al principio di *accountability*, poiché è proprio attraverso l'individuazione e la mitigazione dei rischi di trattamento illecito che il titolare adempie all'obbligo di "responsabilizzazione". Il titolare deve mantenere un approccio proattivo nel prevenire i rischi, dotandosi di una struttura organizzativa che, a tutti i livelli e in tutte le aree di competenza, adotti le necessarie misure per garantire che i dati personali siano trattati sempre in modo lecito.

Va evidenziato che la gestione del rischio è un concetto ben precedente all'introduzione della nuova disciplina europea sul trattamento dei dati. Per la precisione, esso non nasce neppure in un contesto giuridico, venendo elaborato e sviluppato dalle scienze economico-aziendalistiche degli anni '90 che si occupano del c.d. "*risk management*"[323].

Si tratta di quell'insieme di processi attraverso cui un'azienda identifica, analizza, quantifica, monitora, elimina i rischi legati ad un determinato processo produttivo, con l'obiettivo di minimizzare le perdite e massimizzare l'efficacia e l'efficienza dei processi produttivi. Attraverso questo articolato insieme di procedure, l'impresa valuta dapprima la probabilità che si verifichi una determinata situazione negativa e, successivamente, individua le modalità per evitarla, ridurne gli effetti, trasferirla a terzi o infine, in molti casi, accettarne in parte o totalmente le conseguenze, cercando di minimizzare gli impatti sulla stessa attività d'impresa[324].

Lo schema della gestione si compone, in via esemplificativa, delle seguenti fasi: *i)* definizione del contesto; *ii)* identificazione dei rischi; *iii)* analisi del rischio; *iv)* valutazione dei rischi; *v)* controllo dei rischi (che a sua volta consta di due momenti, il primo dedicato alla preparazione ed approvazione del "piano di azione dei rischio" (*risk action plan*), il secondo all'esecuzione, controllo e modifica del piano).

Tale schema presenta una natura tipicamente circolare, perché deve essere ripetuto periodicamente in costanza della mutevolezza dei rischi relativi al contesto di riferimento in cui l'analisi concreta è svolta.

---

[323] Secondo Gellert "*the risk-based regulation emerged in the 1990s in the wave of so-called New Public Management (NPM) in the UK. At its core, one can find the following rationales: a focus on 'explicit standards and measures of performance', on private sector styles of management practice, on 'hands-on professional management' in the public sector, and on greater discipline and parsimony in resource use. In short, risk-based regulation is about the optimum allocation of resources according to the impact and probability of (societal) risks as well as about accounting and legitimizing such use*" (R. GELLERT, *Data protection: a risk regulation? Between the risk management of everything and the precautionary alternative*, *op. cit.*)

[324] Definizione tratta da Borsa Italiana, all'indirizzo https://www.borsaitaliana.it/notizie/sotto-la-lente/risk-management-107.htm.

Innanzitutto, dunque, i rischi devono essere definiti e individuati. In via generale, si definisce "rischio" l'ipotesi non desiderata che si verifichi un evento negativo che possa incidere sulle lecite modalità del trattamento dei dati personali. Nella dottrina anglosassone la *risk regulation* è definita come "*governmental interference with market or social processes to control potential adverse consequences*"[325] e si aggiunge che "*put simply, risk is the chance (understood as a probabilistic notion) that a danger (i.e. an event with harmful consequences) will happen. Risk signals the threat of harm appraised through statistics and probabilities. A more technical definition would be the following: risk is an objective measurable entity combining the probability of an adverse event and the magnitude of its consequences*"[326].

Senza pretesa di esaustività, mutuando le categorie della dottrina aziendalistica, i rischi possono essere classificati nelle seguenti categorie:

- errori umani, che riguardano, ad esempio, le perdite derivanti da comportamenti del personale (errori, frodi, mancato rispetto di regole e procedure interne);
- errori di processo (come malfunzionamenti di procedure interne o lacune nei controlli);
- errori dovuti a fattori esogeni (come minacce ambientali, attività criminali, eventi politici o militari e, ad esempio, modifiche di legge);
- errori di tecnologia, relativi ad esempio agli impianti.

In secondo luogo, i rischi devono essere valutati: si analizza la probabilità che un rischio si realizzi e il suo impatto sull'attività dell'azienda. È necessario verificare quale impatto tali rischi possono determinare sui diritti e le libertà degli individui, quale sia il numero di interessati potenzialmente coinvolti, quale la natura dei dati personali eventualmente interessati nonché la quantità degli stessi.

In questa fase, peraltro, si potrebbero profilare rischi che presentano sì una bassa probabilità di occorrenza ma che, se concretizzati, determinerebbero potenzialmente un impatto assai rilevante; viceversa, un evento potrebbe essere valutate come rischio ad elevata probabilità di occorrenza ma a basso impatto.

Stabilita la probabilità di verificazione e la gravità dell'impatto, i rischi vengono classificati sulla base di uno specifico punteggio: in tal modo, essi possono essere fronteggiati con un approccio il più oggettivo possibile e secondo una scala di priorità adattabile allo specifico contesto in cui rilevano. Si tratta di un'analisi prognostica e probabilistica, svolta in modo esclusivamente astratto-teorico.

L'identificazione dei rischi si rivela, in realtà, un'attività particolarmente complessa, poiché unitamente alla considerazione dei rischi interni all'organizzazione del titolare, devono essere

---

[325] C. HOOD-H. ROTHSTEIN-R. BALDWIN, *op. cit.*

[326] R. GELLERT, *Data protection: a risk regulation? Between the risk management of everything and the precautionary alternative*, *op. cit.*, p. 7.

analizzati anche quelli di natura esterna; evidentemente, è rispetto alle variabili esterne all'azienda che si registrano le maggiori problematiche di monitoraggio e analisi.
Come detto, vengono fissati punteggi e soglie quantitative e qualitative di rilevanza dei rischi (ad es. soglia bassa, media, alta).
All'analisi dei rischi consegue l'individuazione delle procedure di mitigazione degli stessi, attraverso la predisposizione di un piano specifico.
La principale difficoltà legata al *risk management* è connessa al grado di difficoltà legata alle analisi e alle valutazioni da effettuare, nonché alla redazione di un concreto piano di attuazione per fronteggiare i rischi.
Con riferimento alle misure di mitigazione, il titolare può adottare misure organizzative, tecniche o giuridiche.
Ad esempio, ha natura organizzativa la distribuzione delle competenze e la frammentazione dei processi e dei trattamenti dei dati attraverso la predisposizione e l'attuazione di un organigramma. In questo caso, il titolare affida ai soggetti più competenti le fasi più delicate del processo, o valuta l'esternalizzazione delle stesse a favore di soggetti terzi particolarmente qualificati.
Nell'ambito della *cyber security*, vi sono aziende fortemente specializzate nell'offrire soluzioni informatiche di altissimo livello per garantire misure tecniche di mitigazione dei rischi *privacy*, sia esterni (attacchi informatici), sia interni (predisposizione di misure tecniche informatiche che minimizzino il rischio di comportamenti umani errati o poco diligenti).
Inoltre, il titolare che si avvalga dell'attività di soggetti esterni o interni alla propria impresa, delegando agli stessi parti specifiche di trattamento in ragione della loro competenza, dovrebbe provvedere anche alla contrattualizzazione del rapporto che con tali soggetti instaura. In questo modo, imponendo specifici obblighi, il titolare minimizza il rischio che si verifichino eventi negativi.
Nell'approccio della scienza aziendalistica, l'analisi del rischio comporta sempre un bilanciamento tra gli effetti negativi in caso di realizzazione del rischio e i costi di mitigazione dello stesso: talvolta, nella prospettiva dell'impresa, la scelta più efficiente e considerata complessivamente come la più economica è quella di non adottare alcuna misura precauzionale, accettando il verificarsi del rischio stesso. Un'azienda deve, infatti, quantificare la spesa che il monitoraggio di determinati rischi può richiedere, poiché da un'analisi costi/opportunità potrebbe emergere come la gestione di alcuni rischi comporti piuttosto la sottrazione di risorse utili ad attività più redditizie.
Per questa ragione, l'approccio basato sul *risk management*, quando applicato al trattamento dei dati personali, deve mutare, non potendo fondarsi su un mero rapporto costi/benefici, ossia sulla sola efficienza del processo.
La disciplina di protezione dei dati personali impone, infatti, di considerare unitamente i diversi diritti

coinvolti (quelli che fanno capo agli interessati e al titolare) e di bilanciarli al fine di verificare la prevalenza e rilevanza di alcuni in una determinata situazione. Ciò comporta che in determinate situazioni l'azione di mitigazione del rischio è irrinunciabile, quando risulti che un determinato diritto non può essere del tutto soppresso.

In ogni caso, la disciplina per la protezione dei dati stabilisce un principio di proporzionalità anche nell'adozione delle misure di mitigazione più adeguate.

6. La gestione del rischio nel GDPR

Con il GDPR il binomio *accountability*-gestione del rischio trova la sua massima espressione: è attorno a tali concetti che si costruisce la disciplina della protezione dei dati personali. È stato osservato che "*risk management offers substantial benefits for the practice of data protection, focusing scarce resources where they are needed most, protecting individuals' fundamental rights effectively and appropriately, and facilitating efforts to make data protection more seamless across national borders*"[327].

L'attuale sistema, allora, non fa più perno sul consenso informato dell'interessato e sull'autodeterminazione dei singoli, anche se tali concetti permangono pur sempre in svariate disposizioni. Il consenso, tuttavia, ora non è sufficiente, di per sé, a rendere legittimo un trattamento, laddove il titolare non abbia assolto adeguatamente agli obblighi relativi all'*accountability*.

Il GDPR fissa, dunque, degli *standard* valutativi dell'attività dei soggetti coinvolti nel trattamento nonché alcuni aspetti procedurali del processo di gestione dei rischi da parte dei titolari. Le disposizioni in materia di misure di sicurezza, tenuta dei registri, *data breach*, valutazione d'impatto, codici di condotta e certificazioni sono improntate, infatti, all'analisi dei rischi.

Il Regolamento stabilisce un apparato di gestione del rischio c.d. modulare, nel senso che impone procedure di gestione del rischio in via generalizzata per tutti i soggetti che eseguono trattamenti, alle quali si aggiungono poi procedure più complesse per l'esecuzione di trattamenti con un livello di rischio a mano a mano più elevato.

A riguardo, l'art. 24 GDPR impone a tutti i titolari di mettere in atto misure tecniche e organizzative adeguati per garantire, ed essere in grado dimostrare, l'adempimento degli obblighi imposti dal GDPR. La stessa norma fa emergere la doverosa caratteristica di circolarità del modello di gestione, laddove prevede che "*dette misure sono riesaminate e aggiornate qualora necessario*". In altre parole, "*this so-called risk-based approach seems to combine the use of risk management tools with*

---

[327] C. KUNER-F.H. CATE-C. MILLARD-D. J. B. SVANTESSON-O. LYNSKEY, *Risk management in data protection* in *Data Privacy Law,* Vol. 5, No. 2, 2015, pp. 95-98.

a calibration of the data controllers' obligations according to the level of risk at stake"[328].

Rientrano in tale primo "modulo" di disposizioni sulla gestione del rischio anche le disposizioni relative alla *privacy by design* e *by default*, le quali costituiscono piena espressione del modello in esame incentrato al *risk management*. Infatti, è proprio la valutazione preventiva dei rischi e degli impatti che realizza al meglio la gestione dei rischi che possono verificarsi quando il processo viene concretamente posto in essere.

Il GDPR impone, dunque, di verificare in anticipo, all'inizio di ogni fase di progettazione, l'impatto sui dati personali di un nuovo prodotto o servizio[329]. Quest'attività preventiva consente di limitare i rischi e rendere più efficiente la stessa attività d'impresa: una volta realizzato effettivamente il prodotto o il servizio, risulteranno probabilmente superflue ulteriori attività di valutazione, proprio perché tale prodotto (o servizio) è stato già modellato secondo modalità idonee a garantire un adeguato livello di tutela.

Sulla scorta dell'art. 25, le misure tecniche e organizzative devono strutturarsi "*tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento…*".

Questa formulazione viene intesa in due modi differenti.

Un primo orientamento interpreta questa disposizione "*as forcing controllers to implement available technical solution if the cost is not prohibitive*"[330], nel senso che quando una soluzione tecnica è necessaria per l'adempimento di uno specifico obbligo imposto dal GDPR ed esiste sul mercato a un costo ragionevole, il titolare è tenuto all'acquisto[331].

Si tratta, evidentemente, di un criterio assai elastico, non essendo definito dal legislatore europeo cosa significhi che le misure devono essere conformi allo "*stato dell'arte*". Tale formulazione richiama quella prevista in tema di responsabilità per danno da prodotti difettosi, in base alla quale il produttore non risponde se lo stato delle conoscenze scientifiche e tecniche, al momento in cui il produttore ha messo in circolazione il prodotto, non permetteva ancora di considerare il prodotto come difettoso[332].

Sul punto, viene affermato che tale verifica deve essere condotta "*on the basis of the objective state*

---

[328] R. GELLERT, *op. ult. cit.*, p. 13.

[329] "*Article 25 requires every controller and processor (and indirectly all vendors) to implement data protection by design and default. This can mean business as usual in the form of procedural solutions or an explosion of innovative architectural solutions*" (I.S RUBINSTEIN-N. GOOD, *The trouble with Article 25 (and how to fix it): the future of data protection by design and default in International Data Privacy Law*, Vol. 10, No. 1, 2020, pp. 37-56).

[330] I.S RUBINSTEIN - N. GOOD, *op. cit.*, 6.

[331] M. HILDEBRANDT-L. TIELEMANS, *Data Protection by Design and Technology Neutral Law*, in *Computer Law & Security Review*, 2013, 29, p. 509.

[332] Art. 118, lett. e), Cod. consumo.

of the available scientific and technical knowledge including that at the most advanced level and not restricted to the relevant industrial sector"[333].

Secondo un diverso orientamento, più coerente con lo spirito del GDPR, il requisito dello stato dell'arte "*serves as a benchmark requiring controllers to explore the most recent developments and knowledge associated with data processing*"[334], nel senso che il titolare, anche rispetto alla *privacy by design* e *by default*, è tenuto a mantenere un atteggiamento proattivo finalizzato alla conoscenza dei nuovi *standard* tecnologici (sia *software* che *hardware*), della sicurezza informatica, delle innovazioni frutto dalla ricerca.

A questo primo insieme di procedure, si somma l'obbligo previsto dall'art. 35 GDPR, ben più pregnante, di eseguire una valutazione d'impatto ogniqualvolta un tipo di trattamento, in forza dell'utilizzo di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità dello stesso, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

L'esecuzione di tale valutazione d'impatto è, inoltre, obbligatoria nei casi di:

a) valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato (compresa la profilazione), sulla quale si fondano decisioni che producono effetti giuridici o incidono significativamente su dette persone fisiche;
b) trattamento, su larga scala, di categorie particolari di dati personali (in specie, quelli di cui all'art. 9, par. 1, GDPR), di dati relativi a condanne penali e ai reati di cui all'art.10;
c) sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Le Autorità nazionali ben possono individuare ulteriori casi da sottoporsi obbligatoriamente ad una valutazione d'impatto (art. 35, par. 4), nonché prevedere elenchi di trattamenti da considerarsi sempre esentati da tale valutazione (art. 35, par. 5).

6.1. Mappatura dei processi

Al fine di realizzare un'efficace operazione di *risk management* relativamente ai rischi per i dati personali, il titolare del trattamento deve, prima di tutto, provvedere ad eseguire una "mappatura dei trattamenti", ossia deve individuare e tracciare tutti i processi interni alla propria organizzazione che implicano il trattamento di dati personali.

È il principio di *accountability* che impone al titolare di eseguire tale attività: il suo corretto svolgimento è presupposto essenziale per mettere in atto tutte le misure di sicurezza necessarie onde evitare un pregiudizio per gli interessati cui i dati personali si riferiscono.

---

[333] C. VAN DAM, *European Tort Law*, OUP, Oxford 2013.

[334] L. JASMONTAITE & OTHERS, *Data Protection by Design and by Default: Framing Guiding Principles into Legal Obligations in the GDPR*, *European Data Protection Law Review*, 2018, 4, p. 16; I.S RUBINSTEIN-N. GOOD, *op. cit.*, 6.

Lo svolgimento di tale attività di mappatura dei processi, unitamente alla sua documentazione per iscritto, è specificamente imposto dal Regolamento. In particolare, in virtù dell'art. 30 GDPR, il titolare ha l'obbligo di predisporre un "registro delle attività di trattamento", contenente: a) il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare e del responsabile della protezione dei dati; b) le finalità del trattamento (nonché la base giuridica su cui lo stesso si fonda[335]); c) una descrizione delle categorie di interessati e delle categorie di dati personali; d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali; e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate.

Tale registro[336] deve contenere, "…*ove possibile*…", il termine previsto per la cancellazione dei dati e l'indicazione delle misure di sicurezza tecniche e organizzative predisposte per ciascun trattamento[337].

L'obbligo della tenuta del registro non si applica imprese o organizzazioni con meno di 250 dipendenti, a meno che 1) "*il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato",* oppure 2) "*il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10*".

Con riferimento all'ipotesi *sub* 1, si rileva come tale disposizione ricalchi uno dei casi in cui è obbligatorio svolgere la valutazione d'impatto, la quale, dunque, andrà sempre "tracciata" anche all'interno del registro delle attività di trattamento. In relazione all'ipotesi *sub* 2, si rammenta che il titolare è obbligato alla nomina del responsabile per la protezione dei dati nel caso in cui una delle

---

[335] AUTORITÀ GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *FAQ sul registro delle attività di trattamento*, 8.10.2018, all'indirizzo https://www.garanteprivacy.it/home/faq/registro-delle-attivita-di-trattamento.

[336] Come indicato dal Garante, il registro dei trattamenti è redatto su una griglia/tabella (generalmente predisposta tramite il programma excel) e ogni riga della tabella viene dedicata ad un trattamento specifico, affinché sia identificato singolarmente.

[337] Parallelo al suddetto obbligo è quello previsto per il responsabile di tenere un registro dei trattamenti che svolge per ciascuno titolare, indicando: a) il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati; b) le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento; c) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate; d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

attività principali consista 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*". Dunque, se il titolare svolge non occasionalmente trattamenti che includono tali categorie di dati, è obbligato a rilevarlo per iscritto nel registro; se tale attività non solo è continuativa e diffusa, ma è anche svolta "*su larga scala*", il GDPR impone, in aggiunta, la nomina del responsabile. Quest'ultimo, si ricorda, presta attività di consulenza al titolare anche nella tenuta del registro, dunque nell'individuazione dei trattamenti, e ad esso il titolare è tenuto a rivolgersi nello svolgimento della valutazione d'impatto (su cui v. *infra*).

Dal combinato delle disposizioni testé citate emerge appieno la "modularità" del sistema di gestione del rischio descritto dal Regolamento: il legislatore prevedere un insieme di obblighi che possono, ed anzi, devono informare il comportamento del titolare alla luce della complessità delle situazioni che gli si prospettino. In altri termini, a trattamenti che possono comportare rischi maggiori per i diritti e le libertà degli interessati deve accompagnarsi il rispetto di maggiori e più stringenti obblighi di condotta.

La tenuta del registro dei trattamenti e la nomina del responsabile per la protezione dei dati non sono, dunque, sempre obbligatorie e certamente sarebbero del tutto superflue in svariate ipotesi pratiche.

Tuttavia, la redazione del registro che dà atto dello svolgimento di attività di trattamento deve essere presa in considerazione dal titolare anche al di fuori delle ipotesi specifiche dell'art. 30, in vista dell'adempimento dell'obbligo di *accountability*. Infatti, talvolta, anche le imprese di piccole e medie dimensioni effettuano numerosi trattamenti e instaurano flussi di dati con differenti responsabili esterni: in queste circostanze, la tenuta di un registro delle attività di trattamento è essenziale per il titolare al fine di monitorare adeguatamente tutte le attività realizzate e considerare con efficacia i rischi insisti nella propria organizzazione; inoltre, la tenuta di tale registro dimostra che la responsabilizzazione del titolare, dunque diviene uno strumento fondamentale ai fini della prova liberatoria per andare esente da responsabilità.

Lo stesso meccanismo può applicarsi alla nomina del responsabile per la protezione dei dati personali: anche al di fuori delle ipotesi in cui l'art. 37 GDPR pone la nomina come obbligatoria, può essere utile designare un responsabile affinché sovrintenda e monitori tutte le attività di trattamento dei dati poste in essere dall'impresa. Trattasi, anche in tal caso, di uno strumento che può rivelarsi essenziale per l'adempimento all'obbligo di *accountability*, nonché per la sua dimostrazione.

Il registro delle attività di trattamento e la nomina del responsabile per la protezione dei dati costituiscono, pertanto, due presidi fondamentali per la mappatura e il tracciamento dei processi che involgono il trattamento di dati personali.

6.2. Valutazione d'impatto: contenuto, finalità, modalità esecutive

Il Regolamento generale sulla protezione dei dati non definisce formalmente il concetto di valutazione d'impatto sulla protezione dei dati, ma ne fornisce solamente il contenuto minimo (art. 35, par. 7):

- descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;
- valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
- valutazione dei rischi per i diritti e le libertà degli interessati;
- indicazione delle misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per assicurare la protezione dei dati personali e dimostrare la conformità al GDPR, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Il significato e il ruolo della valutazione d'impatto vengono chiariti dal Considerando n. 84, il quale afferma che per "*potenziare il rispetto del presente regolamento qualora i trattamenti possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento dovrebbe essere responsabile dello svolgimento di una valutazione d'impatto sulla protezione dei dati per determinare, in particolare, l'origine, la natura, la particolarità e la gravità di tale rischio*" e prevede, inoltre, che "*l'esito della valutazione dovrebbe essere preso in considerazione nella determinazione delle opportune misure da adottare per dimostrare che il trattamento dei dati personali rispetta il presente regolamento*".

Al fine di svolgere adeguatamente la valutazione d'impatto, il titolare deve, inoltre, tenere in considerazioni le seguenti linee guida e pareri[338]:

- linee guida del Gruppo di Lavoro Articolo 29 in materia di "*valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate il 4.4.2017[339];
- dichiarazione del Gruppo di Lavoro Articolo 29 sul "*ruolo di un approccio basato sul rischio nei quadri giuridici in materia di protezione dei dati*" adottata il 30.5.2014[340];
- linee guida del Gruppo di Lavoro Articolo 29 "*sui responsabili della protezione dei dati*"

[338] Si veda anche TRILATERAL RESEARCH & CONSULTING, *Privacy impact assessment and risk management – Repost for the Information Commissioner's Office*, 4.5.2013, che offre una panoramica delle principali metodologie e standard utilizzati per la gestione del rischio e per la valutazione d'impatto sui dati personali, anche attraverso lo studio di casi pratici, nonché R. BINNS, *Data protection impact assessments: a meta-regulatory approach* in *International Data Privacy Law*, Vol. 7, No. 1, 2017, pp. 22-35.

[339] Reperibili all'indirizzo https://ec.europa.eu/newsroom/article29/items/611236/en.

[340] "*WP29 Statement 14/EN WP 218 on the role of a risk-based approach to data protection legal frameworks*" all'indirizzo web http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf?wb48617274=72C54532.

adottate il 13.12.2016[341];

- parere del Gruppo di Lavoro Articolo 29 sulla "*limitazione della finalità*" adottato il 2.4.2013[342];
- norme internazionali considerate buone prassi nella gestione del rischio, come la norma ISO 31000:2009 sulla "*Gestione del rischio - Principi e linee guida*" (modificata dalla ISO 31000:2018) e la ISO/IEC 29134 (progetto), *Information technology – Security techniques – Privacy impact assesment – Guidelines*[343].

Dall'insieme di questo quadro normativo risulta che la valutazione d'impatto sulla protezione dei dati è un processo inteso a descrivere il trattamento, valutarne la necessità e la proporzionalità, nonché a contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali, valutando detti rischi e determinando le misure per affrontarli.

Lo scopo non è eliminare del tutto il rischio, poiché si tratterebbe, in molte ipotesi, di un obiettivo non raggiungibile, come osservato dalla dottrina secondo cui "*contrary to what is often claimed by governments themselves, zero-risk (ie avoiding all risks stemming from an activity) is simply impossible*" [344]. Infatti, la stessa nozione di rischio dimostra che è impossibile controllare ogni fattore o variabile: "*one may always discover a new factor, so that whatever one does, and no matter how many risk factors they untangle, there will always be another reason for the risk to occur. 'If risks cannot be avoided, they must therefore be managed'*": si tratta, piuttosto, di governare i rischi nel modo più efficiente, mitigandoli il più possibile alla luce del contesto di riferimento.

Come osservato dal Gruppo di Lavoro Articolo 29 nelle recenti Linee Guida del 4.4.2017, la valutazione d'impatto sulla protezione dei dati è uno strumento fondamentale per la responsabilizzazione, in quanto sostiene i titolari del trattamento non soltanto nel rispettare i principi del Regolamento, ma anche nel dimostrare che sono state adottate misure appropriate per garantire il rispetto delle disposizioni prescritte. In altre parole, una valutazione d'impatto sulla protezione dei dati è un processo inteso a garantire e dimostrare la conformità al Regolamento, ovverosia i due

---

[341] Documento 16/EN WP 243 "Linee guida sui responsabili della protezione dei dati (RPD)" all'indirizzo web http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf?wb48617274=CD63BD9A.

[342] "*WP29 Opinion 03/2013 on purpose limitation*" all'indirizzo web http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf?wb48617274=39E0E409.

[343] Norma ISO 31000:2009, *Gestione del rischio - Principi e linee guida*, Organizzazione internazionale per la normazione (ISO); ISO/IEC 29134 (progetto), *Information technology – Security techniques – Privacy impact assesment – Guidelines* (in inglese), Organizzazione internazionale per la normazione (ISO). La ISO 31000 è la metodologia di gestione del rischio più diffusa. Questa norma riconosce la varietà della natura, del livello e la complessità dei rischi e fornisce delle linee guida generali sui principi e sull'attuazione della gestione dei rischi. Va evidenziato che essa tratta di una metodologia generica di gestione del rischio; pertanto, non affronta specificamente i rischi privacy: i suoi principi vanno dunque adatti alla materia dei dati personali.

[344] R. GELLERT, *op. ult. cit.*, p. 15.

aspetti fondamentali dell'*accountability*.

Le Linee Guida del Gruppo di Lavoro Articolo 29 definiscono il "rischio" come uno scenario che descrive un evento e le sue conseguenze, stimato in termini di gravità e probabilità; la "gestione dei rischi", invece, viene definita come l'insieme delle attività coordinate volte a indirizzare e controllare un'organizzazione in relazione ai rischi.

L'art. 35 fa riferimento al possibile rischio elevato "*per i diritti e le libertà delle persone fisiche*". Come indicato nella dichiarazione del Gruppo di Lavoro Articolo 29 sulla protezione dei dati sul "*ruolo di un approccio basato sul rischio nei quadri giuridici in materia di protezione dei dati*", il riferimento a "diritti e libertà" degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la libertà di parola, la libertà di pensiero, la libertà di circolazione, il divieto di discriminazione, il diritto alla libertà di coscienza e di religione.

Il GDPR prevede che si possa ricorrere a una singola valutazione d'impatto nel caso di trattamenti multipli simili tra loro in termini di natura, ambito di applicazione, contesto, finalità e rischi. Questo perché le valutazioni d'impatto sulla protezione dei dati mirano a studiare sistematicamente nuove situazioni che potrebbero portare a rischi elevati per i diritti e le libertà delle persone fisiche; non è dunque necessario realizzare una valutazione d'impatto nei casi (quali, ad es., operazioni di trattamento in un contesto specifico e per una finalità specifica) che siano già stati oggetto d'esame. Ciò avviene, ad esempio, quando si utilizzi una tecnologia simile per raccogliere la stessa tipologia di dati e per le medesime finalità[345].

La realizzazione di una valutazione d'impatto sulla protezione dei dati è obbligatoria soltanto qualora il trattamento "*possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche*" (Art. 35, par. 1, illustrato e integrato, rispettivamente, dai par. 3 e 4 della stessa disposizione). Così, essa risulta imprescindibile nelle ipotesi in cui viene introdotta una nuova tecnologia di trattamento dei dati, come emerge dal combinato dei Considerando nn. 89 e 91[346].

---

[345] Linee Guida del Gruppo di Lavoro Articolo 29, 4.4.2017.

[346] In particolare il Considerando n. 91 prevede che sia necessario svolgere una valutazione d'impatto quando vengono svolti trattamenti su larga scala, che mirano al trattamento di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato, ad esempio, data la loro sensibilità, laddove, in conformità con il grado di conoscenze tecnologiche raggiunto, si utilizzi una nuova tecnologia su larga scala, nonché ad altri trattamenti che presentano un rischio elevato per i diritti e le libertà degli interessati, specialmente qualora tali trattamenti rendano più difficoltoso, per gli interessati, l'esercizio dei propri diritti. Inoltre, il Considerando afferma che è "*opportuno altresì effettuare una valutazione d'impatto sulla protezione dei dati nei casi in cui i dati personali sono trattati per adottare decisioni riguardanti determinate persone fisiche in seguito a una valutazione sistematica e globale di aspetti personali relativi alle persone fisiche, basata sulla profilazione di tali dati, o in seguito al trattamento di categorie particolari di dati personali, dati biometrici o dati relativi a condanne penali e reati o a connesse misure di sicurezza*".

L'elenco previsto dall'art. 35 non si considera, comunque, esaustivo: vi possono essere operazioni di trattamento a "*rischio elevato*" che non trovano collocazione in tale elenco ma che presentano, tuttavia, rischi altrettanto elevati. Anche tali trattamenti devono essere accompagnati dalla realizzazione di valutazioni d'impatto sulla protezione dei dati.

Il problema è, dunque, quello di definire il "*rischio elevato*".

Le Linee Guida del Gruppo di Lavoro Articolo 29 prevedono nove criteri interpretativi che possono essere utilizzati dal titolare del trattamento per verificare se un trattamento si debba considerare a rischio "elevato". Nello specifico, è necessario verificare se il trattamento avviene con le seguenti modalità o per il perseguimento delle finalità di seguito elencate.

1. Valutazione o assegnazione di un punteggio, inclusiva di profilazione e previsione, in particolare in considerazione di *"aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato"* (Considerando 71 e 91).
2. Processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente (art. 35, par. 3, lett. a)).
3. Monitoraggio sistematico per osservare, monitorare o controllare gli interessati, ivi inclusi i dati raccolti tramite reti o "*la sorveglianza sistematica su larga scala di una zona accessibile al pubblico*" (art. 35, par. 3, lett. c)). Questo tipo di monitoraggio rappresenta un criterio in quanto i dati personali potrebbero essere raccolti in circostanze in cui gli interessati possono non essere a conoscenza di chi sta raccogliendo i loro dati e di come li utilizzerà.
4. Trattamento avente ad oggetto dati sensibili o dati aventi carattere altamente personale: questo criterio include categorie particolari di dati personali, così come definite all'art. 9 (ad es., informazioni sulle opinioni politiche delle persone), nonché dati personali relativi a condanne penali o reati di cui all'art. 10[347]. Infatti, alcune categorie di dati possono aumentare il possibile rischio per i diritti e le libertà delle persone fisiche. Tali dati personali sono considerati sensibili poichè legati ad attività a carattere personale o domestico (come le comunicazioni elettroniche la cui riservatezza deve essere protetta), oppure perché influenzano l'esercizio di un diritto fondamentale (come, ad es., i dati relativi all'ubicazione, la cui raccolta mette in discussione la libertà di circolazione), oppure perché la violazione in relazione a tali dati implica chiaramente gravi ripercussioni sulla vita quotidiana dell'interessato (si pensi, ad es., a dati finanziari che potrebbero essere utilizzati per frodi relative ai pagamenti).

[347] Un esempio potrebbe essere quello di un ospedale generale che conserva le cartelle cliniche dei pazienti oppure quello di un investigatore privato che conserva i dettagli dei trasgressori.

5. Trattamento di dati su larga scala: il Regolamento generale sulla protezione dei dati personali non definisce, tuttavia, la nozione di "*su larga scala*". Al fine di verificare se un trattamento sia effettuato su larga scala possono considerarsi i seguenti ulteriori criteri[348]:
    a) il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;
    b) il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;
    c) la durata, ovvero la persistenza, dell'attività di trattamento;
    d) la portata geografica dell'attività di trattamento.
6. Creazione di corrispondenze o combinazione di insiemi di dati, ad esempio, a partire da dati derivanti da due o più operazioni di trattamento, svolte per finalità diverse e/o da titolari del trattamento diversi, secondo una modalità che va oltre le ragionevoli aspettative dell'interessato[349].
7. Dati relativi a interessati vulnerabili (Considerando n. 75): il trattamento di questa tipologia di dati assurge a criterio in ragione dell'aumento dello squilibrio di potere tra interessati e titolare del trattamento; tale aspetto fa sì che le persone possono non essere in grado di acconsentire od opporsi al trattamento dei loro dati o di esercitare i propri diritti.
8. Uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative, quali la combinazione tra uso dell'impronta digitale e del riconoscimento facciale per un miglior controllo degli accessi fisici, ecc. Il Regolamento chiarisce che l'utilizzo di una nuova tecnologia, definita "*in conformità con il grado di conoscenze tecnologiche raggiunto*", può comportare la necessità di realizzare una valutazione d'impatto sulla protezione dei dati. L'utilizzo di tale tecnologia può implicare nuove forme di raccolta e di utilizzo dei dati, con ciò costituendo un rischio elevato per i diritti e le libertà delle persone. Infatti, le conseguenze personali e sociali dell'utilizzo di una nuova tecnologia potrebbero essere sconosciute.
9. Quando il trattamento in sé "*impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto*" (art. 22 e Considerando 91). Ciò include i trattamenti che mirano a consentire, modificare o rifiutare l'accesso degli interessati a un servizio oppure la stipula di un contratto.

Secondo il Gruppo di Lavoro Articolo 29, un titolare del trattamento dovrebbe considerare come ad alto rischio un trattamento che soddisfi due criteri e, conseguentemente, svolgere una valutazione d'impatto sulla protezione dei dati. In ogni caso, maggiore è il numero di criteri soddisfatti dal trattamento, più è probabile che sia presente un rischio elevato per i diritti e le libertà degli interessati

---

[348] *Cfr*. GRUPPO DI LAVORO ARTICOLO 29, *Linee guida sui responsabili della protezione dei dati (RPD*, op. cit.

[349] Spiegazione contenuta nel parere del Gruppo di Lavoro Articolo 29 sulla limitazione della finalità, pag. 24.

e, di conseguenza, che sia necessario realizzare una valutazione d'impatto sulla protezione dei dati, indipendentemente dalle misure che il titolare del trattamento ha previsto di adottare.

Tuttavia, in talune ipotesi, il titolare può ritenere comunque di sottoporre un trattamento, che pur soddisfi soltanto uno di tali criteri, ad una valutazione d'impatto sulla protezione dei dati. All'opposto, nonostante la corrispondenza anche con tutti i criteri sopra elencati, un trattamento potrebbe essere sottratto alla valutazione di impatto da parte del relativo titolare, alla luce del fatto che questi lo classifica come trattamento tale "non presentare un rischio elevato". Certo è che, in tali casi, il titolare del trattamento è tenuto a giustificare e documentare i motivi che lo hanno spinto a non effettuare una valutazione d'impatto sulla protezione dei dati.

La valutazione d'impatto sulla protezione dei dati va effettuata "*prima del trattamento*". Ciò è coerente con i principi di protezione dei dati fin dalla progettazione e di protezione per impostazione predefinita.

La valutazione d'impatto va considerata come uno strumento finalizzato a contribuire al processo decisionale in materia di trattamento. Secondo le buone prassi, una valutazione d'impatto sulla protezione dei dati va riesaminata continuamente e rivalutata con regolarità. Dunque, essa va avviata il prima possibile nella fase di progettazione del trattamento, ed anche se alcune delle operazioni di trattamento non sono ancora note perché il titolare non conosce ancora l'intera catena di sviluppo del nuovo prodotto/servizio. L'aggiornamento della valutazione d'impatto nel corso dell'intero ciclo di vita del progetto, dall'un lato garantirà che la protezione dei dati e della vita privata sia presa in considerazione e, dall'altro, favorirà la creazione di soluzioni che promuovono la conformità del prodotto/servizio al Regolamento. Può essere altresì necessario ripetere singole fasi della valutazione a mano a mano che il processo di sviluppo evolve, così da attualizzare e ripensare costantemente le misure di sicurezza da adottare nei singoli segmenti della catena produttiva.

È interessante evidenziare che il GDPR prevede che, nello svolgimento di una valutazione d'impatto, il titolare possa coinvolgere direttamente gli interessati, decidendo di "*raccogliere le opinioni degli interessati o dei loro rappresentanti*" (art. 35, par. 9).

Secondo il Gruppo di Lavoro Articolo 29, in questi casi:

- tali opinioni possono essere raccolte attraverso una varietà di mezzi, a seconda del contesto[350];
- qualora la decisione finale del titolare del trattamento si discosti dalle opinioni degli interessati, deve documentarne le ragioni;
- sebbene non sia obbligato al coinvolgimento dei terzi, il titolare del trattamento deve giustificare, altresì documentandola, l'eventuale mancata raccolta delle opinioni degli

[350] Ad esempio "*uno studio generico relativo alla finalità e ai mezzi del trattamento, una domanda posta ai rappresentanti del personale oppure indagini abituali inviate ai futuri clienti del titolare del trattamento*".

interessati, qualora decida che ciò non sia appropriato (ad es., quando ciò sarebbe sproporzionato o rischierebbe di pregiudicare la riservatezza di informazioni aziendali);

- se lo svolgimento della valutazione d'impatto sulla protezione dei dati è proposto da dipendenti del titolare, gli stessi dovrebbero essere coinvolti nel processo di convalida di detta valutazione nonché fornire contributi alla valutazione d'impatto medesima;
- si raccomanda di verificare l'opportunità di consultare esperti indipendenti dotati di competenze specialistiche differenziate (giuridiche, informatiche, di sicurezza, sociologiche, ecc.);
- il titolare deve prevedere, nei contratti stipulati con i responsabili a cui affida parti del trattamento, il coinvolgimento degli stessi nei casi in cui la valutazione d'impatto abbia ad oggetto i trattamenti esternalizzati; il responsabile deve, dunque, assistere il titolare nello svolgimento della valutazione d'impatto tenendo conto della natura del trattamento e delle informazioni a disposizione di detto responsabile del trattamento;
- un ruolo fondamentale viene assolto dal responsabile capo della sicurezza dei sistemi d'informazione, se nominato, così come dal responsabile della protezione dei dati; tali soggetti dovrebbero suggerire al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento e dovrebbero, inoltre, assistere il titolare circa la metodologia da seguire, contribuire alla valutazione della qualità della valutazione dei rischi e del grado di accettabilità del rischio residuo, nonché allo sviluppo di conoscenze specifiche in merito al contesto proprio del titolare del trattamento;

L'attuazione della valutazione d'impatto sulla protezione dei dati è modulabile a seconda delle caratteristiche del titolare che deve eseguirla: anche un titolare di piccole dimensioni può progettare e attuare una valutazione d'impatto sulla protezione dei dati adatta alle proprie attività di trattamento. Il Considerando 90 del GDPR, mentre delinea una serie di elementi minimi della valutazione d'impatto sulla protezione dei dati, descrive solo in termini generali le modalità di esecuzione, delegando al titolare di individuare la metodologia più opportuna nel caso di specie.

In termini di gestione dei rischi, una valutazione d'impatto sulla protezione dei dati mira a "gestire i rischi" per i diritti e le libertà delle persone fisiche, utilizzando i seguenti processi:

- stabilendo il contesto: "*tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento e delle fonti di rischio*";
- valutando i rischi: "*valutare la particolare probabilità e gravità del rischio*";
- trattando i rischi: "*attenuando tale rischio*" e "*assicurando la protezione dei dati personali*", e "*dimostrando la conformità al GDPR*".

Spunti interessanti possono essere ricavati dalla norma ISO 31000[351] che propone specifiche metodologie per la gestione dei rischi aziendali: tuttavia, i procedimenti in essa descritti vanno adeguati alla materia dei dati personali.

Il GDPR offre ai titolari del trattamento la flessibilità di stabilire la struttura e la forma precisa della valutazione d'impatto sulla protezione dei dati, così da permettere che la stessa si adatti alle pratiche di lavoro esistenti. Esistono diversi processi stabiliti all'interno dell'UE e nel mondo che tengono conto degli elementi costitutivi della valutazione, come descritti dal GDPR stesso. In ogni caso, indipendentemente dalla sua forma, una valutazione d'impatto sulla protezione dei dati deve essere una vera e propria valutazione dei rischi che consenta ai titolari del trattamento di adottare misure effettive per affrontarli.

A livello pratico, le Linee Guida del Gruppo di Lavoro Articolo 29 prevedono due allegati che fissano i contenuti e gli step da seguire per svolgere correttamente la valutazione d'impatto.

Tali allegati chiariscono i requisiti essenziali della valutazione ma, al contempo, consentono la coesistenza di forme diverse di attuazione: pongono criteri possono essere utilizzati per dimostrare che una particolare metodologia di valutazione d'impatto sulla protezione dei dati soddisfa i parametri imposti dal Regolamento.

Spetta al titolare del trattamento scegliere una metodologia che risulti, comunque, conforme alle finalità fissate dal GDPR.

Al termine della valutazione, se necessario, "*il titolare del trattamento procede a un riesame per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento*" (art. 35, par. 11).

Ogniqualvolta il titolare del trattamento non è in grado di trovare misure sufficienti per ridurre i rischi a un livello accettabile (ossia i rischi residui restano comunque elevati) è necessario consultare l'autorità di controllo.

Un esempio di "rischio residuo elevato inaccettabile" è quello in cui gli interessati potrebbero subire conseguenze significative, o addirittura irreversibili, insuperabili (ad es., l'accesso illegittimo a dati che comportano una minaccia per la vita degli interessati, un loro licenziamento, un rischio finanziario), oppure quando appare evidente che il rischio si verificherà (ad es., poiché non si è in grado di ridurre il numero di persone che accedono ai dati a causa delle loro modalità di condivisione, utilizzo o distribuzione o quando non è possibile porre rimedio a una vulnerabilità ben nota).

Qualora si intenda effettuare un trattamento che potrebbe presentare un rischio elevato, il titolare del

[351] Processi di gestione del rischio: comunicazione e consultazione, definizione del contesto, valutazione dei rischi, trattamento dei rischi, monitoraggio e riesame

trattamento deve:

- scegliere una metodologia per la valutazione d'impatto sulla protezione dei dati (anche seguendo gli esempi riportati nell'Allegato 1 o 2 alle Linee Guida), oppure specificare ed attuare un processo sistematico di valutazione d'impatto sulla protezione dei dati che:
    1. sia conforme, comunque, ai criteri di cui agli Allegati delle Linee Guida;
    2. sia integrato nei processi in materia di progettazione, sviluppo, cambiamento, rischio e riesame operativo in conformità con i processi, il contesto e la cultura interni;
    3. coinvolga le parti interessate appropriate e definisca chiaramente le loro responsabilità (titolare del trattamento, responsabile della protezione dei dati, interessati o loro rappresentanti, imprese, servizi tecnici, responsabili del trattamento, responsabile della sicurezza dei sistemi d'informazione, ecc.);
- fornire la relazione relativa alla valutazione d'impatto sulla protezione dei dati all'autorità di controllo, laddove venga richiesto di procedere in tal senso;
- consultare l'autorità di controllo, qualora il titolare del trattamento non sia riuscito a determinare misure sufficienti per attenuare i rischi elevati;
- riesaminare periodicamente la valutazione d'impatto sulla protezione dei dati e il trattamento che essa valuta, almeno quando si registra una variazione del rischio posto dal trattamento;
- documentare, infine, le decisioni prese.

È solo attraverso lo svolgimento di questa attività, così come procedimentalizzata dal GDPR, che il titolare dimostra l'assolvimento all'obbligo di *accountability* e, di conseguenza, può andare esente da responsabilità nel caso in cui si verifichi un danno per l'interessato (su questo aspetto, si rinvia al capitolo successivo).

6.3. (segue) Alcune osservazioni sulla valutazione d'impatto

Dall'analisi della disciplina sulla valutazione d'impatto emergono due aspetti particolarmente interessanti ai fini del presente lavoro di ricerca.

Il primo è costituito dalla possibilità di coinvolgimento, nell'esecuzione della valutazione d'impatto, degli interessati o delle associazioni rappresentative, di cui può essere raccolta l'opinione, ai sensi dell'art. 35, par. 8.

Si tratta di uno strumento che consentirebbe, laddove reso obbligatorio almeno per le ipotesi di rischi più gravi per i diritti e le libertà degli interessati, di garantire un livello di trasparenza particolarmente elevato. L'integrazione di quest'obbligo consentirebbe, dall'un lato, agli interessati di aumentare il proprio livello di fiducia nei confronti delle imprese che trattano dati personali e, dall'altro,

garantirebbe la possibilità di esercitare un controllo maggiore sui trattamenti, sia da parte degli utenti sia da parte delle autorità di controllo.

In secondo luogo, nella valutazione d'impatto non sembra che siano tenuti adeguatamente in considerazione i rischi per i diritti della collettività e per interessi più ampi e diffusi rispetto a quelli dell'individuo. Anche nelle opinioni e pareri del Gruppo di Lavoro Articolo 29, nonché nelle linee guida delle principali organizzazioni internazionali, non sembra che sia dedicata un'attenzione particolare a questo aspetto, in quanto le principali metodologie tengono in considerazione prettamente i rischi per i diritti e le libertà dell'individuo.

6.4. Violazione di sicurezza

Il GDPR disciplina la procedura da seguire in caso di violazione dei dati personali[352], definita, all'articolo 4, punto 12, 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*"[353].

In particolare, il regolamento generale sulla protezione dei dati introduce l'obbligo di notificare una violazione dei dati personali all'autorità di controllo nazionale competente (oppure, in caso di violazione transfrontaliera, all'autorità capofila) e, in alcuni casi, di comunicare la violazione alle singole persone fisiche i cui dati personali sono stati interessati dalla violazione.

Mentre la direttiva 95/46/CE sulla protezione dei dati non conteneva uno specifico obbligo di notifica delle violazioni, il GDPR rende ora la notifica obbligatoria per tutti i titolari del trattamento "*a meno che sia improbabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche*" (art. 35). Inoltre, i responsabili del trattamento devono notificare qualsiasi violazione al proprio titolare del trattamento, affinché provveda alla notifica all'Autorità di controllo.

Il fatto che il GDPR imponga obblighi di notifica al verificarsi della violazione non significa assenza di obblighi antecedenti: il principio di *accountability* e della gestione del rischio impongono di considerare, tra i rischi, anche le possibili future violazioni di dati personali. Infatti, le linee guida del

---

[352] Sulla responsabilità conseguente alle violazioni di sicurezza, si v. A. MITRAKAS, *Assessing liability arising from information security breaches in data privacy,* in *International Data Privacy Law*, Vol. 1, No. 2, 2021, pp. 29-136.

[353] In tema di violazione dei dati personali, il Garante ha stilato una lista esemplificativa dei rischi principali (si v. GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Violazioni di dati personali (data breach) in base alle previsioni del Regolamento (UE) 2016/679*, all'indirizzo https://www.garanteprivacy.it/regolamentoue/databreach):

- l'accesso o l'acquisizione dei dati da parte di terzi non autorizzati;
- il furto o la perdita di dispositivi informatici contenenti dati personali;
- la deliberata alterazione di dati personali;
- l'impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, virus, malware, ecc.;
- la perdita o la distruzione di dati personali a causa di incidenti, eventi avversi, incendi o altre calamità;
- la divulgazione non autorizzata dei dati personali.

Gruppo di Lavoro Articolo 29 precisano che i titolari e i responsabili del trattamento devono pianificare anticipatamente e mettere in atto processi specifici per essere in grado di rilevare e limitare tempestivamente gli effetti di una violazione, valutare il rischio per le persone fisiche e stabilire se sia necessario notificare la violazione all'autorità di controllo competente e comunicarla alle persone fisiche interessate, ove necessario: dunque, la notifica all'autorità di controllo dovrebbe costituire parte del piano di intervento in caso di incidente[354].

Ciò significa, ad esempio, che il titolare deve conformare la propria organizzazione interna in modo da poter rilevare le violazioni, anche formando il proprio personale affinché le riconosca: può essere importante per il titolare, dotarsi di una *policy* interna che istruisca il personale sui passaggi da seguire per intervenire rapidamente, mitigando sin da subito i pregiudizi conseguenti alla violazione e interessando immediatamente gli organi aziendali più esperti per gestire la stessa.

Il GDPR delinea alcune tipologie di eventi che determinano violazione dei dati personali: a) distruzione dei dati, quando gli stessi non esistono più o non esistono più in una forma che sia di qualche utilità per il titolare del trattamento; b) perdita dei dati personali, quando i dati potrebbero comunque esistere, ma il titolare del trattamento ne ha perso il controllo o l'accesso, oppure non ne ha più il possesso; c) trattamento non autorizzato o illecito, che includere la divulgazione di dati personali o l'accesso da parte di destinatari non autorizzati a ricevere, oppure qualsiasi altra forma di trattamento in violazione del regolamento[355].

Effetto delle violazioni di dati personali è che il titolare non è più in grado di garantire l'osservanza dei principi relativi al trattamento di cui al GDPR.

Come osservato dalle Linee Guida del Gruppo di Lavoro Articolo 29, gli effetti negativi della violazione possono essere potenzialmente diversi e numerosi: danni fisici, danni di tipo materiale o immateriale (ad esempio perdita del controllo da parte degli utenti sui loro dati personali), limitazione dei diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonomizzazione, pregiudizio alla reputazione e perdita di riservatezza dei dati personali protetti da segreto professionale, nonché qualsiasi altro danno economico o sociale significativo alle persone fisiche interessate.

Laddove i rischi siano effettivamente alti, il GDPR prevede il coinvolgimento dell'Autorità di

---

[354] Linee Guida Gruppo di Lavoro Articolo 29 adottate il 6.2.2018, *Linee guida sulla notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679*, ove si evidenzia che "*qualsiasi piano di risposta alle violazioni dovrebbe mirare a proteggere le persone fisiche e i loro dati personali. Di conseguenza, la notifica della violazione dovrebbe essere vista come uno strumento per migliorare la conformità in materia di protezione dei dati personali*".

[355] Nella prassi, si suole distinguere in: "violazione della riservatezza", in caso di divulgazione dei dati personali o accesso agli stessi non autorizzati o accidentali; "violazione dell'integrità", in caso di modifica non autorizzata o accidentale dei dati personali; "violazione della disponibilità", in caso di perdita, accesso o distruzione accidentali o non autorizzati di dati personali.

controllo, imponendo al titolare del trattamento di notificare le violazioni (fatta salva l'ipotesi di improbabilità che la violazione presenti il rischio che si verifichino i precitati effetti negativi), nonché di comunicare la violazione alle persone fisiche interessate non appena ciò sia ragionevolmente possibile[356].

È necessario che il titolare sia in grado di identificare una violazione di dati personali, di valutare il rischio per le persone fisiche e, di conseguenza, di effettuare la notifica se necessario. Il Considerando n. 87 del GDPR afferma la necessità di verificare "se siano state messe in atto tutte le misure tecnologiche e organizzative adeguate di protezione per stabilire immediatamente se c'è stata violazione dei dati personali e informare tempestivamente l'autorità di controllo e l'interessato", e che "è opportuno stabilire il fatto che la notifica sia stata trasmessa senza ingiustificato ritardo, tenendo conto in particolare della natura e della gravità della violazione dei dati personali e delle sue conseguenze e effetti negativi per l'interessato. Siffatta notifica può dar luogo a un intervento dell'autorità di controllo nell'ambito dei suoi compiti e poteri previsti dal presente regolamento".

Di conseguenza, il titolare del trattamento deve predisporre procedure interne per poter rilevare una violazione e porvi rimedio. Le Linee Guida del Gruppo di Lavoro Articolo 29 prevedono, ad esempio, che per rilevare talune irregolarità nel trattamento dei dati, il titolare o il responsabile del trattamento "*può utilizzare alcune misure tecniche certe come il flusso di dati e gli analizzatori di registri, dai quali è possibile definire eventi e allerte correlando qualsiasi dato di registro. È importante che quando viene rilevata una violazione, la stessa venga segnalata al livello superiore appropriato di gestione, in maniera da poter essere trattata e, se del caso, notificata in conformità all'articolo 33 e, se necessario, all'articolo 34*".

Queste misure organizzative e meccanismi di segnalazione interni vengono generalmente dettagliati nei piani di intervento (policy) del titolare per il caso di incidente e/o nei dispositivi di governo societario. Ciò dovrebbe consentire al titolare di pianificare in maniera efficace e di stabilire chi ha la responsabilità operativa all'interno dell'organizzazione per la gestione di una violazione, nonché le modalità o l'opportunità di segnalare un incidente al livello gerarchico superiore, se del caso. Come ulteriori misure di sicurezza, il titolare del trattamento dovrebbe, inoltre, disporre di accordi con i responsabili del trattamento ai quali fa ricorso, i quali hanno a loro volta l'obbligo di notificare al titolare del trattamento eventuali violazioni.

L'art. 33, par. 3, stabilisce il contenuto minimo della notifica della violazione, prevedendo che essa

---

[356] In particolare, l'articolo 33, par. 1, stabilisce che "*in caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo*".

debba:

a) descrivere la 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;
b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
c) descrivere le probabili conseguenze della violazione dei dati personali;
d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Oltre alla notifica all'autorità di controllo, l'art. 34, par. 1, stabilisce che "quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo". Il par. 3 dell'art. 34 fissa tre condizioni in presenza delle quali non è necessaria la comunicazione agli interessati, ossia:

1. il titolare del trattamento ha applicato misure tecniche e organizzative adeguate per proteggere i dati personali prima della violazione, in particolare misure atte a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi. Ciò potrebbe prevedere ad esempio la protezione dei dati personali con cifratura allo stato dell'arte oppure mediante tokenizzazione;
2. immediatamente dopo una violazione, il titolare del trattamento ha adottato misure destinate a garantire che non sia più probabile che si concretizzi l'elevato rischio posto ai diritti e alle libertà delle persone fisiche. Ad esempio, a seconda delle circostanze del caso, il titolare del trattamento può aver immediatamente individuato e intrapreso un'azione contro il soggetto che ha avuto accesso ai dati personali prima che questi fosse in grado di utilizzarli in qualsiasi modo. È necessario altresì tenere in debito conto delle possibili conseguenze di qualsiasi violazione della riservatezza, anche in questo caso, a seconda della natura dei dati in questione;
3. contattare gli interessati richiederebbe uno sforzo sproporzionato, ad esempio nel caso in cui i dati di contatto siano stati persi a causa della violazione o non siano mai stati noti.

Da questo quadro normativo emerge che non appena il titolare del trattamento viene a conoscenza di una violazione, è fondamentale che non si limiti a contenere l'incidente, ma valuti anche il rischio che potrebbe derivarne per i diritti e le libertà degli interessati.

Infatti, solo valutando adeguatamente tale rischio il titolare potrà, innanzitutto, porre in essere le

misure adeguate al fine di contenere la violazione e, in secondo luogo, verificare se è necessaria la notifica all'Autorità di controllo e la comunicazione agli utenti.

Anche in questo ambito è perciò fondamentale svolgere una specifica analisi del rischio, che deve essere individuato e quantificato adeguatamente.

L'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA) ha elaborato raccomandazioni in merito a una metodologia di valutazione della gravità di una violazione, che possono essere utili per i titolari del trattamento e i responsabili del trattamento nella progettazione del loro piano di risposta per la gestione delle violazioni[357].

Con l'utilizzo di tale metodologia il titolare del trattamento è guidato attraverso il processo da specifici criteri quantitativi per effettuare una valutazione complessiva del rischio privacy.

I tre principali criteri presi in considerazione dall'ENISA e che devono essere utilizzati dal titolare durante la valutazione della gravità di una violazione dei dati personali sono:

Contesto di elaborazione dei dati (DPC): criterio che valuta il tipo di dati violati, insieme ad altri fattori legati al contesto complessivo in cui il trattamento è effettuato. È il criterio centrale che calcola la "criticità complessiva"[358].

Facilità di identificazione degli interessati (EI): criterio che determina la facilità con cui è possibile dedurre l'identità degli interessati coinvolti nella violazione. Corregge, in aumento o diminuzione, la "criticità complessiva", dunque EI è un fattore correttivo del DPC[359].

---

[357] ENISA, *Recommendations for a methodology of the assessment of severity of personal data breaches*, Dicembre 2013. L'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA) ha esaminato le attuali misure e procedure negli Stati membri dell'UE in materia di violazioni dei dati personali e pubblicato nel 2011 uno studio sull'attuazione tecnica dell'art. 4 della Direttiva ePrivacy, che includeva raccomandazioni su come pianificare e prepararsi alle violazioni dei dati, come rilevare e valutarli, come informare le persone e le autorità competenti e come rispondere ai dati violazioni. È stata inoltre proposta una metodologia per la valutazione della gravità della violazione dei dati personali incluso in allegato alle suddette raccomandazioni, che tuttavia non è stato considerato sufficientemente maturo per essere utilizzato a livello nazionale dalle diverse Autorità per la protezione dei dati.

In questo contesto, le autorità per la protezione dei dati di Grecia e Germania in collaborazione con l'ENISA ha sviluppato, sulla base del lavoro sopra menzionato, una metodologia aggiornata per i dati valutazione della gravità della violazione che può essere utilizzata sia dalle autorità di protezione dei dati che dai responsabili del trattamento.

[358] Le Raccomandazioni Enisa definiscono nello specifico le modalità di calcolo per definire i punteggi dei singoli criteri, offrendo numerosi esempi per orientare l'attività dell'interprete.

Per definire il punteggio DPC, il titolare del trattamento deve seguire un procedimento articolato in 2 fasi. Nella prima fase è necessario definire e classificare la tipologia di dati personali (le tipologie di dati sono precisate nell'Allegato 1 delle Raccomandazioni Enisa); nella fase successiva, modifica il punteggio ottenuto seguendo una scala di fattori (es. quantità di dati, caratteristiche particolari dei titolari o delle persone fisiche, invalidità/inesattezza di dati, disponibilità al pubblico prima della violazione, natura dei dati).

[359] La facilità di identificazione (EI) valuta quanto sarà facile per l'autore della violazione abbinarli univocamente a una determinata persona. Ai fini di questa metodologia vengono definiti quattro livelli di EI (trascurabile, limitato, significativo e massimo): il punteggio più basso è dato quando la possibilità di identificare l'individuo è trascurabile, il che significa che è estremamente difficile abbinare i dati a un individuo, ma comunque potrebbe essere possibile in

Circostanze di violazione (CB): criterio che affronta e quantifica le circostanze specifiche della violazione, che possono o meno essere presenti (ad es. perdita di sicurezza dei dati, coinvolgimento di terzi, ecc.). Tale criterio può, dunque, solo aumentare la "criticità complessiva"[360].

Il risultato ottenuto dalla combinazione dei criteri sopra esposti[361] determina un punteggio che viene rapportato ad una scala suddivisa in quattro intervalli di valori, corrispondenti a quattro livelli di gravità della violazione e degli effetti pregiudizievoli per gli interessati (basso, medio, alto, molto alto.

In questo modo, il titolare ottiene una "quantificazione" numerica del rischio, necessaria in primo luogo per valutare la necessità procedere alla notifica all'Autorità di controllo e alla comunicazione agli interessati, nonché per valutare le procedure di mitigazione dei rischi più opportune da intraprendere.

Così operando, il titolare può, inoltre, evitare che si verifichino danni per gli interessati o limitare l'aggravamento di quelli già prodottisi.

7. Integrazione della gestione del rischio *privacy* nell'organizzazione

Da quanto esposto nei paragrafi precedenti emerge che la gestione del rischio privacy dovrebbe essere applicata all'intera organizzazione del titolare, a tutte le aree e livelli, così da considerare tutte le specifiche attività di trattamento.

Sarà essenziale per il titolare dotarsi di un *modello organizzativo privacy*, che descriva compiutamente tutto il sistema approntato per la gestione dei trattamenti di dati. Questo modello dovrà contenere le procedure formalizzate dal titolare per la gestione dei processi che involgono dati personali, le linee guida e gli eventuali codici di condotta adottati dal titolare per garantire il rispetto del GDPR, le *policy* interne per garantire la sicurezza dei trattamenti e le linee guida da seguire immediatamente nel caso in cui si verifichi la violazione dei dati; il modello dovrebbe dettare le condizioni specifiche per l'esecuzione delle eventuali valutazioni d'impatto e descrivere quelle che sono state già eseguite, con i relativi risultati; esso conterrà, dunque, la mappatura di tutti i processi, la valutazione dei rischi, l'elenco delle misure di sicurezza previste per la mitigazione degli stessi;

---

determinate condizioni; viene indicato il punteggio più alto quando l'identificazione è possibile direttamente dai dati violati.

[360] Questo criterio valuta e quantifica effetti pregiudizievoli che possono conseguire alla violazione, ossia: perdita di riservatezza (l'entità della perdita varia in base all'ambito di divulgazione, al potenziale numero e tipo di soggetti che potrebbe avere illegittimamente accesso alle informazioni); perdita di integrità: la perdita di integrità (la situazione più grave si verifica quando ci sono gravi possibilità che i dati alterati siano stati utilizzati in un modo che potrebbe danneggiare l'individuo); perdita di disponibilità (che può essere momentanea o permanente); eventuale coinvolgimento doloso di terzi (es. furto o pirateria informatica).

[361] Attraverso la seguente formula: SE = DPC x EI + CB

dovrà tenere conto del rispetto degli obblighi di formazione dei dipendenti e delle persone che effettuano trattamento di dati; dovrà dar conto dell'esistenza di eventuali contitolari e responsabili e delle misure di sicurezza adottate nell'esternalizzazione dei trattamenti.

Questo *modello organizzativo privacy* costituisce un presidio di *accountability* e consentirà al titolare di poter dimostrare all'Autorità di controllo l'adempimento degli obblighi previsti dal GDPR: infatti, sebbene si tratti di un documento riservato, esso verrà messo a disposizione del Garante in caso di richiesta o di ispezione.

Inoltre, l'adozione di una struttura formalizzata per garantire il rispetto del GDPR consente al titolare di dimostrare l'eventuale non imputabilità di eventuali danni in caso di trattamenti illeciti. Ad esempio, il titolare potrà dimostrare con più facilità di aver adottato tutte le misure di sicurezza più adeguate e che l'evento dannoso è stato prodotto da terzi, senza che fosse possibile, secondo una valutazione prognostica, evitare tale evento. Egli potrà così dimostrare di aver adottato ogni precauzione, con la massima diligenza pretendibile nel caso specifico, per individuare i rischi e per gestirli adeguatamente, provando così che l'evento è esterno alla propria sfera di controllo.

Per essere realmente efficace, inoltre, la gestione dei rischi privacy dovrebbe essere parte integrante del più ampio sistema di gestione dei rischi aziendali (dunque, non solo quelli relativi alla protezione dei dati).

Il *modello organizzativo privacy* può essere, innanzitutto, integrato nel sistema di gestione ex d.lgs. n. 231/2001, ossia quell'insieme di regole, procedure e modalità operative che definiscono il sistema organizzativo, di gestione e controllo interno di un'azienda, e che viene adottato allo scopo di prevenire e impedire la commissione, da parte degli amministratori o dipendenti, dei reati sanzionati dal d.lgs. n. 231/2001, tra i quali compaiono anche i delitti informatici (art. 24-*bis*).

Inoltre, il *modello* di gestione dei rischi privacy può essere integrato all'interno dei "sistemi di gestione", come i sistemi previsti dalle norme ISO. Ci si riferisce, in particolare, alle norme ISO 9001-Gestione della qualità e ISO 27001 – Sicurezza delle informazioni.

Le procedure formalizzate per la gestione dei trattamenti di dati potranno, dunque, essere inserite all'interno di questi più ampi sistemi, così da divenire parte complementare ed essenziale dell'organizzazione del titolare, per assolvere all'obbligo di *accountability*. Evidente che tale integrazione sarà uno strumento fondamentale per dimostrare la conformità della condotta del titolare al principio di liceità del trattamento dettato dal GDPR[362].

---

[362] Nel caso di violazione del GDPR, l'aver adottato un *modello organizzativo privacy* è elemento che viene valorizzato dall'Autorità garante per determinare l'irrogazione di una sanzione più lieve. Infatti, l'art. 83 GDPR afferma che nell'irrogare la sanzione si tiene "debito conto" di alcuni elementi, tra cui "[…] *c) le misure adottate dal titolare del*

Con riferimento alle imprese di dimensioni ancora maggiori, il sistema di gestione dei dati personali dovrà essere integrato anche nel sistema dei controlli interni, laddove adottato[363].

I sistemi di controllo interno prevedono, tendenzialmente, che i controlli siano distribuiti su tre livelli di organizzazione[364], che dovranno dunque includere specifiche procedure di monitoraggio per la protezione e sicurezza dei dati:

- controlli di linea ("primo livello"), diretti ad assicurare il corretto svolgimento delle operazioni dell'impresa. Essi sono effettuati dalle stesse strutture operative (ad es., controlli di tipo gerarchico), anche attraverso unità dedicate esclusivamente a compiti di controllo, le quali riportano i risultati ai responsabili delle strutture operative[365]; per quanto possibile, essi dovrebbero essere incorporati nelle procedure informatiche, in modo da garantire l'automaticità. Le strutture operative sono le prime responsabili di attuare un efficace gestione dei rischi: nel corso dell'ordinaria operatività giornaliera, tali unità aziendali "*devono identificare, misurare o valutare, monitorare, attenuare e riportare i rischi derivanti dall'ordinaria attività aziendale in conformità con il processo di gestione dei rischi; esse devono rispettare i limiti operativi loro assegnati coerentemente con gli obiettivi di rischio e con le procedure in cui si articola il processo di gestione dei rischi*".
- controlli sui rischi e sulla conformità ("secondo livello"), che assicurano: 1) la corretta attuazione del processo di gestione dei rischi; 2) il rispetto dei limiti operativi assegnati alle varie funzioni; 3) la conformità dell'operatività aziendale alle norme, incluse quelle di autoregolamentazione. Le funzioni preposte ad eseguire i controlli di secondo livello devono essere distinte da quelle produttive; esse concorrono, inoltre, alla definizione delle politiche di governo dei rischi e del processo di gestione dei rischi;
- revisione interna ("terzo livello"), che ha la funzione di individuare le violazioni delle procedure e della regolamentazione nonché a valutare periodicamente "*la completezza, l'adeguatezza, la funzionalità (in termini di efficienza ed efficacia) e l'affidabilità del sistema dei controlli interni e del sistema informativo (ICT audit), con cadenza prefissata in relazione alla natura e all'intensità dei rischi*".

---

trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati; d) il grado di responsabilità del titolare del trattamento o del responsabile del trattamento tenendo conto delle misure tecniche e organizzative da essi messe in atto ai sensi degli articoli 25 e 32".

[363] In determinate ipotesi il legislatore impone l'adozione di un sistema formalizzato di controlli interni, prevedendone le caratteristiche generali. È il caso, ad esempio, delle Banche in Italia.

[364] Banca d'Italia, *Il sistema dei controlli interni*, Circolare n. 285, 17.12.2013.

[365] Possono essere, ad esempio, controlli sistematici o a campione.

8. *Duty of care* e prova liberatoria negli altri Stati UE

Sia con riferimento alla responsabilità di cui alla Dir. 95/46, sia in relazione a quella ex GDPR, la dottrina transazionale evidenzia che il titolare è soggetto a due tipi di obblighi: in certi casi si tratta di "*obligations that specify a* result *to be achieved (e.g. "personal data must be collected for legitimate purposes and not further processed in a way incompatible with those purposes")*"[366], in altre ipotesi, "*the obligations are specified as an obligation to make reasonable efforts to do something ("obligation of means")*"[367].

Si tratta di una classificazione sostanzialmente sovrapponibile alla distinzione tra obbligazioni di risultato e obbligazioni di mezzi, proposta da Mengoni[368] e coltivata da dottrina e giurisprudenza successive, la quale, tuttavia, risulta ora tendenzialmente superata dalla più recente giurisprudenza di legittimità[369].

Dunque, il titolare è assoggettato ad un *duty of care*, che viene interpretato come una "*obligation of means*", nel senso che il titolare non è obbligato a predisporre le misure tecniche e organizzative "perfette", ma solo quelle "adeguate" rispetto alla situazione e al contesto, peraltro tenendo conto dei costi di attuazione e dei rischi esistenti.

Si registrano tuttavia orientamenti contrastati sull'elemento soggettivo dell'illecito, in particolare ci si chiede se la colpa del titolare sia, o meno, presupposto della responsabilità.

Ad esempio, si discute se una violazione della sicurezza comporti sempre l'obbligo di risarcimento dei danni, oppure se è necessario che sia riscontrata anche una violazione al GDPR da parte del titolare: potrebbe essere il caso, ad esempio, di una società che ha organizzato in modo efficiente ed adeguato la propria struttura informatica, anche sotto il profilo della *cybersecurity*, ma che subisca un attacco hacker con sottrazione di dati a causa di una falla nel sistema di *firewall*, il cui mancato aggiornamento dipende da un responsabile esterno, scelto tra le società di sicurezza informatica più

---

366 B. VAN ALSENOY, *Liability under EU Data Protection Law. From Directive 95/46 to the General Data Protection Regulation*, op. cit.

367 B. VAN ALSENOY, *op. cit.*, l'autore pone i seguenti esempi: *"article 6.d provides that the controller must take "every reasonable step" to ensure that data which are inaccurate or incomplete shall be erased or rectified. Similarly, article 17 requires the controller to implement "appropriate" measures to ensure the confidentiality and security of processing. Finally, it should be noted that certain requirements necessitate a further assessment in light of the specific circumstances of the processing (e.g., whether or not personal data are "excessive" will depend inter alia on the purposes of the processing)".*

368 L. MENGONI, *Obbligazioni "di risultato" e obbligazioni "di mezzo",* in *Riv. dir. comm*., 1954, p. 185.

369 Infatti, le Sezioni Unite hanno affermato che la distinzione tra obbligazioni di mezzi e obbligazioni di risultato "*se può avere una funzione descrittiva, è dogmaticamente superata* […] *in realtà, in ogni obbligazione si richiede la compresenza sia del comportamento del debitore che del risultato, anche se in proporzione variabile, sicché molti Autori criticano la distinzione poiché in ciascuna obbligazione assumono rilievo così il risultato pratico da raggiungere attraverso il vincolo, come l'impegno che il debitore deve porre per ottenerlo*" (CASS., sez. un., 11.1.2008, n. 577).

prestigiose[370]. In questo caso, alla violazione di sicurezza non corrisponde alcuna violazione del Regolamento da parte del titolare.

Secondo una parte della dottrina europea, il titolare non dovrebbe essere considerato responsabile[371], in quanto vi sarebbe assenza di negligenza e la violazione di sicurezza sarebbe stata determinata da un fattore al di fuori della sfera di controllo del titolare. In particolare, si afferma che non si configura alcuna violazione del GDPR se la sicurezza dei dati è stata violata nonostante l'attuazione di misure adeguate. Dunque, in questo caso l'interessato non avrebbe diritto al risarcimento del danno, mancando un presupposto necessario, ossia la violazione dell'art. 32 GDPR. Il titolare può, infatti, delegare ad un responsabile l'attuazione delle misure di sicurezza informatiche; anzi, è tenuto a farlo quando deve predisporre misure di sicurezza particolarmente complesse che non è in grado di attuare autonomamente. Sicché la decisione di delegare ad un'impresa specializzata l'attuazione della *cybersecurity* è conforme, in taluni casi, al principio di responsabilizzazione.

Al contrario, taluni autori[372] affermano che il *duty of care* non sarebbe mai delegabile all'esterno ad un responsabile, con la conseguenza che la violazione imputabile al terzo deve necessariamente essere imputata, in via oggettiva, al titolare. Questo perché la Direttiva e il Regolamento pongono un dovere generale al titolare di assicurare la conformità del trattamento agli obblighi di legge e, infatti, il responsabile viene trattato, da entrambi i testi normativi, quasi alla stregua di un esecutore materiale delle istruzioni del titolare, sul quale continua a gravare un generale "*duty of care*", considerato non delegabile al responsabile.

La responsabilità del titolare per i trattamenti posti in essere dal responsabile viene accomunata, infatti, all'ipotesi del fatto illecito commesso dagli ausiliari o preposti dell'imprenditore (che

---

[370] L'esempio ricalca un caso tratto da P. T. J. WOLTERS, *The security of personal data under the GDPR: a harmonized duty or a shared responsibility?,* in *International Data Privacy Law,* Vol. 7, No. 3, pp. 165-178, saggio in cui l'autore analizza approfonditamente il meccanismo della prova liberatoria per il titolare.

Si evidenzia che esempi molto simili sono contenuti in B. VAN ALSENOY, *Liability under EU Data Protection Law. From Directive 95/46 to the General Data Protection Regulation*, op.cit; E. O'DELL, *Compensation for breach of the general data protection regulation* in *Dublin ULJ*, 2017, pp. 97-164; J. KNETSCH, *The compensation of non-pecuniary loss in GDPR infringement cases* in *Eur. J. Privacy L. & Tech.*, 2020, pp. 63-70. Sul tema si v. inoltre, A. MITRAKAS, *Assessing liability arising from information security breaches in data privacy,* op. cit., pp. 29-136; M. J. RADIN, *Compensation and commensurability* in *Duke LJ*, 1993, pp 56-86; M. N. LINTVEDT, *Putting a price on data protection infringement,* in *International Data Privacy Law,* Vol. 00, No. 0, 2021, pp. 1-15; A. S. BOHM-E. J. GEORGE-B. CYPHERS-S. LU, *Privacy and Liberty in an Always-on, Always-listening World*, op. cit*.,* 2017, pp. 1-45; B. WONG, *Problems with controller-based responsibility in EU data protection law,* in *International Data Privacy Law,* Vol. 11, No 4, 2021, pp. 375-387.

[371] P. T. J. WOLTERS, *op. cit.*

[372] B. VAN ALSENOY, *op. cit.* L'autore osserva che la Direttiva e il Regolamento pongono un dovere generale al titolare di assicurare la conformità del trattamento agli obblighi di legge e, infatti, il responsabile viene trattato, da entrambi i testi normativi, quasi alla stregua di un esecutore materiale delle istruzioni del titolare, sul quale continua a gravare un generale "*duty of care*", considerato non delegabile al responsabile. Dunque, il titolare continua a rimanere il principale responsabile per i trattamenti illeciti posti in essere dal responsabile e non può andare esente da responsabilità, nei confronti del danneggiato, dimostrando di non avere colpa nella scelta o supervisione del responsabile.

configura un'ipotesi speciale di responsabilità aquiliana anche nel nostro ordinamento), che è codificato nei principi del diritto extracontrattuale europeo (PETL) Infatti, l'art. 6:102 dei *Principles of European Tort Law* (PETL), rubricato "*Liability for auxiliaries*", così recita: "*A person is liable for damage caused by his auxiliaries acting within the scope of their functions provided that they violated the required standard of conduct*"[373]. Si tratterebbe, dunque, di una responsabilità a titolo di rischio "d'impresa" o "organizzativo", derivante dall'inadempimento ad un'obbligazione di mezzi.

Altri autori sostengono che la responsabilità può essere evitata se il titolare del trattamento dimostra che la violazione della sicurezza è causata dalle azioni di un terzo, come un hacker[374], in quanto saremmo nell'ipotesi di un fatto non imputabile alla sfera di controllo del titolare[375]. Nell'esempio descritto, il danno sarebbe dipeso da un errore dello sviluppatore di *firewall*, che è stato accuratamente selezionato dal titolare, con la conseguenza che nessuna violazione dovrebbe essere imputata al titolare.

In ogni caso, la tesi che appare più coerente con lo spirito del GDPR è quella secondo cui, nei confronti del danneggiato, il titolare non può in alcun modo sottrarsi a colpa, anche nel caso in cui dimostrasse che l'evento dannoso è imputabile esclusivamente al responsabile, senza che vi sia stata alcuna violazione del GDPR da parte del titolare.

In questo senso, la responsabilità viene definita oggettiva, perlomeno nei confronti del danneggiato, il quale si verrebbe a trovare, di conseguenza, in una posizione di vantaggio anche quando il danno sia stato causato interamente dal responsabile, per negligenza e nelle ipotesi di dolo[376]. Tuttavia, in queste ipotesi, il titolare non in colpa che abbia risarcito interamente la vittima può agire nei confronti

---

[373] Il modello di responsabilità della disciplina sulla protezione dei dati è ispirato anche ai principi del diritto extracontrattuale europeo (PETL), ed infatti talune innovazioni rispetto alla disciplina previgente costituiscono una sorta di codificazione di principi generali del PETL (B. VAN. ALSENOY, *Liability under EU Data Protection Law. From Directive 85/46 to the General Data Protection Regulation,* op. cit., in cui l'autore pone a confronto le due discipline).

[374] P. LAROUCHE-M. PEITZ-N. PURTOVA*, Consumer privacy in network industries. A CERRE Policy Report*, CERRE, 2016, p. 57.

[375] M. THOMPSON, *'Beyond Gatekeeping: The Normative Responsibility of Internet Intermediaries*, in *Vand J. Ent. & Tech L.*, 2016, Vol. 18:4, pp. 783 ss.

[376] R. STRUGAŁA, *Art. 82 GDPR: strict liability or liability based on fault?,* in *European Journal of Privacy Law & Technologies Special issue*, pp. 71-79. L'Autore si sofferma sulla rilevanza della colpa all'interno della responsabilità da illecito trattamento di dati, osservando che non è chiaro se questa responsabilità sia basata sulla colpa oppure se sia puramente oggettiva, circostanza che comporterebbe l'accertamento della responsabilità indipendentemente da qualsiasi tipo di colpa da parte del titolare o del responsabile del trattamento. Questi dubbi derivano anche dalle differenti versioni linguistiche del Regolamento. Osserva, infatti, che "*whereas the majority of the language versions use the formula, according to which the controller and processor may be exempt from liability if they prove that they are „not in any way responsible for the event giving rise to the damage", the Polish version dictates that the exemption comes into play where the controller or processor prove not to be at fault*".

del responsabile per l'intero risarcimento[377].

9. Il danno materiale e immateriale

La risarcibilità dei danni non patrimoniali per illecito trattamento dei dati era espressamente prevista dalla l. 675/1996, nonché dall'art. 15 cod. privacy; ora l'art. 82, par. 1, prevede espressamente la risarcibilità del danno materiale e di quello "immateriale".

La previsione di cui all'art. 15 cod. privacy si è resa necessaria onde garantire la risarcibilità dei danni di natura non patrimoniale: la formulazione dell'art. 2059 c.c. consente, infatti, la risarcibilità dei danni non patrimoniali nei soli casi previsti dalla legge. In assenza di una previsione come quella di cui al citato art. 15, non vi sarebbe stato alcun ristoro di tale danno, non costituendo il trattamento illecito un reato.

Com'è noto, peraltro, il danno ad un diritto personale dell'individuo, quale il diritto alla *privacy* e alla protezione dei dati, determina tipicamente un danno di tipo non patrimoniale, consistente, ad esempio, nelle sofferenze psichiche patite dal danneggiato a seguito della lesione; pertanto, sarebbe stata del tutto inadeguata una disciplina di protezione dei dati che non consentisse la risarcibilità di questo tipo di danno.

Prima di procedere all'analisi dei profili di risarcibilità del danno non patrimoniale conseguente ad illecito trattamento di dati personali, è opportuno ripercorrere sinteticamente la tormentata evoluzione giurisprudenziale in merito alla costruzione di uno statuto del danno non patrimoniale in generale (lungi dal potersi dire, comunque, definitivamente consolidato). Gli esiti di questo percorso hanno evidente influenza diretta anche sulla responsabilità per illecito trattamento dei dati; si ribadisce, comunque, che l'origine europea del GDPR imporrà di considerare, nella definizione dei danni effettivamente risarcibili, anche gli orientamenti della Corte di giustizia e della dottrina transazionale.

Con riferimento al percorso evolutivo in tema di danno non patrimoniale, è doveroso, in prima battuta, evidenziare i passi realizzati per giungere alla moderna lettura assiologica, costituzionalmente orientata, che ha permesso di abbandonare i limiti imposti dall'art. 2059 c.c. correlati all'accertamento

---

[377] *Cfr.* B. VAN ALSENOY, *op. cit.*, "*the standard of care incumbent upon the processor may, however, be informed by the contract between controller and processor. In any event, the controller who has been held liable by the data subject, should be able to claim back the damages from the processor on the basis of the contract between them*". L'autore analizza anche il caso in cui il responsabile abbia intenzionalmente agito violando le istruzioni impartite dal titolare. In questa ipotesi, il responsabile viene considerato titolare del trattamento in quanto determina autonomamente le finalità del trattamento; tuttavia, il titolare originario non potrà comunque andare esente da responsabilità dimostrando che il responsabile ha violato le istruzioni, nemmeno se dimostra la totale assenza di colpa nella scelta e supervisione del responsabile.

di un reato[378].

Le tappe fondamentali di tale percorso giurisprudenziale sono state: *i*) l'intervento delle sentenze gemelle della Cassazione del 2003[379] (confermate dalla Corte Costituzionale[380]), *ii*) la successiva reinterpretazione offerta dalle decisioni gemelle di San Martino del 2008, *iii*) il recente decalogo di controriforma ad opera della Terza Sezione civile della Cassazione del 2018.

Con le sentenze gemelle della Cassazione del 2003 viene inaugurato il superamento dell'orientamento tradizionale che identificava il danno non patrimoniale con il solo danno morale soggettivo.

Le citate sentenze gemelle, dall'un lato, hanno ridotto l'ambito di operatività dell'art. 2059 c.c. circoscrivendolo unicamente al danno morale soggettivo (incidente, questo, sulla sfera psichica del danneggiato e determinate un ingiusto turbamento del suo stato d'animo); dall'altro lato, hanno evidenziato una nuova figura di danno non patrimoniale, il danno biologico, ovverosia il danno conseguente alla lesione dell'integrità psico-fisica della persona[381].

Il danno biologico, pertanto, viene sottratto dall'ambito di operatività dell'art. 2059 c.c. e, in particolare, dai limiti derivanti dalla riserva di legge ivi prevista, per essere ricondotto nell'alveo della risarcibilità di cui all'art. 2043 c.c.

Sulla scorta dell'interpretazione della Corte Costituzionale, il danno biologico viene successivamente ricondotto all'interno del perimetro di operatività dell'art. 2059 c.c., non in quanto coincidente con il danno morale soggettivo ma poiché con quest'ultimo condivide la categoria di appartenenza, ossia la categoria – giuridicamente unitaria – del danno non patrimoniale. Trattasi, pertanto, di specie diverse di un unico genere.

Le sentenze gemelle della Cassazione hanno il pregio, comunque, di aver portato alla luce la distinzione tra *danno evento* – consistente nella lesione del diritto in sé e per sé considerata – e *danno conseguenza* – da identificarsi nei concreti effetti pregiudizievoli della lesione del diritto.

Come anticipato, la lettura offerta dalla Corte di Cassazione ha trovato conferma da parte della Corte Costituzionale che, con sentenza n. 223/2003, delinea una tripartizione del danno alla persona

---

[378] Il richiamo di tale disposizione ai "*casi previsti dalla legge*" veniva, infatti, limitato esclusivamente all'art. 185 c. p., con il risultato che unicamente ai danni di natura non patrimoniale derivanti dalla commissione di un fatto di reato veniva accordata, se del caso, tutela risarcitoria.

[379] CASS., 31.5.2003, n. 8827; CASS., 31.5.2003, n. 8828, in *Resp. civ. e prev*., 2003, p. 675, con note di P. CENDON, *Anche se gli amanti si perdono l'amore non si perderà. Impressioni di lettura su Cass., 8828/2003*; E. BERGELLI, *Danno non patrimoniale ed interpretazione costituzionalmente orientata dell'art. 2059*; P. ZIVIN, *E poi non rimase nessuno*; nonché in *Danno resp*., 2003, p. 816, con note di F. D. BUSNELLI, *Chiaroscuri di estate. La Corte di Cassazione e il danno alla persona*; G. PONZANELLI, *Ricomposizione dell'universo non patrimoniale: le scelte della Corte di Cassazione*.

[380] CORTE COST., 11.6.2003, n. 223, in *Rass. dir. civ*., 2003, pp. 770 ss., con nota di G. PERLINGIERI., *L'art. 2059 c.c.: uno e bino: una interpretazione che non convince*.

[381] CORTE COST., 14.7.1086, n. 184, in *Foro it*., 1986, I, c. 2053 ss., sulla scorta dell'elaborazione dottrinale di R. SCOGNAMIGLIO, *Il danno morale. Contributo alla teoria del danno extracontrattuale*, in *Riv. dir. civ.,* 1957, I, pp. 277 ss.

riconducibile alla categoria del danno non patrimoniale. Precisamente *i) danno morale*, consistente nel turbamento psichico della persona danneggiata; *ii) danno biologico*, rappresentato dalla lesione dell'integrità psicofisica della persona danneggiata; *iii) danno esistenziale* della persona, ravvisabile nella lesione di interessi di rango costituzionale della persona danneggiata[382].

Ben presto, però, di fronte ad un confuso proliferare di decisioni difformi in punto di riconoscimento del danno esistenziale quale autonoma categoria di danno, si è reso quantomai doveroso un intervento chiarificatore da parte della Corte di Cassazione a Sezioni Unite.

Con l'intervento del 2008 (c.d. sentenze gemelle di San Martino[383]), le Sezioni Unite hanno provveduto ad individuare con precisione quali fossero le lesioni meritevoli di ristoro, ossia quali tra queste fossero effettivamente inerenti a diritti inviolabili della persona. Si erano profilati, infatti, notevoli dubbi circa l'identificazione della nozione di interessi e, quindi, delle situazioni giuridiche azionate, con tutti i rischi, poi, di proliferazione delle voci di danno[384].

La giurisprudenza di legittimità del 2003 aveva, infatti, omesso di considerare una notevole differenza: e cioè, aveva finito impropriamente per attribuire rilevanza costituzionale non ai diritti o agli interessi della persona, ma al danno (il c.d. *danno conseguenza*), dovendosi, all'opposto, vagliare la rilevanza costituzionale con riferimento al diritto fondamentale della persona leso da una condotta offensiva (ossia al c.d. *danno evento*)[385].

La lettura del danno non patrimoniale delineata nel 2008, legata alla violazione di un diritto inviolabile della persona di spessore costituzionale, non è rimasta comunque esente da critiche: in

---

[382] Tale categoria ha suscitato accesi dibattiti e opinioni contrastanti. La dottrina, sul punto, si mostra divisa tra chi è favorevole a riconoscere autonoma configurabilità al tale tipologia di danno e chi, all'opposto, la nega. Si vedano, tra i primi, P. CENDON-P. ZIVIZ, *Risarcimento del danno esistenziale*, Giuffrè, 2003; tra i secondi, G. PONZANELLI, *Il risarcimento integrale senza danno esistenziale*, Cedam, 2007. In giurisprudenza, a favore di una configurabilità autonoma del danno esistenziale: CASS., sez. un., 2.3.2006, n. 6572, in *Foro it*., 2006, 5, c. 1343 ss.; CASS., 12.6.2006, n. 13546, in *Dir. Fam. Pers*., 2007, 1, pp. 93 ss. Si vedano *contra*: CASS., 15.7.2005, n. 15022, in *Foro it*., 2006, 5, c. 1344; CASS., 9.11.2006, n. 23918; CASS., 20.4.2007, n. 9510; CASS., 27.6.2007, n. 14846.

[383] CASS., sez. un., 11.11.2008, n. 26972, n. 26973, n. 26974 e n. 26975, in *Riv. dir. civ*., 2009, II, p. 97, con nota di F. D. BUSNELLI, *Le sezioni unite e il danno non patrimoniale*; in *Giur. it*., 2009, p. 259; con nota di G. CASSANO, *Danno non patrimoniale ed esistenziale: primissime note critiche a Cassazione civile, Sezioni Unite, 11 novembre 2008, n. 25972;* in *Giur. it.,* 2009, p. 317; con nota di V. TOMARCHIO, *L'unitarietà del danno non patrimoniale nella prospettiva delle Sezioni unite*; in *Resp. civ. e prev*., 2009, p. 38; con note di P.G. MONATERI, *Il pregiudizio esistenziale come voce del danno non patrimoniale*; E. NAVARRETTA, *Il calore della persona nei diritti inviolabili e la complessità dei danni non* patrimoniali; D. POLETTI, *La dualità del sistema risarcitorio e l'unicità della categoria dei danni non patrimoniali*; P. ZIVIZ, *Il danno non patrimoniale: istruzioni per l'uso*.

[384] Sulla scorta di CASS., sez. un., 11.11.2008, n. 26972, cit., "*è compito del giudice accertare l'effettiva consistenza del pregiudizio allegato, a prescindere dal nome attribuitogli, individuando quali ripercussioni negative sul valore-uomo si siano verificate e provvedendo alla loro integrale riparazione*".

[385] In altri termini, la ricostruzione elaborata nel 2003 confondeva il piano del pregiudizio da riparare con quello dell'ingiustizia da dimostrare. Il danno è unicamente da intendersi come la conseguenza logica della violazione/lesione di un diritto o interesse della persona meritevole di tutela.

base a questa, infatti, restava comunque sguarnita di protezione la categoria dei diritti fondamentali costituzionalmente protetti a rilevanza economica, quali – per esempio – il diritto di proprietà, il diritto di iniziativa economica privata, o ancora, i danni conseguenti alla violazione del diritto alla concorrenza[386].

È stato rilevato, correttamente, come sarebbe del tutto inaccettabile che l'art. 2059 c.c. venisse inteso come norma discriminatrice tra interessi della persona e relativi danni.

Invero, dovrebbe considerarsi "*norma che consente il risarcimento del danno non patrimoniale oltre che nei casi previsti, in cui l'ingiustizia è già tipizzata, anche in quelli non tipizzati, rispetto ai quali dovrebbe pur sempre rimanere possibile la valutazione dell'ingiustizia ex art. 2043 c.c.*"[387].

Con l'intervento delle sentenze di San Martino, le Sezioni Unite del 2008 hanno delineato la categoria di danno non patrimoniale quale categoria unitaria, relegando alle sottocategorie del danno biologico, morale ed esistenziale un ruolo semplicemente descrittivo. La finalità espressa – si ribadisce – è quella di evitare indebite duplicazioni risarcitorie e risarcimenti di danni bagatellari[388].

Il danno alla persona viene così collocato all'interno un sistema bipolare: gli artt. 2043 c.c. e 2059 c.c. costituiscono il referente normativo per il risarcimento dei danni di natura, rispettivamente, patrimoniale e non patrimoniale, questi ultimi da considerarsi complessivamente[389].

---

[386] Con riferimento a tale lettura "chiusa" del danno non patrimoniale alla persona, in senso critico si vedano: F. D. BUSNELLI, *Le Sezioni Unite e il danno non patrimoniale*, in *Riv. dir. civ*., 2009, pp. 105 ss.; V. SCALISI, *Danno alla persona e ingiustizia*, in *Riv. dir. civ*., 2007, pp. 152 ss.; ID., *Illecito civile e responsabilità: fondamento e senso di una distinzione*, in *Riv. dir. civ*., 2009, pp. 657 ss.; C. SCOGNAMIGLIO, *Il sistema del danno non patrimoniale dopo le decisioni delle Sezioni Unite*, in *Resp. civ. prev*. 2009, pp. 261 ss. e pp. 266 ss.;

[387] V. SCALISI, *Danno alla persona e ingiustizia*, cit., pp. 152 ss.; D. BUSNELLI, *Le Sezioni Unite e il danno non patrimoniale*, cit., pp. 105 ss.

[388] Le citate sentenze di San Martino hanno censurato il fenomeno esponenziale delle c.d. liti bagatellari, ovverosia le cause risarcitorie in cui il danno consequenziale *i)* è futile o irrisorio, *ii)* ovvero, pur essendo oggettivamente serio, è tuttavia, secondo la coscienza sociale, non grave ma insignificante o irrilevante per il livello raggiunto. In realtà, non può non farsi notare la contraddizione in termini contenuta nell'elaborazione di un principio di diritto che contempli la lesione di un diritto fondamentale come bagatellare: tale valutazione non potrà certo incidere sull'*an debeatur* – posto che non può ammettersi la lesione di un diritto fondamentale dotato di copertura costituzionale né insignificante né futile – ma semmai sul *quantum debeatur*, dunque sul solo piano liquidatorio, ammettendosi, così, una quantificazione limitata dal punto di vista della monetizzazione del disagio della persona conseguente alla lesione del diritto fondamentale. Così, E. TOSI, *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale*, Giuffrè 2019, pp. 207 ss.; nello stesso senso, F. QUARTA, *Risarcimento e sanzione nell'illecito civile*, Esi, 2013, pp. 127 ss.; analoghe perplessità in G. CONTE, *Il difficile equilibrio tra l'essere e l'avere: considerazioni critiche sulla nuova configurazione del danno non* patrimoniale, in *Giur. It.,* 2009, pp. 1030 ss.

[389] I principi di diritto sanciti con l'intervento del 2008 della Corte di Cassazione (sentenze di San Martino) hanno trovato conferma anche in CASS., sez. un., 16.2.2009, n. 3677, con riferimento ad una fattispecie di danno non patrimoniale derivante da illegittimo licenziamento. Nella citata sentenza viene delineato un modello in cui l'area del danno non patrimoniale viene identificata con quella del danno "morale" in senso lato. Viene ribadito che la categoria del danno non patrimoniale è unitaria, dividendosi l'area tra danno patrimoniale e danno non patrimoniale. Viene specificato altresì che il danno morale è risarcibile nei casi stabiliti dalla legge (dal codice penale e dalle leggi speciali) nonché nei casi di

Nel solco della lettura giurisprudenziale già avviata nel 2003, viene confermata la non configurabilità di un danno in *re ipsa*, risarcibile per il sol fatto che venga dimostrata la mera lesione del diritto, e, conseguentemente, evidenziata la rilevanza che deve assumere, all'opposto, il pregiudizio effettivo ed obbiettivamente apprezzabile conseguenza della lesione del diritto stesso[390]. Peraltro, con l'arresto del 2008, è stato chiarito che anche la lesione di un diritto fondamentale della persona può essere qualificato bagatellare in mancanza del superamento del c.d. "doppio filtro di ammissibilità"[391].

Altresì il quadro delineato dalle sentenze di San Martino è stato oggetto di osservazioni critiche. Concependo la liquidazione del danno non patrimoniale in modo unitario, comprometteva, rispetto al danno biologico, il danno morale soggettivo: ovverosia, quella sofferenza interiore, non quantificabile sulla base di perizia medico legale, nei casi previsti dalla legge (si pensi all'art. 82, comma 3, GDPR) oppure ammesso al ricorrere di una lesione di diritti fondamentali tutelati dalla Costituzione.

È dato, dunque, accolto con favore l'intervento della Terza Sezione Civile della Cassazione del 27.3.2018 – il c.d. *decalogo* nomofilattico *de facto*[392] – tramite il quale viene rivalutata la peculiarità

---

violazione di calori della persona costituzionalmente protetti. Il danno esistenziale viene definito come quel danno derivante dalla violazione di un "*diritto inviolabile della persona costituzionalmente protetto*" e, pertanto, non assume alcuna autonoma rilevanza.

[390] G. PONZANELLI, *Limiti del danno esistenziale*, in *Il danno esistenziale. Una nuova categoria della responsabilità civile*, a cura P. CENDON-P. ZIVIZ di Giuffrè, 2000, pp. 803 ss.; G. PONZANELLI (a cura di), *Il "nuovo" danno non patrimoniale*, Cedam, 2004.

[391] Si. v. l'opinione contraria di E. TOSI, *ult. op. cit.*, secondo cui "*tale valutazione, invero, non potrà mai incidere sull'an debeatur non potendosi ritenere la lesione di un diritto fondamentale tutelato dalla Costituzione né insignificante né futile, ma semmai solo sul piano liquidatorio – quantum debeatur – potendosi ammettere una quantificazione questa sì, limitata dal punto di vista della monetizzazione del disagio della persona conseguente alla lesione del diritto fondamentale*", nonché F. QUARTA, secondo cui questa argomentazione "*stenta a persuadere già a partire dalla considerazione del rango – supremo – degli interessi coinvolti, ma persuade ancor meno se si osserva che un simile criterio discretivo risulta, invero, inoperante per i danni di natura patrimoniale, reputati sempre rilevanti, senza limiti quantitativi*" (F. QUARTA, *Risarcimento e sanzione nell'illecito civile*, Esi, 2013, pp. 127 ss.).

[392] CASS., ord. 27.3.2018, n. 7513, in *Danno e resp.*, 2018, pp. 456 ss., con nota di G. PONZANELLI, *Danno non patrimoniale: l'abbandono delle Sezioni Unite di San Martino*, pp. 467 ss. Pubblicata anche in *Nuova giur civ. comm*., 2018, I, con note di G. PONZANELLI, *Il decalogo sul risarcimento del danno non patrimoniale e la pace all'interno della Terza Sezione*, e di M. FRANZONI, *Danno evento, ultimo atto?* Nel solco tracciato dal decalogo, si vedano anche: CASS., 17.1.2018, n. 901 (Pres. ed Est. Travaglino), - N.C. c. Generali Italia s.p.a. già Ina Assitalia s.p.a., secondo cui: "*La natura unitaria ed onnicomprensiva del danno non patrimoniale, come predicata dalle Sezioni unite della S.C., deve essere interpretata, rispettivamente, nel senso di unitarietà rispetto a qualsiasi lezione di un interesse o valore costituzionalmente protetto non suscettibile di valutazione economica e come obbligo, per il giudice di merito, di tenere conto, a fini risarcitori, di tutte le conseguenze derivanti dall'evento di danno, nessuna esclusa, con il concorrente limite di evitare duplicazioni risarcitorie, attribuendo nomi diversi a pregiudizi identici, e di non oltrepassare una soglia minima di apprezzabilità, procedendo ad una accertamento concreto e non astratto, dando ingresso a tutti i mezzi di prova normativamente previsti, ivi compreso il fatto notorio, le massime di esperienza, le presunzioni. In tema di risarcimento del danno non patrimoniale conseguente alla lesione di interessi costituzionalmente protetti, il giudice di merito, dopo aver identificato la situazione soggettiva protetta a livello costituzionale, deve rigorosamente valutare, sul piano della prova, tanto l'aspetto interiore del danno (c.d. danno morale), quanto il suo impatto modificativo "in pejus" con la vita quotidiana (il danno c.d. esistenziale, o danno alla vita di relazione, da intendersi quale danno dinamico-relazionale),*

del danno morale soggettivo: quest'ultimo riacquista così spazi di liquidazione autonoma rispetto al danno biologico[393].

I principi di diritto di questa vera e propria controriforma dello statuto del danno non patrimoniale possono così essere sintetizzati:

- l'ordinamento prevede due sole categorie di danni: patrimoniale e non patrimoniale. Trattasi di categorie giuridicamente – anche se non fenomenologicamente – unitarie;
- nella liquidazione del danno non patrimoniale, il giudice è tenuto a prendere in considerazione tutte le conseguenze dannose derivanti dalla condotta illecita, evitando di attribuire nomi diversi a pregiudizi identici;
- in sede istruttoria, deve procedersi ad un articolato e approfondito accertamento in concreto dell'effettiva sussistenza dei pregiudizi affermati (o negati), dando ingresso a tal fine ogni fondamentale mezzo di prova, compreso il ricorso al fatto notorio, alle massime di esperienza e alle presunzioni, senza tuttavia rifugiarvisi aprioristicamente e procedere ad automatismi risarcitori;
- costituisce duplicazione risarcitoria, in presenza di un danno permanente alla salute, il riconoscimento di una somma di denaro a titolo di risarcimento del danno biologico e l'attribuzione di un'ulteriore somma a titolo di risarcimento per il danno dinamico-relazionale (ossia il pregiudizio alle attività quotidiane, personali e relazionali, indefettibilmente dipendenti dalla perdita anatomica o funzionale). Di tali ultimi pregiudizi, infatti, è già espressione il grado percentuale di invalidità permanente;
- a fronte di un danno permanente alla salute, non è ammessa alcuna personalizzazione in aumento del risarcimento qualora i pregiudizi patiti ricadano all'interno delle "conseguenze dannose normali e indefettibili" secondo l'*id quod plerumque accidit*. Unicamente il ricorrere di conseguenze dannose del tutto anomale e peculiari può, se del caso, giustificare modificazioni in aumento della somma da corrispondersi a titolo risarcitorio;
- ricorrendo un danno permanente alla salute, non dà luogo a duplicazione risarcitoria la congiunta attribuzione di una somma di denaro a titolo di risarcimento del danno biologico e l'ulteriore somma a titolo di risarcimento di pregiudizi che non trovano fondamento medico-legale, rappresentati dalla sofferenza interiore (il dolore dell'animo, la vergogna, la disistima

---

atteso che oggetto dell'accertamento e della quantificazione del danno risarcibile – alla luce dell'insegnamento della Corte costituzionale (sent. n. 235 del 2014) e del recente intervento del legislatore (omissis) – è la sofferenza umana conseguente alla lesione di un diritto costituzionalmente protetto, la quale, nella sua realtà naturalistica, si può connotare in concreto di entrambi tali aspetti essenziali, costituenti danni diversi e , perciò, autonomamente risarcibili, ma solo se provati caso per caso con tutti i mezzi di prova normativamente previsti".

[393] C. SCOGNAMIGLIO, *Danno morale soggettivo*, in *Nuova Giur. civ. comm.*, 2010, pp. 327 ss.

di sé, la paura, la disperazione), ovverosia il c.d. danno morale soggettivo.

- non solo alla lesione della salute, ma anche a quella di altri interessi costituzionalmente tutelati, può conseguire un danno di natura non patrimoniale il quale, non diversamente dalle ipotesi analizzate sopra, andrà liquidato in considerazione tanto del pregiudizi patiti dalla vittima nella relazione con sé stessa (*id est* danno morale interiore/interiore), quanto di quelli relativi alla dimensione dinamico-relazionale della vita del soggetto leso; in entrambi i casi, senza automatismi risarcitori e a seguito di approfondita istruttoria[394].

10. Art. 82 GDPR e filtro di risarcibilità

Come la dottrina maggioritaria, anche la giurisprudenza di legittimità assoggetta la responsabilità per illecito trattamento dei dati alle regole tradizionali proprie della responsabilità aquiliana.

In particolare, la giurisprudenza maggioritaria sostiene che l'illecito trattamento di dati personali, sebbene comportante un'ingiustificata lesione del diritto fondamentale alla protezione dei dati personali, debba comportare altresì in concreto una lesione che, andando oltre la soglia di tollerabilità, ne renda significativamente apprezzabile la portata e costituzionalmente meritevole il ristoro.

Sul punto, la Corte di Cassazione ha affermato che "*il danno non patrimoniale risarcibile ai sensi del D.Lgs. n. 196 del 2003, art. 15 (Codice della privacy), pur determinato da una lesione del diritto fondamentale alla protezione dei dati personali tutelato dagli artt. 2 e 21 Cost. e dall'art. 8 della CEDU, non si sottrae alla verifica della "gravità della lesione" e della "serietà del danno", in quanto anche per tale diritto opera il bilanciamento con il principio di solidarietà ex art. 2 Cost., di cui quello di tolleranza della lesione minima è intrinseco precipitato, sicché determina una lesione ingiustificabile del diritto non la mera violazione delle prescrizioni poste dall'art. 11 del codice della privacy, ma solo quella che ne offenda in modo sensibile la sua portata effettiva, restando comunque il relativo accertamento di fatto rimesso al giudice di merito*"[395].

Dunque, alla stregua dell'orientamento diffuso, il danno conseguente alla violazione delle norme poste a tutela dei dati personali deve essere dimostrato, poiché ciò che è risarcibile non è la lesione dell'interesse alla *privacy*, ma le conseguenze negative della stessa, in quanto "*il danno alla privacy,*

---

[394] Tale decalogo pare maggiormente in linea con il quadro comunitario in materia di risarcimento del danno non patrimoniale. "*Dall'analisi delle norme, e della giurisprudenza della CGUE, non solo non si individuano regole che limitano il risarcimento del danno alla persona, ma anzi, si riscontrano disposizioni che parlano genericamente di danno, quale nozione comprensiva di ogni conseguenza derivante da fatto illecito – basti pensare al Regolamento Roma II – oppure norme – come in materia di responsabilità del produttore – che, mentre pongono restrizioni per il risarcimento del danno materiale o al patrimonio, nessun limite prescrivono per il danno alla persona*", così M. A. ASTONE, *Il danno non patrimoniale nel diritto interno e sovranazionale tra antiche e nuove questioni*, in *Eur. e dir. priv.*, fasc. 4., 1, 2018, pp. 1183 ss.; E. TOSI, *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale*, cit., pp. 212 ss.

[395] CASS., 20.8.2020 n. 17383; CASS., 10.6.2021, n. 16402.

come ogni danno non patrimoniale, non sussiste in "re ipsa", non identificandosi il danno risarcibile con la mera lesione dell'interesse tutelato dall'ordinamento, ma con le conseguenze di tale lesione, seppur può essere provato anche attraverso presunzioni"[396].

Non è affatto sufficiente, ai fini del riconoscimento di un diritto al risarcimento, la sola prova della violazione degli obblighi derivanti dalla disciplina a protezione dei dati personali, dovendosi dimostrare, unitamente a questa, la lesione subita al diritto alla personalità nonché le conseguenze pregiudizievoli occorse[397].

10.1. La gravità della lesione

Nel pensiero giurisprudenziale corrente, per ottenere il riconoscimento del diritto al risarcimento del danno non patrimoniale da illecito trattamento dei dati è sempre necessario accertare se la lesione è "*grave*" e "*seria*"[398].

Nonostante la risarcibilità di questo tipo di danno sia espressamente prevista dall'art. 82 GDPR (e fosse prevista in precedenza dall'art. 15 cod. privacy), il suo effettivo riconoscimento richiede i medesimi requisiti di gravità e serietà della lesione, non essendo risarcibile il pregiudizio futile e non

---

[396] CASS. n. 19434/2019; CASS. n. 29206/2019; CASS., 10.6.2021, n. 16402. Sul tema, si v. anche CASS., 20.1.2015, n. 824, secondo cui il risarcimento del danno non patrimoniale "*non può derivare dalla mera violazione delle prescrizioni di cui al d.lgs. n. 196/2003, artt. 11-15 e art. 2050 c.c., sebbene comportante l'ingiustificata lesione del diritto fondamentale alla protezione dei dati personali; ma richiede che tale violazione abbia determinato in concreto una lesione che, andando oltre la suddetta soglia di tollerabilità`, ne renda significativamente apprezzabile la portata e costituzionalmente meritevole il ristoro*". Nonché CASS., 15.7.2014, n. 16133, in *Danno e resp*., 2015, pp. 339 ss., con note di V. CECCARELLI, *La soglia di risarcibilità del danno non patrimoniale da illecito trattamento dei dati personali* e M. NITTI, *La valutazione della "gravità della lesione" e della "serietà del danno" nel risarcimento del danno non patrimoniale da violazione della privacy*; CASS., 10.5.2001, n. 6507, in *Resp. civ. e prev*., 2001, p. 1177, con nota di P. ZIVIZ, *I "nuovi danni" secondo la Cassazione*. Si v., però, anche la giurisprudenza di merito contraria a tale orientamento, che non richiede il "doppio filtro" della serietà e gravità del danno per il riconoscimento del diritto al risarcimento, TRIB. POTENZA, 27.1.2010, in *Danno e resp*., 2011, p. 131; TRIB. MILANO, 5.6.2007, in *Guida dir*., 2007, 41, pp. 56 ss.; APP. MILANO, 19.6.2007, in *Dir. inf.*, 2007, p. 1101; Trib. Latina, 19.6.2006, in *Foro it.,* 2007, I, c. 324; TRIB. MILANO, 8.5.2003, in *Danno e Resp*., 2004, p. 303.

[397] Sul danno risarcibile per illecito trattamento di dati personali, si v. F. BILOTTA, *La responsabilità civile nel trattamento dei dati personali*, in *Circolazione e protezione dei dati personali*, a cura di PANETTA, cit., pp. 445 ss.; E. LUCCHINI GUASTALLA, *Il nuovo regolamento europeo sul trattamento dei dati personali: i principi ispiratori*, in *Contr. e impresa*, 2018, pp. 106 ss.; ID., *Trattamento dei dati personali e danno alla riservatezza*, in *Resp. civ. e prev*., 2003, pp. 632 ss. spec. 650; G. RESTA-A. SALERNO, *La responsabilità civile per il trattamento dei dati personali*, in G. ALPA (a cura di), *La responsabilità d'impresa*, Giuffrè, 2016, p. 660; D. MESSINETTI, *I nuovi danni. Modernità, complessità della prassi e pluralismo della nozione giuridica di danno*, in *Riv. crit. dir. priv*., 2006, pp. 543 ss., spec. p. 564; F. DI CIOMMO, *Il danno non patrimoniale da trattamento dei dati personali*, in *Il "nuovo" danno non patrimoniale*, a cura di G. PONZANELLI, cit., pp. 274 ss.; S. SICA, *Commento sub artt. 11-22,* in *La nuova disciplina della privacy (d. lgs. 30 giugno 2003, n. 196)*, a cura di S. SICA e M. G. STANZIONE, Le riforme del diritto italiano, 2005., p. 8; A. THIENE, *Segretezza e riappropriazione di informazioni di carattere personale: riserbo e oblio nel nuovo Regolamento europeo*, in *Nuove leggi civ*., 2017, p. 443; G. RAMACCIONI, *La protezione dei dati personali: il tema/problema del risarcimento del danno non patrimoniale*, in *Danno e resp.*, 2018, pp. 665.

[398] S. THOBANI, *Il danno non patrimoniale da trattamento illecito dei dati personali*, cit., pp. 427 ss.

serio[399].

Va evidenziato che la disciplina del GDPR si compone principalmente di norme di condotta, ossia precetti imposti con finalità conformativa dell'attività del titolare rispetto al trattamento dei dati.

Secondo la giurisprudenza di legittimità, è necessario venga provata la sussistenza di una sensibile offesa alla portata effettiva dell'interesse protetto dalle norme del GDPR violate.

Si ricordi, poi, che il requisito dell'ingiustizia opera in modo indipendente rispetto all'antigiuridicità della condotta, nel senso che occorre individuare una situazione soggettiva, lesa dall'attività di trattamento, che sia tutelata dall'ordinamento anche al di fuori della normativa in materia di protezione dei dati personali[400]. La Corte di Cassazione, infatti, in molteplici occasioni ha accordato tutela risarcitoria in ipotesi in cui dalla condotta illecita (contraria alla disciplina sulla protezione dei dati) fosse derivata altresì una violazione dei diritti fondamentali dell'individuo; in particolare, diffuso è il richiamo agli artt. 2 e 21 Cost. e 8 Conv. eur. dir. uomo.

Una volta individuato, dunque, l'interesse costituzionale protetto dalla norma sul trattamento dei dati violata dal titolare, la Corte di Cassazione verifica se tale posizione individuale abbia subito un pregiudizio che può essere definito grave (su questo requisito, v. *infra* par. successivo).

Si registrano, tuttavia, due orientamenti difformi in dottrina, che criticano l'impostazione della Corte di Cassazione per un duplice ordine di ragioni.

Secondo un primo orientamento, l'antigiuridicità della condotta sarebbe sufficiente per il riconoscimento del diritto al risarcimento del danno. Il legislatore avrebbe già, *ex ante*, svolto un giudizio di gravità e antigiuridicità della condotta, nel momento stesso in cui ha fissato un precetto conformativo a cui il titolare deve attenersi, con la conseguenza che è la stessa violazione della norma che dimostra la lesione all'interesse del singolo[401]. Il danno sarebbe, dunque, sempre oggettivamente presente, dovendosi solo procedere ad una sua quantificazione (tesi che, se estremizzata, porta ad una sorta di "oggettivizzazione" del danno, su cui v. *infra*).

Altro orientamento della dottrina ritiene, invece, corretto individuare un ulteriore interesse giuridico

---

[399] CASS., 15.7.2014, n. 16133; CASS., 5.3.2015, n. 4443; CASS., 20.5.2015, n. 10280; CASS., 19.7.2016, n. 14694; CASS., 20.5.2016, n. 10510; CASS., 25.1.2017, n. 1931.

[400] Dunque, secondo l'orientamento maggioritario della giurisprudenza di legittimità non è sufficiente che sia violata una norma sul trattamento affinché il danno possa essere qualificato come "ingiusto", dovendosi sempre verificare se la condotta illecito ha leso un interesse specifico dell'individuo.

[401] V. COLONNA, *Il sistema della responsabilità civile da trattamento dei dati personali*, in *Diritto alla riservatezza e circolazione dei dati personali*, a cura di R. PARDOLESI, Giuffrè, 2003, II, pp. 53 ss.; S. SICA, *Danno e nocumento nell'illecito trattamento di dati personali*, in *Dir. inf. e inform.*, 2004, p. 721; F. DI CIOMMO, *La risarcibilità del danno non patrimoniale da illecito trattamento dei dati personali,* in *Danno e resp*., 2005, p. 803; D. MESSINETTI, *Pluralismo dei modelli risarcitori. Il criterio di ingiustizia "tradito*", in *Riv. crit. dir. priv*., 2007, pp. 561 ss.

che fa capo all'individuo in relazione al quale valutare la gravità della lesione[402]: in questo senso, tale orientamento non si discosta dall'impostazione giurisprudenziale. Si discute, tuttavia, se sia corretto ricercare tale interesse al di fuori della disciplina sulla protezione dei dati, dunque all'interno delle Carte fondamentali, poiché il GDPR costituisce proprio l'attuazione dei diritti fondamentali riconosciuti all'individuo. In altre parole, la disciplina sulla protezione dei dati statuisce, nel dettaglio, le prescrizioni che tutelano i diritti fondamentali, individuando i comportamenti illeciti e gli specifici interessi degli individui.

A titolo esemplificativo, le norme che obbligano il titolare a rendere determinate informazioni in modo trasparente sono poste a tutela di un interesse dell'individuo già valutato dal legislatore come meritevole di tutela, con la conseguenza che la violazione della disposizione pregiudicherebbe direttamente e sicuramente tale interesse, in ogni situazione. Ancora, è il caso delle norme sulle comunicazioni indesiderate, poste a tutela della tranquillità dell'individuo.

I suddetti casi dimostrano, sulla scorta della seconda impostazione di cui si è dato atto, che il GDPR pone una normativa di dettaglio che tutela specifici e già individuati interessi degli individui, che derivano dai diritti fondamentali. Dunque, il requisito della gravità andrebbe valutato in relazione ad un interesse leso dell'individuo, con la conseguenza che non sarebbe sufficiente la condotta illecita per il riconoscimento del diritto al risarcimento del danno; tuttavia, tale interesse va individuato all'interno dello stesso GDPR, facendo riferimento all'interesse protetto dalla norma di condotta specificamente violata.

10.2. La serietà del danno

Secondo l'orientamento maggioritario della giurisprudenza di legittimità, affinché il diritto al risarcimento per illecito trattamento dei dati sia riconosciuto, la lesione deve essere grave e il danno deve essere "serio", ossia non futile né ipotetico.

Dunque, una volta accertata la gravità della lesione all'interesse protetto, devono valutarsi le conseguenze pregiudizievoli subite dal danneggiato[403].

---

[402] E. PELLECCHIA, *La responsabilità civile per trattamento dei dati personali*, in *Resp. civ. e prev*., 2006, pp. 8 ss.; F. PIRAINO, *Ingiustizia del danno e antigiuridicità,* in *Europa e dir. priv*., 2005, pp. 746 ss.; B. MASTROPIETRO, *Il danno da illecito trattamento di dati personali*, in *Nuova giur. civ. comm.,* 2004, I, pp. 679 ss.; G. COMANDÈ, *Sub art. 18,* in *Nuove leggi civ. comm*., 1999, I, p. 500; M. FRANZONI, *Dati personali e responsabilità civile*, in *Resp. civ. e prev*., 1998, p. 903.

[403] Il Considerando n. 75 afferma che "*I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità , perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano». Si veda, inoltre, il considerando n. 83 del GDPR*."

Il danno non potrà considerarsi sussistente *in re ipsa*, ma dovrà essere allegata e provata – anche per presunzioni – una conseguenza negativa specifica subita dal soggetto.

Secondo la consolidata ricostruzione della giurisprudenza di legittimità, deve infatti distinguersi il danno-evento, ossia la lesione alla situazione giuridica soggettiva, dal danno-conseguenza, che sono le specifiche conseguenze negative subite.

In particolare, dall'un lato, il danno-evento è imputato ad un determinato soggetto agente, il danneggiante, sulla base del nesso di causalità materiale (espressione che sta ad indicare "l'appartenenza" di una data condotta ad un determinato agente), ricostruito secondo le note teorie della *condicio sine qua non* e della causalità adeguata (per citare solo i principali criteri di imputazione della condotta); dall'altro lato, il nesso di causalità giuridica seleziona, tra gli eventi negativi conseguenti al danno-evento, quelli effettivamente risarcibili (si tratta di causalità "giuridica" poiché il riferimento è al giudizio "giuridico" del legislatore, che ha selezionato solo alcune conseguenze come rilevanti, mentre ha ritenuto che altre non siano risarcibili).

Tuttavia, se questo è l'orientamento consolidato, può divenire complesso valutare se una determinata conseguenza di un trattamento illecito possa dirsi "grave" per l'individuo: si tratta di un giudizio con ampi spazi di discrezionalità e interpretazione.

Ad esempio, la Corte ha più volte precisato che non sono meritevoli di tutela risarcitoria "*i pregiudizi consistenti in disagi, fastidi, disappunti, ansie ed in ogni altro tipo di insoddisfazione concernente gli aspetti più disparati della vita quotidiana che ciascuno conduce nel contesto sociale, ai quali ha invece prestato tutela la giustizia di prossimità. Non vale, per dirli risarcibili, invocare diritti del tutto immaginari, come il diritto alla qualità della vita, allo stato di benessere, alla serenità: in definitiva, il diritto ad essere felici*"[404], arrivando, per tale ragione, a rigettare talune domande di risarcimento danni conseguenti a illecito trattamento[405].

Questo orientamento è stato criticato da una parte della dottrina, secondo cui solo se una disposizione del GDPR pone un obbligo di condotta a tutela di un interesse dell'individuo, il danno deve sempre essere considerato ingiusto e rilevante, anche se ciò che viene protetto è il mero interesse a non subire fastidi e disagi. Tale orientamento osserva che "*se il legislatore tutela la qualità della vita sotto un suo determinato aspetto (come, nel caso che qui interessa, l'interesse a non ricevere comunicazioni indesiderate), sanzionando la violazione di tale interesse con il risarcimento del danno non patrimoniale, la lesione non può, di per sé, essere considerata qualitativamente futile e, dunque,*

[404] CASS., 11.11.2008, n. 26972.

[405] CASS., 10.10.2014, n. 21415; CASS., 28.2.2013, n. 5096; CASS., 25.2.2016, n. 3727.

irrisarcibile (e il danno è dunque necessariamente ingiusto)"[406].

Pertanto, anche disagi e fastidi possono costituire danni effettivamente risarcibili, non potendo essere esclusi perché considerati futili: secondo tale orientamento, andrà svolto su di essi il giudizio di gravità.

11. Osservazioni critiche al doppio filtro di ammissibilità: prospettive ermeneutiche verso l'oggettivizzazione del danno

In seguito all'entrata in vigore del nuovo Regolamento, la tesi che riconduce la responsabilità per illecito trattamento dei dati personali alla disciplina comune della responsabilità extracontrattuale è stata criticata da una parte della dottrina che, in particolar modo, ne ha evidenziato alcune intrinseche contraddizioni.

Come detto, secondo l'orientamento prevalente e consolidato da molteplici pronunce della giurisprudenza di legittimità, il danno non patrimoniale risarcibile – ora ai sensi dell'art. 82, par. 3, GDPR, in precedenza ai sensi dell'abrogato art. 15 cod. privacy – sia pure cagionato da una lesione del diritto fondamentale alla protezione dei dati personali, non si sottrae alla verifica della gravità della lesione e della serietà del danno. Di qui, l'esclusione di ogni forma di automatismo che consideri risarcibile *in re ipsa* il danno di natura immateriale derivante da illecito trattamento di dati personali, dovendo, al contrario, subordinarsi l'accesso alla tutela risarcitoria ai citati parametri-soglia[407].

Dunque, con ogni violazione dei principi e delle regole di condotta poste dal GDPR porta ad una lesione ingiusta del diritto tutelato, ma unicamente quella che ne offenda in modo sensibile la sua portata effettiva.

All'opposto, vi sono autori (e qualche pronuncia giurisprudenziale isolata) che abbracciano la teoria del danno-evento (o danno *in re ipsa*), favorevoli al riconoscimento di una tutela risarcitoria al

---

[406] S. THOBANI, *Invio di comunicazioni indesiderate: il risarcimento del danno non patrimoniale*, in *Giur. it.*, 2017, pp. 1537 ss.; EAD., *Il danno non patrimoniale da trattamento illecito dei dati personali*, cit.

[407] Così, *ex multis*, CASS., 3.7.2014, n. 15240; CASS., 15.7.2014, n. 16133 che, ribadendo l'impossibilità di ravvisare un danno non patrimoniale *in re ipsa*, si rifà anche al criterio introdotto dalla giurisprudenza della Corte Europea dei Diritti dell'Uomo, in applicazione del paragrafo 3 b) dell'art. 35 della Convenzione (*Cusan e Fazzo c. Italia*, n. 77/07, 7.1.2014). La Suprema Corte, in quest'ultima pronuncia, nell'affermare l'imprescindibilità di un doppio filtro, ne rinviene la ragione nella circostanza che "…*anche nella fattispecie di danno non patrimoniale di cui al citato art. 15 opera il bilanciamento del diritto tutelato da detta disposizione con il principio di solidarietà – di cui il principio di tolleranza è intrinseco precipitato – il quale, nella sua immanente configurazione, costituisce il punto di mediazione che permette all'ordinamento di salvaguardare il diritto del singolo nell'ambito di un'esistenza collettiva. L'accertamento di fatto rimesso, a tal fine, al giudice del merito, in forza di previe allegazioni e di coerenti istanze istruttore di parte, dovrà essere ancorato alla concretezza della vicenda materiale portata alla cognizione giudiziale ed al suo essere maturata in un dato contesto temporale e sociale, dovendo l'indagine, illuminata dal bilanciamento anzidetto, proiettarsi sugli aspetti contingenti dell'offesa e sulla singolarità delle perdite personali verificatesi. Un siffatto accertamento che, ove l'offesa non superi la soglia di minima tollerabilità o il danno sia futile, può condurre anche ad escludere la possibilità di somministrare il risarcimento del danno, è come tale sottratto al sindacato di legittimità se congruamente motivato*".

verificarsi di ogni condotta realizzata in spregio alle regole conformative previste in materia, a prescindere dalla prova del pregiudizio in concreto subito.

Secondo tale ultimo orientamento, sarebbe necessario "*superare la tradizionale soglia di risarcibilità correlata all'ulteriore generale presupposto dell'ingiustizia del danno*"[408] e, di conseguenza, dimostrare esclusivamente la lesione al diritto protetto – in specie, il diritto fondamentale alla riservatezza e diritto fondamentale alla protezione dei dati personali – da qualificarsi, questa lesione, come causa già sufficiente per scivolare nel piano della risarcibilità. Tale lesione, di per sé sola, integrerebbe un danno *in re ipsa,* per il semplice fatto che è stato leso un diritto fondamentale della persona[409].

È stato, infatti, osservato che "*la questione del danno alla persona, riportata alla riprovevolezza in sé della condotta, in considerazione della natura speciale del valore leso, ripropone la rilevanza del valore giuridico della persona nella sua dimensione più propria: la condotta antigiuridica*"[410].

Tale prospettiva trae origine dal fatto che né l'ormai abrogato art. 15 cod. privacy né l'attuale art. 82 GDPR richiedono, ai fini del riconoscimento del diritto al risarcimento, il profilarsi di un danno "*ingiusto*", caratteristica, quest'ultima, specificamente richiamata nella disciplina generale in tema di responsabilità extracontrattuale[411].

---

[408] E. TOSI, *Illecito trattamento dei dati personali, responsabilizzazione, responsabilità oggettiva e danno nel GDPR: funzione deterrente-sanzionatoria e rinascita del danno morale soggettivo*, in *Contr. e impr.*, 2020, pp. 1115 ss.

[409] Nella giurisprudenza di merito, si vedano: TRIB. MILANO, 23.9.2009, in *Corr. merito*, 2010, p. 19; TRIB. MILANO, 27.6.2007; APP. MILANO, 19.6.2007, in *Dir. Informaz. e Informatica*, 2007, p. 1101; TRIB. CATANIA, 18.1.2007: TRIB. LATINA, 19.6.2006, in *Foro it*., 2007, I, c. 324; TRIB. TRIESTE, 21.9.2005, in *Nuova Giur. Civ. Comm*., 2006, I, p. 1179.

[410] D. MESSINETTI, *I nuovi danni. Modernità, complessità della prassi e pluralismo della nozione giuridica di danno*, cit., p. 552.

[411] F. DI CIOMMO, *La risarcibilità del danno non patrimoniale da illecito trattamento dei dati personali*, in *Danno e Resp.,* 2005, 7, p. 803; R. MONTINARO, *Tutela della riservatezza e risarcimento del danno nel nuovo "codice in materia di protezione dei dati personali"*, in *Giust. civ*., 2004, p. 259; S. SICA, *Danno e nocumento nell'illecito trattamento di dati personali*, in *Dir. Informazione e informatica*, 2004, p. 721; V. COLONNA, *Il sistema della responsabilità civile da trattamento dei dati personali*, cit., pp. 53 ss. In tal senso *cfr.* D. MESSINETTI, *Pluralismo dei modelli risarcitori. Il criterio di ingiustizia "tradito"*, in *Riv. crit. dir. priv*., 2007, pp. 561 ss.; sul punto, si veda anche S. THOBANI, secondo cui "*se invece il legislatore ha presidiato una norma di condotta (non inviare comunicazioni indesiderate) a tutela di un determinato interesse (la tranquillità) con la sanzione del risarcimento del danno non patrimoniale, non si vede come possa ritenersi che il pregiudizio derivante dalla lesione di tale interesse (l'essere disturbati dalle email pubblicitarie) sia di per sé qualitativamente futile. In altre parole, una volta che il legislatore ha previsto la risarcibilità del danno non patrimoniale a tutela di certi interessi, non pare esservi spazio per una valutazione giudiziale di non serietà del pregiudizio che ne deriva. La lesione della tranquillità individuale non può dunque essere considerata, di per sé, un pregiudizio futile, dato che costituisce proprio l'interesse tutelato dalla norma la cui violazione è sanzionata con il risarcimento del danno non patrimoniale. Né vale ad affermare il contrario la qualificazione dell'interesse leso come diritto costituzionalmente tutelato alla protezione dei dati personali, posto che, come già evidenziato, è alle previsioni legislative (le quali hanno già effettuato un bilanciamento tra i contrapposti interessi) che occorre fare riferimento per verificare il contenuto di tale posizione soggettiva. Nella nostra materia la risarcibilità del danno non patrimoniale deriva infatti dalla previsione del legislatore e quindi prescinde dai confini del diritto costituzionalmente tutelato che*

Entrambe le disposizioni citate richiedono, quale presupposto base della risarcibilità, unicamente la violazione della disciplina dettata in tema di protezione dei dati al fine di qualificare come "*illecita*" la condotta del danneggiante. Così ragionando, pertanto, si assisterebbe ad una sorta di "*oggettivizzazione*" del danno, sempre ricorrente e necessariamente risarcibile.

Secondo questa stessa ricostruzione ermeneutica, la responsabilità per illecito trattamento di dati presenti profili di visibile specialità rispetto alla disciplina comune, dai quali, pertanto, non può che discendere un'adeguata differenziazione sul piano della disciplina applicabile.

Di conseguenza, nell'ambito di responsabilità per illecito trattamento di dati "*rileva esclusivamente l'antigiuridicità della condotta, senza che sia necessario dimostrare l'ingiustizia del danno in quanto presupposta dalla norma, con conseguente configurabilità del risarcimento del danno evento o danno* in re ipsa".

Mentre secondo la disciplina di diritto comune è necessario verificare l'esistenza di un danno *contra ius* e *non iure*, la responsabilità per illecito trattamento di dati è costruita "*in funzione di un comportamento riprovevole nella sua antigiuridicità, valutato* ex ante *tramite la prescrizione di principi e regole di condotta conformative relative alla liceità del trattamento che prescindono dall'ulteriore verifica di causazione di un danno ingiusto,* recte *lo presuppongono in ragione della violazione del precetto conformativo in ordine alla liceità del trattamento*"[412].

I sostenitori di tale orientamento considerano, come elemento idoneo a suffragarlo, il regime della prova liberatoria di cui all'art. 82, par. 3, GDPR, in virtù del quale il titolare del trattamento (o il responsabile del trattamento) è esonerato da responsabilità "*se dimostra che l'evento dannoso non gli è in alcun modo imputabile*"[413]. Tale disposizione, infatti, farebbe esclusivo riferimento all'"*evento dannoso*", ovverosia alla condotta lesiva dell'interesse tutelato, difettando qualsivoglia richiamo – all'interno del medesimo art. 82 – alle *conseguenze dannose* di tale lesione.

Vertendo nella materia (dai profili quantomai evanescenti) della risarcibilità dei diritti personali, è nota la difficoltà di provare e dimostrare l'effettiva sussistenza di un danno, anche e soprattutto nel

---

eventualmente ne sta alla base, stando alla potestà del legislatore prevedere la risarcibilità anche oltre gli interessi costituzionalmente protetti", S. THOBANI, *Invio di comunicazioni indesiderate: il risarcimento del danno non patrimoniale*, in *Giur. it.*, 2017, pp. 1537 ss.

[412] E. TOSI, *Illecito trattamento dei dati personali, responsabilizzazione, responsabilità oggettiva e danno nel GDPR: funzione deterrente-sanzionatoria e rinascita del danno morale soggettivo*, in *Contr. e impresa*, 2020, pp. 1115 ss., secondo cui si registrerebbe così "*l'oggettivazione del danno in forza della quale la struttura della responsabilità muta da regola comune a regola speciale: rileva non più la valutazione del danno in quanto effetto di condotta lesiva ma semplicemente la condotta antigiuridica* ex se".

[413] Analoga formulazione è contenuta nel Considerando n. 146: esso prevede che il titolare del trattamento o il responsabile del trattamento dovrebbe risarcire i danni cagionati ad una persona da un trattamento non conforme al Regolamento, "*ma dovrebbe essere esonerato da tale responsabilità se dimostra che l'evento dannoso non gli è in alcun modo imputabile*".

suo preciso ammontare[414].

Coloro che formulano osservazioni critiche alla ricostruzione del danno quale danno-conseguenza ne evidenziano il carattere "*irrazionale*" evidenziando come, aderendovi, si accetterebbe un'ingiusta asimmetria regolatoria tra risarcibilità del danno patrimoniale – non assoggettato al vaglio di ammissibilità del doppio filtro – e del danno non patrimoniale; ancora, si accetterebbe un'ingiusta compressione di tutela rispetto ai diritti fondamentali della persona di rango costituzionale, con un paradossale rovesciamento della gerarchia delle fonti per effetto del quale una norma della Costituzione finisce per ricoprire una posizione subordinata rispetto alla norma di cui all'art. 2043 c.c., referente normativo della responsabilità civile[415].

Di qui, la propensione verso una sorta di "*oggettivizzazione*" del danno, fenomeno ritenuto necessario onde garantire piena effettività al sistema di *private enforcement* costruito dal GDPR.

12. Onere della prova e quantificazione del danno non patrimoniale

A più riprese la giurisprudenza di legittimità ha ribadito la necessità che del danno subito a seguito di una condotta lesiva di illecito trattamento dei dati personali venga data prova specifica in giudizio, non potendosi ravvisare un danno non patrimoniale nel mero accertamento dell'illiceità del trattamento.

In forza della teoria del c.d. *danno-conseguenza*, il soggetto tutelato dalla normativa è onerato di fornire in giudizio specifica prova dell'effettivo pregiudizio subito quale conseguenza della lesione patita[416]. Tale prospettazione si pone in linea con la nozione di danno ingiusto fatta propria dalla Suprema Corte – per la prima volta nel 2003 ed in seguito consacrata in via definitiva dalle Sezioni Unite – secondo cui è tale qualsiasi lesione di un interesse giuridicamente rilevante preso in considerazione dell'ordinamento, da cui siano derivate conseguenze pregiudizievoli oggettivamente

---

[414] Quanto al profilo della prova, il consolidato orientamento giurisprudenziale (c.d. danno-conseguenza) ritiene che il danno debba essere "*allegato e provato da chi chiede il relativo risarcimento, anche se, trattandosi di un pregiudizio proiettato nel futuro, è consentito il ricorso a valutazioni prognostiche e a presunzioni sulla base di elementi obbiettivi che è onere del danneggiato fornire*" (così CASS., ord. 18.1.2018, n. 907); altresì CASS., sez. un., 11.11.20008, n. 26972, che ha chiarito che è "*da respingere […] l'affermazione che nel caso di lesione di valori della persona il danno sarebbe in re ipsa perché la tesi snatura la funzione del risarcimento, che verrebbe concesso non in conseguenza dell'effettivo accertamento di un danno, ma quale pena privata per un comportamento lesivo*".

[415] In questi termini, in particolare, si veda E. TOSI, *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale*, cit., p. 253.

[416] In questo senso, CASS., 3.8.2017, n. 19423; CASS., 25.1.2017, n. 1931 (con riguardo ad un'ipotesi di illegittima segnalazione in Centrale Rischi); CASS., 20.1.2015, n. 824; CASS., 5.9.2014, n. 18812, in *Foro it*., 2015, 1, c. 119, secondo cui il danno non patrimoniale "*deve essere allegato dal danneggiato e, quindi, da lui provato. Il danno di cui all'art. 15* [del Codice privacy] *non si può, dunque, identificare nell'evento dannoso, cioè nell'illecito trattamento dei dati personali, ma occorre che si concreti in un pregiudizio della sfera non patrimoniale di interesse del danneggiato*". In dottrina, in senso favorevole si vedano B. MASTROPIETRO, *Il danno da illecito trattamento dei dati personali nel quadro dei recenti orientamenti in materia di danno non patrimoniale*, op. cit., pp. 667 ss.

apprezzabili, patrimoniali o meno che siano[417].

Non sono mancate decisioni di merito che, all'opposto, facendo propria la teoria del *danno-evento* (o *danno in re ipsa*), hanno fatto conseguire al mero accertamento dell'illecito trattamento dei dati personali la sussistenza di un danno non patrimoniale risarcibile[418].

Milita nel senso della teoria del *danno-conseguenza* più di un dato testuale del Regolamento europeo. Il disposto dell'art. 82 sancisce il risarcimento del danno materiale o immateriale "*causato*" o "*cagionato*" da un trattamento in violazione del Regolamento, con ciò – evidentemente – dimostrando che il danno non coincide con il fatto in sé del trattamento illecito.

Rileva nello stesso senso il Considerando n. 75, che, riferendosi "*ai rischi per i diritti e le libertà delle persone fisiche*", aventi probabilità e gravità diverse, che possono derivare da trattamenti di dati personali (quali il furto o l'usurpazione di identità, la decifratura non autorizzata della preudonomizzazione, ecc.), utilizza, di nuovo, l'espressione "*suscettibili di cagionare un danno fisico, materiale o immateriale* […] *o qualsiasi altro danno economico o sociale significativo*".

Ancora, il Considerando n. 85, riferendosi all'obbligo in capo al titolare del trattamento di notificare all'autorità di controllo la violazione di dati personali di cui venga a conoscenza, afferma che tale violazione "*può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della preudonomizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata*".

Sulla scorta di tale impostazione, il danneggiato che agisce onde ottenere un risarcimento, una volta provata l'ingiustizia del danno, dovrà dare specifica prova del pregiudizio subito con riguardo al profilo del *quantum* da risarcirsi.

Si registra una certa apertura da parte della giurisprudenza quanto all'assolvimento dell'onere probatorio richiesto sul punto. Tale atteggiamento trova il suo fondamento in un ordinamento – GDPR e Codice privacy – che, consapevole delle difficoltà intrinseche di provare il danno non patrimoniale, mostra una funzione protettiva nei riguardi del soggetto leso. Il legislatore europeo, infatti, in considerazione del fatto che il trattamento illecito di dati personali produce molti più danni di natura

---

[417] Così CASS., 31.5.2003, n. 8827.

[418] Si vedano, nella giurisprudenza di merito: TRIB. POTENZA, 27.1.2010, in *Danno e resp*., 2011, p. 131, con nota adesiva di R. FOFFA, *Illecito trattamento dei dati personali in condominio*; TRIB. MANTOVA, 24.11.2009, in *Resp. civ. prev*., 2010, p. 233; TRIB. MILANO, 23.9.2009, in *Corr. merito*, 2010, p. 19; TRIB. TRIESTE, 21.9.2005, in *Nuova giur. comm*., 2006, I, p. 1179; TRIB. MILANO, 8.8.2003, in *Danno e resp*., 2004, p. 303; TRIB. ROMA, 10.1.2003, in *Danno e resp*., 2003, p. 532; TRIB. ROMA, 22.11.2022, in *Danno e resp*., 2003, p. 525.

non patrimoniale che patrimoniale, e che in tale ambito si rivela del tutto insoddisfacente il rimedio del risarcimento dei soli danni patrimoniali, riconosce la generale risarcibilità del danno di tipo immateriale al verificarsi di un trattamento di dati non conforme alla normativa.

Di qui, la possibilità, per il danneggiato, di ricorrere all'argomento presuntivo e di avvalersi di fatti notori, fermo restando, comunque, l'onere di indicare tutti gli elementi necessari al fine di ricostruire la serie concatenata di fatti noti che permettano al giudice di risalire presuntivamente al fatto ignoto.

I danni non patrimoniali – in specie, il danno morale in senso stretto – risultano difficilmente calcolabili poiché presentano intrinseche difficoltà probatorie in ordine al *quantum* della lesione; sfuggendo ad una valutazione economica oggettiva, la loro stima in termini economici non può che avvenire con un elevato grado di arbitrarietà[419].

Il problema dell'individuazione di criteri oggettivi di liquidazione del danno non patrimoniale è tema controverso e ampiamente dibattuto in dottrina e giurisprudenza[420].

Viene condiviso il richiamo al giudizio di equità[421] ma, a ben vedere, anche tale giudizio, pur strutturalmente flessibile, dovrebbe potersi ancorare a parametri per quanto possibile uniformi e oggettivi. Così operando si potrebbe circoscrivere il rischio di asimmetrie di trattamento e di violazioni al principio di integrale risarcimento del danno, enfatizzando al contempo le peculiarità del fatto concreto.

È generalmente avvertita l'esigenza di definire "*un nucleo probatorio forte costituito da criteri costanti, oggettivamente affidabili e non manipolabili, quali il tipo di interesse leso e la gravità dell'offesa nonché le condizioni oggettive del danneggiato su cui l'offesa ricade*"[422], da cui inferire

---

[419] *Ex multis*, si vedano: CASS., 15.10.2015, n. 20890, in *Danno e Resp*., 2016, 372; Cass., 13.11.2015, n. 23206; CASS., 18.11.2014, n. 24474. Sul tema della prova del danno non patrimoniale, si veda CASS., sez. un., 11.11.2008, n. 26972, cit, la quale ha ammesso che essa possa fornirsi anche con presunzioni semplici, fermo restando però l'onere del danneggiato di fornire gli elementi di fatto dai quali desumere l'entità di tale pregiudizio. Sul tema, altresì C. SALVI, *Il risarcimento integrale del danno non patrimoniale, una missione impossibile*. *Osservazione sui criteri per la liquidazione del danno non patrimoniale*, in *Eur. e dir. priv.*, 2014, pp. 517 ss.

[420] V. ZENO ZENCOVICH, *La quantificazione del danno alla reputazione e ai dati personali: ricognizione degli orientamenti 2013 del Tribunale di Roma*, in *Dir. inf*., 2014, p. 405; A. PINORI, *Internet e responsabilità civile per il trattamento dei dati personali*, in *Contr. e impr.*, 2007, p. 1565; S. PERON, *Ancora sul risarcimento del danno non patrimoniale da violazione della privacy*, in *Resp. civ. prev*., 2016, pp. 957 ss.; ID., *Sul risarcimento del danno non patrimoniale da violazione della privacy*, in *Resp. civ. prev*., 2013, pp. 225 ss.; R. FOFFA, *Il caso Vieri: quanto vale la lesione della privacy*, in *Danno e resp*., 2013, pp. 55 ss.

[421] Come noto, la valutazione equitativa è volta a determinare la compensazione economica socialmente adeguata del pregiudizio, ossia quella che l'ambiente sociale accetta come compensazione equa. Così M. GAMBINI, *Principio di responsabilità e tutela aquiliana dei dati personali*, cit., p. 114.

[422] Così, testualmente, E. NAVARRETTA, Il *contenuto del danno non patrimoniale e il problema della liquidazione*, in *Il danno non patrimoniale. Principi, regole e tabelle per la liquidazione*, a cura di E. NAVARRETTA, Giuffrè, 2010, p. 91, secondo il quale "*La loro costante ricorrenza in certe tipologie di casi consente, infatti, un confronto sul quantum ed una tendenziale equiparazione – nel rispetto del principio di eguaglianza formale – della loro stima monetaria a parità di condizioni*".

le conseguenze negative di tipo emotivo ed esistenziale che vengono a determinarsi in capo al danneggiato, onde favorire una qualche uniformità e/o prevedibilità delle soluzioni adottate.

L'esigenza è, pertanto, quella di adeguare la liquidazione alla sofferenza effettivamente patita dal danneggiato e a tutte le circostanze del caso in concreto.

Per la definizione del *quantum debeatur*, sono stati elaborati alcuni parametri – a partire dalla giurisprudenza in materia giornalistica[423] nonché dalla normativa dedicata alla protezione dei dati personali[424] – cui ancorare tale giudizio di equità; alcuni di essi, tuttavia, spuri in quanto non areddituali, pur essendo riferiti al danno non patrimoniale. Tra di essi: il rango del diritto violato, la gravità del pregiudizio, la durata del pregiudizio conseguente a trattamento illecito, l'ambito di diffusione del trattamento illecito, la natura dei dati trattati (comuni, bancari-finanziari o particolari), il rilievo economico del trattamento illecito, la notorietà della persona danneggiata, il ravvedimento operoso del danneggiante, le condizioni oggettive del danneggiato (sociali, economiche e professionali) da cui è possibile dedurre l'effettivo patimento sofferto sotto il profilo emotivo ed esistenziale, non solo personale ma altresì sul piano relazionale.

Peraltro, non manca un orientamento giurisprudenziale diametralmente opposto: questo rifugge da parametri rigidamente fissati in astratto – da cui discenderebbe una mera uguaglianza formale e non già sostanziale tra soggetti danneggiati – favorendo criteri elastici e flessibili, rifiutando esplicitamente il ricorso a indici tabellari, valori percentuali e scelte giudiziali equitative che non siano rispettose delle specificità del caso concreto[425].

Vi è chi tenta una sintesi tra giudizio di equità svincolato da ogni parametro uniforme e giudizio di equità vincolato a parametri tabellari e indici percentuali, proponendo di elaborare un metodo condiviso di liquidazione del danno non patrimoniale da trattamento illecito, formulando almeno i principali parametri che il giudice dovrà considerare per addivenire ad una liquidazione equa e flessibile, senza, tuttavia, pretendere di liquidare preventivamente in via generale ed astratta tale

---

[423] Viene ritenuto sufficiente dalla giurisprudenza, per quantificare il danno, la verifica dei parametri di liceità previsti dalla normativa vigente che in concreto abbiano determinato le modalità e la gravità dell'illecito. Sul punto, CASS., 15.10.2015, n. 20890, che considera, nella determinazione equitativa del danno non patrimoniale, natura dei dati (in quanto sensibili) e soggetto responsabile (ente pubblico), finalità concrete dell'ente danneggiante contrarie da quelle istituzionali.

[424] *Ex multis* si vedano CASS., 7.6.2011, n. 12408, in *Corr. Giur.*, 2011, pp. 1076 ss.; CASS., sez. un., 11.11.2008, n. 26972; CASS., 23.1.2014, n. 1361. In dottrina, si veda M. GAGLIARDI, *La prova del danno non patrimoniale in caso di trattamento illecito di dati personali*, in *Danno e resp.*, 2016, p. 378, secondo cui le norme che disciplinano le singole attività di trattamento dei dati personali possono essere fattivamente utilizzate per estrapolare parametri in grado di influenza la maggiore o minore pericolosità per l'individuo delle operazioni sui suoi dati e conseguentemente influire sulla liquidazione equitativa del danno.

[425] Relativamente a tale filone, si vedano CASS., 23.1.2014, n. 1361, cit., e l'ordinanza di rimessione alle Sezioni Unite: CASS., 6.5.2016, n. 9978, in *Nuova Giur. Civ. Comm.*, 2016, p. 1287.

tipologia di danno[426].

Con riguardo al trattamento illecito di dati personali nell'ambito dell'attività giornalistica e al correlato bilanciamento tra diritto di cronaca, dall'un lato, e diritto alla riservatezza e protezione dei dati personali, dall'altro, si è raggiunta una qualche uniformità nei parametri utilizzati ai fini della quantificazione del danno non patrimoniale[427].

Al di fuori del contesto giornalistico e televisivo in generale, in relazione alla liquidazione del danno da trattamento illecito *tout court* le pronunce giurisprudenziali si mostrano scarsamente uniformi[428].

Si reputa quantomai necessario un intervento in tal senso in occasione della prossima revisione delle tabelle di liquidazione del danno alla persona da parte del Tribunale di Milano, elaborato dall'Osservatorio sulla Giustizia civile, considerato fonte autoritativa di riferimento nazionale.

Di fronte ad un atteggiamento ancora incerto rispetto alla liquidazione del danno non patrimoniale, si è portati a rimeditare sul ruolo e la funzione del rimedio risarcitorio del danno non patrimoniale derivante da violazione della *privacy*.

Tale rimedio, infatti, si mostra difficilmente conciliabile con la finalità reintegrativa tradizionalmente assolta dall'istituto. Nell'ambito della tutela dei dati personali, ma anche, più in generale, in tutto il contesto della tutela della persona, risultano talmente evidenti i limiti di operatività di tale rimedio che vi è chi ha contestato l'importanza della regola della responsabilità civile in questa materia[429].

Tali limiti originano, principalmente, dal carattere non omogeneo del ristoro riconosciuto e del pregiudizio patito dal danneggiato che, stante la peculiare natura del bene protetto (i diritti e le libertà fondamentali della persona e, in particolare, il diritto alla protezione dei dati personali), sfugge ad una valutazione in termini economici e di natura oggettiva.

---

[426] E. TOSI, *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale*, cit., p. 244.

[427] Sul tema, si vedano in giurisprudenza: TRIB. MILANO, 26.11.2004, in *Giust*., 2005, I, p. 1383; TRIB. MILANO, 13.4.2000; TRIB. LIVORNO, 19.2.2010; TRIB. ROMA, 12.1.2010. Tali parametri sono stati individuati, principalmente, nella potenzialità diffusiva della notizia (con particolare riguardo all'estensione spazio temporale-raggiunta), nella rilevanza data nelle pagine del giornale, nelle conseguenze negative che discendono al soggetto leso sul piano della sfera sociale, economico-professionale e nell'ambiente familiare, oltre che nella gravità dell'offesa arrecata.

[428] Vengono considerati parametri quali: la durata dell'attività illecita (in specie, il protrarsi delle intrusioni, il numero di messaggi indesiderati ricevuti: *cfr*. TRIB. LATINA, 19.6.2006); le modalità e gli effetti del trattamento e della diffusione dei dati (nello specifico, l'effetto mediatico causato dalla successiva diffusione tramite i mezzi di informazione: *cfr*. CASS., 15.7.2014, n. 16133); la tipologia e la gravità delle violazioni commesse; la condizione soggettiva del danneggiato (rilevando altresì la relazione tra persona offesa e autore delle condotte illecite); il senso di turbamento e di ansia ingenerati nel soggetto leso coinvolto (*cfr*. TRIB. MILANO, 3.10.2012).

[429] D. CARUSI, *La responsabilità*, in *La disciplina del trattamento dei dati personali*, a cura di V. CUFFARO-V. RICCIUTO, Giappichelli, 1997, pp. 351 ss.; F. GRITTI, *La responsabilità civile nel trattamento dei dati personali*, in *Il codice del trattamento dei dati personali*, a cura di V. CUFFARO-R. D'ORAZIO-V. RICCIUTO, Giappichelli, 2007, p. 142; M. AMBROSOLI, *La tutela dei dati personali e la responsabilità civile*, in *Riv. dir. priv*., 1998, p. 297; V. CALDERAI, *Danno da lesione dell'identità e della riservatezza e il trattamento illecito dei dati personali*, in *Il danno non patrimoniale. Principi, regole e tabelle per la liquidazione*, a cura di E. NAVARRETTA, cit., pp. 283 ss.

Il valore-persona, una volta leso, non può essere ricostituito. Di conseguenza, il riconoscimento di una somma di denaro a titolo di risarcimento del danno non patrimoniale rischierebbe di perdere la funzione reintegrativa venendo, piuttosto, ad assolvere una funzione solidaristico-satisfattiva. L'attribuzione di una somma di denaro finisce con il rappresentare una consolazione per il male subito, non potendo certo corrispondere al controvalore della perdita subita dalla vittima in conseguenza dell'illecito[430].

13. I danni risarcibili negli altri Stati UE

Anche la dottrina europea ha evidenziato il problema della risarcibilità, in termini di definizione e di quantificazione[431], dei danni "immateriali" derivanti da illecito trattamento di dati[432].

Tendenzialmente per danni materiali vengono intese tutte le conseguenze negative di un danno che non sono immediatamente (*per sé*) soggette a una valutazione in termini monetari; tuttavia, è difficile trovare definizioni generali che li descrivano in modo positivo e che ne coprano tutte le sfaccettature.

Il GDPR non fornisce linee guida sulla valutazione dei danni, limitandosi ad affermare al Considerando n. 146 che gli interessati devono ricevere pieno ed effettivo risarcimento e questo comporta un grave problema di uniformità nell'applicazione del Regolamento all'interno degli Stati Membri.

In data 21.5.2021 l'Oberster Gerichtshof (Austria) ha proposto alla Corte di Giustizia domanda di pronuncia pregiudiziale[433] sulle seguenti questioni:

> 1) Se ai fini del riconoscimento di un risarcimento ai sensi dell'articolo 82 del regolamento (UE) 2016/679 (1) (RGPD) occorra, oltre a una violazione delle disposizioni dell'RGPD, che il ricorrente abbia patito un danno, o se sia già di per sé sufficiente la violazione di disposizioni dell'RGPD per ottenere un risarcimento.
>
> 2) Se esistano, per quanto riguarda il calcolo del risarcimento, altre prescrizioni di diritto dell'Unione, oltre ai principi di effettività e di equivalenza.
>
> 3) Se sia compatibile con il diritto dell'Unione la tesi secondo cui il presupposto per il riconoscimento di un danno immateriale è la presenza di una conseguenza o di un effetto della

---

[430] Così M. GAMBINI, *Principio di responsabilità e tutela aquiliana dei dati personali*, cit., pp. 120 ss.

[431] Si v. M. J. RADIN, *Compensation and commensurability* in *Duke LJ*, 1993, pp. 56-86, che osserva "*when someone who has lost an arm in an accident receives $100,000 in compensation through the tort system, what does this transaction mean? Does it mean that an arm is "worth" $100,000? […] I will suggest that our legal practice reflects conflict in how compensation for personal injury is understood-that compensation is a contested concept. A commodified conception of compensation, in which harm to persons can be equated with a dollar value, coexists with a noncommodified conception, in which harm cannot be equated with dollars. In the commodified conception, harm and dollars are commensurable, and in the noncommodified conception, they are incommensurable*".

[432] J. KNETSCH, *op. cit.*

[433] Causa C-300/21, 2021/C 320/24, *UI v. Österreichische Post AG*.

violazione di un diritto avente almeno un certo peso e che vada oltre l'irritazione provocata dalla violazione stessa.

La domanda di pronuncia pregiudiziale dimostra l'incertezza interpretativa della Corte austriaca sia nell'accertamento dell'*an debeatur*, sia nell'accertamento del *quantum* dell'obbligazione risarcitoria. Inoltre, con la terza questione propone alla Corte di Giustizia il medesimo dibattito, attuale anche in Italia, attorno alla soglia di risarcibilità dei danni conseguenti alla violazione di diritti personali.

È evidente che l'assenza nel Regolamento di criteri precisi per l'accertamento e la quantificazione del danno può comportare applicazioni particolarmente difformi negli Stati membri, con il rischio di una perdita di effettiva della disciplina di protezione dei dati.

Ad esempio, in UK (prima del recesso dai Trattati) i danni non patrimoniali vengono liquidati attraverso le *Guidelines for the Assessment of General Damages in Personal Injury Cases* del Judicial College[434] che indicano valori di riferimento sulla base dei precedenti giurisprudenziali.

In Francia vi sono delle tabelle di riferimento denominate "*Référentiel Mornet*"[435].

In alcuni stati membri dell'UE, come Francia e Belgio, la dottrina prevalente ritiene insostenibile l'idea che un risarcimento possa essere rifiutato per il fatto che la lesione non abbia raggiunto una certa soglia di rilevanza[436].

In altri Stati, come Italia e Germania, viene richiesta una lesione "grave" al diritto alla personalità per il riconoscimento del diritto al risarcimento.

Nello specifico, in due differenti casi un tribunale tedesco, pur riconoscendo la violazione alla disciplina di protezione dei dati personali, non ha riconosciuto il risarcimento:

1) nel primo caso il tribunale ha osservato che la lesione era da considerarsi "banale"; in particolare il tribunale ha affermato che "*Dass dem Kläger durch die Sperrung ein materieller oder immaterieller Schaden im Sinne des Art. 82 DSGVO entstanden wäre, kann der Senat überdies nicht erkennen. Die bloße Sperrung seiner Daten stellt ebenso wie der Datenverlust noch keinen Schaden im Sinne der DSGVO dar (Wybitu/Haß/Albrecht, NJW 2018 S. 113 (114). Die behauptete Hemmung in der Persönlichkeitsentfaltung durch die dreitägige Sperrung hat allenfalls Bagatellcharakter (s.o.). Auch wenn in der Literatur unter Bezug auf Erwägungsgrund 146 der DSGVO vereinzelt die Auffassung vertreten wird, eine wirksame Durchsetzung europäischen Datenschutzrechts erfordere einen Abschreckungseffekt und den*

---

[434] JUDICIAL COLLEGE*, Guidelines for the Assessment of General Damages in Personal Injury Cases*, Oxford, 2019.

[435] *L'indemnisation des Prejudices en cas de blessures ou de décès*, pubblicato nel settembre 2021, a cura di Benoît Mornet (*Conseiller à la Cour de cassation*).

[436] J. KNETSCH, *op. cit.*; sul tema si v. inoltre J. POHLE, *Data Privacy Legislation In The European Union Member States– A Pratical Overview. How EU Member States have adjusted their domestic data privacy law to the GDPR,* in *Computer Law Review International*, 2018, pp. 97-116, ove l'autore analizza le principali normative nazionali adottate dagli Stati membri per l'attuazione del GDPR.

Verzicht auf die nach bisherigem Recht (vgl. hierzu BGH, Urteil vom 29.11.2016 - VI Z 530/15) geltende Erheblichkeitsschwelle (Gola, DSGVO, 2. Aufl. Art 82 Rn 13 m.w.N.; so auch AG Dietz, Urteil vom 7.11.2018 - 8 C 130/18 -juris), rechtfertigt dies keinen Ausgleich immaterieller Bagatellschäden"[437];

2) nel secondo caso il tribunale ha osservato che anche se non è necessaria una violazione grave dei diritti personali, per il risarcimento deve comunque essere apprezzabile in via oggettiva l'esistenza di un danno; il Tribunale afferma che "*Einerseits ist eine schwere Verletzung des Persönlichkeitsrechts nicht (mehr) erforderlich. Andererseits ist auch weiterhin nicht für einen Bagatellverstoß ohne ernsthafte Beeinträchtigung bzw. für jede bloß individuell empfundene Unannehmlichkeit ein Schmerzensgeld zu gewähren; vielmehr muss dem Betroffenen ein spürbarer Nachteil entstanden sein und es muss um eine objektiv nachvollziehbare, mit gewissem Gewicht erfolgte Beeinträchtigung von persönlichkeitsbezogenen Belangen gehen*"[438].

A seguito di questo primo approccio restrittivo, tuttavia, anche nei tribunali tedeschi si registra ora una tendenza a riconoscere più facilmente i danni immateriali conseguenti al trattamento illecito[439].

Nei Paesi Bassi, sono giunti alla Corte d'appello quattro casi in cui il tribunale di primo grado aveva riconosciuto un risarcimento pari ad € 500[440]. In tre casi la Corte ha riformato la sentenza e rigettato la domanda, osservando che la mera violazione di un diritto fondamentale non determina automaticamente il diritto al risarcimento del danno e il danneggiato non aveva dimostrato il superamento di una certa soglia di tollerabilità[441]; in un altro caso il tribunale olandese ha riconosciuto un risarcimento pari ad € 250 per l'ansia e lo stress causati dalla divulgazione illecita di dati personali[442].

Evidente, dunque, la diffusa incertezza interpretativa sul concetto di danni immateriali: se il Regolamento, infatti, ribadisce più volte che il risarcimento deve essere "effettivo", di fatto non indica

---

[437] OBERLANDESGERICHT DRESDEN BESCHL., v. 11.06.2019, Az.: 4 U 760/19, all'indirizzo https://www.iww.de/quellenmaterial/id/218575.

[438] AMTSGERICHT DIEZ SCHLUSSURTEIL, v. 7.11.2018 - 8 C 130/18, all'indirizzo https://openjur.de/u/2116788.html.

[439] Si v. ad esempio, DARMSTADT REGIONAL COURT, 26.5.2020, case no. 13 O 244/19; LÜBECK LABOR COURT, 20.6.2020, case no. 1 Ca 538/19; NEUMÜNSTER LABOR COURT, 11.8.2020, case no. 1 Ca 247 c/20; DRESDEN LABOR COURT, 26.8.2020, case no. 13 Ca 1046/20, tutte in https://dejure.org/.

Si v. anche il rapporto LATHAM & WATKINS, *GDPR Violations in Germany: Civil Damages Actions on the Rise*, 21.12.2020, all'indirizzo https://www.jdsupra.com/legalnews/gdpr-violations-in-germany-civil-84570/

[440] Si v. gli esempi contenuti nella ricerca M. N. LINTVEDT, *Putting a price on data protection infringement* in *International Data Privacy Law,* Vol. 00, No. 0, 2021, pp. 1-15.

[441] RaadVanState Uitspraak 201905087/1/A2, all'indirizzo https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RVS:2020:899.

[442] Rechtbank Amsterdam 7560515 CV EXPL 19-4611, all'indirizzo https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2019:6490.

alcun criterio o parametro per il suo accertamento e quantificazione, con il rischio di una differenza di uniformità rilevante sul territorio UE, che comporta una forte perdita di effettività della disciplina di protezione dei dati. Nell'ambito del GDPR, si ripercuote con forza il problema della risarcibilità dei danni non patrimoniali conseguenti a lesioni dei diritti della personalità, che generano danni non direttamente apprezzabili in termini economici.

Sul punto, è stata osservata l'importanza del principio di effettività dei rimedi privatistici per la tutela dei dati[443], in quanto "*claims for compensation are an important part of the enforcement architecture of the GDPR. Private enforcement will help to discourage infringements of the rights of data subjects; it will make a significant contribution to the protection of privacy and data protection rights in the European Union; and it will help to ensure that the great promise of the GDPR is fully realized*"[444].

Ma questo problema di effettività origina anche dal fatto che la prospettiva della disciplina dei dati e ancora eccessivamente focalizzata sull'individuo, al cui solo viene demandata la scelta di azionare i rimedi privatistici.

[443] "*To ensure that any person who has suffered such damage has an effective remedy pursuant to Article 47 CFR, Member States will have to provide, pursuant to Article 19TEU, remedies sufficient to ensure effective legal protection in the fields of privacy and data protection. In particular, they will have to provide expressly for a claim for compensation, incorporating Article 82(1) GDPR into national law*" (E. O'DELL, *Compensation for breach of the general data protection regulation* in *Dublin ULJ*, 2017, pp. 97-164).

[444] ID., *op. cit.,* p. 148.

Conclusioni

La prima parte del lavoro è stata dedicata all'evoluzione che ha portato all'affermazione del diritto alla protezione dei dati, quale espressione del diritto alla *privacy*, tenendo in considerazione il contesto tecnologico in cui tale riconoscimento è maturato. Le principali teorie della dottrina e della giurisprudenza statunitensi che hanno contribuito all'affermazione del diritto alla *privacy* lo hanno inteso in chiave essenzialmente personalistica. Ed infatti questa concezione individualistica è approdata nella dottrina europea e italiana che successivamente si sono occupate di diritto alla riservatezza.

A seguito dello sviluppo tecnologico degli anni '60 (in particolare il diffondersi delle banche dati e degli elaboratori elettronici), da cui derivano rischi di discriminazione per le minoranze, si sono affermate forme di tutela per la protezione dei dati personali.

Tuttavia, ancorché si trattasse di rischi fortemente sociali e collettivi, il diritto alla protezione dei dati è stato conformato in chiave essenzialmente individuale. Ed infatti questo diritto presenta notevoli punti di contatto con il diritto alla riservatezza, il diritto all'identità personale, il diritto all'autodeterminazione.

Si è tuttavia evidenziata l'esistenza di un orientamento minoritario, di origine transazionale, secondo cui il diritto alla *privacy* e la *data protection* devono essere tenute del tutto distinti, in quanto solo la privacy sarebbe un diritto, mentre la *data protection* sarebbe esclusivamente una legislazione finalizzata a proteggere i cittadini da alcune nuove tecnologie. Questa tesi presenta il notevole pregio di esaltare non solo la funzione individualistica di questo diritto, ma anche gli interessi sociali che vi sono connessi.

Dunque, sebbene non possa negarsi la portata personale del diritto alla *privacy*, sembra potersi condividere questo orientamento laddove evidenzia i punti in comune della disciplina per la protezione dei dati personali con la disciplina per la protezione dell'ambiente, che predispone meccanismi e procedure per la gestione dei rischi ambientali e per la salute umana.

L'evoluzione esponenziale degli strumenti tecnologici dell'epoca moderna mette in crisi la concezione del diritto alla protezione dei dati in chiave essenzialmente individualistica. In particolare, la creazione di internet, le piattaforme informatiche, i *social network*, lo sviluppo dell'intelligenza artificiale e gli algoritmi predittivi, rischiano di rendere del tutto inefficiente ed inadeguato un sistema di tutela basato su una concezione meramente personalistica del diritto alla protezione dei dati. L'intera disciplina del trattamento dei dati ruota, infatti, attorno ai concetti di consenso e di informazione dell'utente, i quali sono, tuttavia, categorie classiche di diritto civile che poco s'attagliano per le nuove istanze sociali di protezione dei dati.

Nello specifico, è noto che ormai dagli anni '70 una parte della dottrina ha iniziato a sottolineare il "valore sociale" della *privacy* e i nuovi rischi per la società derivanti dall'utilizzo dei dati personali.
Il sistema di tutela inteso in chiave essenzialmente personalistica non è in grado di offrire sempre una tutela adeguata ed efficiente.
Questo è dimostrato dallo studio del caso di Cambridge Analytica, che attraverso la raccolta e l'utilizzo illeciti di dati personali e algoritmi di profilazione basati su *big data* e intelligenza artificiale, ha determinato un'alterazione delle volontà elettorali dei cittadini durante la campagna elettorale.
Inoltre, ulteriori rischi, di tipo sociale/collettivo, attengono al tema della sorveglianza e della manipolazione della volontà esercitata tramite sorveglianza.
Per approfondire maggiormente questa problematica, è stato necessario muovere l'analisi da un approccio interdisciplinare, relativo alle cd. tre fasi delle teorie della sorveglianza sociale, analizzate dalla filosofia del diritto e dalla sociologia, scienze che si sono occupate del fenomeno del controllo sociale, anche nell'era digitale: 1) il *Panopticon* di Bentham e il successivo sviluppo di Foucault; 2) le teorie post-panottiche della sorveglianza (Deleuze, Guattari); 3) le concettualizzazioni contemporanee della sorveglianza e il capitalismo della sorveglianza di Zuboff.
Questa analisi ha portato alla luce particolare particolari interessi collettivi legati all'uso dei dati, che è possibile tutelare solo da una prospettiva più ampia, che non lasci al singolo danneggiato la possibilità di esercitare rimedi di tipo privatistico, secondo una classica concezione della responsabilità civile.
Solo tenendo in considerazione i valori sociali che devono essere protetti da un sistema di responsabilità civile è possibile valutarne effettivamente l'adeguatezza.
L'analisi si è, dunque, spostata sul terreno dell'art. 82 GDPR, per individuarne esattamente la portata applicativa.
Dopo aver analizzato la figura del danneggiato (tenendo in considerazione il dibattito sulla trasmissibilità *mortis causa* del diritto alla protezione dei dati), il percorso argomentativo si è soffermato sui differenti soggetti coinvolti nel trattamento (titolare, responsabile contitolare, responsabile "intero", responsabile per la protezione dei dati) e, in particolare, sul riparto di responsabilità tra questi soggetti e il rapporto di responsabilità che li lega direttamente al danneggiato.
In seguito, si è dedicata attenzione alla nozione di illiceità del trattamento e, dunque, ai principi del trattamento enunciati dal GDPR (liceità, necessità, correttezza, trasparenza, finalità, qualità, *accountability*).
Dall'analisi di questi principi sembrano potersi evidenziare due tendenze.
Innanzitutto, un ruolo ancora fondamentale è rivestito dal consenso, come condizione di liceità che rende possibile il trattamento. Esso sottende che l'interessato sia in grado di ponderare esattamente i

rischi conseguenti al trattamento, con la conseguenza che il consenso assorbe e supera la necessità di qualsiasi altro bilanciamento tra diritti, che invece viene richiesto qualora il trattamento si fondi su una differente "base giuridica". Tuttavia, si tratta di un assunto che confligge con l'attuale società tecnologica: l'utilizzo dei *big data* e degli algoritmi di intelligenza artificiale consentono di aggregare i dati raccolti da dispositivi differenti e potenzialmente distanti nel tempo e nel luogo, per ricavare dati anche particolarmente personali. Un meccanismo di tutela ancora fondato sul consenso determina perciò una forte perdita di effettività del sistema di tutela dei dati.

La seconda tendenza della disciplina è quella di focalizzarsi maggiormente sulla figura del titolare, su cui gravitano obblighi pregnanti, in particolare quello di *accountability*. Il titolare, in quanto soggetto che tratta direttamente i dati, può individuare meglio di chiunque altro i rischi conseguenti ai trattamenti e, dunque, è tenuto a svolgere un'attività di ponderazione dei rischi per mettere in atto misure tecniche e organizzative per evitarli o mitigarli. Egli è tenuto a monitorare costantemente i processi della sua attività imprenditoriale che involgono l'utilizzo di dati ed è tenuto a conformare la propria attività nell'osservanza dei principi del GDPR.

Nell'ultima parte, la ricerca è stata dedicata alla natura e alla disciplina della responsabilità per illecito trattamento dei dati personali, alla luce dei differenti orientamenti della dottrina e della giurisprudenza (anche in relazione alla disciplina previgente di cui all'art. 15 d.lgs. n. 196/2003). Questi si muovono sostanzialmente tra una responsabilità di tipo oggettivo e una responsabilità per colpa presunta o aggravata, in ogni caso viene evidenziata la forte responsabilizzazione gravante sul titolare, tenuto a predisporre tutte le misure organizzative e di sicurezza adeguate a prevenire il danno; egli è tenuto, in un'ottica proattiva, ad attivarsi per individuare i possibili rischi, ponendo in essere un'adeguata operazione di *risk management*, che conformi la struttura organizzativa dell'impresa verso un fine di *compliance* ai principi del GDPR. La dottrina europea mette l'accento, per evidenziare il particolare livello di responsabilità disegnato dall'art. 82 GDPR, sul cd. *duty of care* gravante sul titolare, che sebbene non imponga un'obbligazione di risultato in senso proprio, determina una responsabilità considerata, per lo più, a titolo oggettivo.

L'analisi ha evidenziato l'acceso dibattito che ruota attorno al problema dei danni risarcibili a seguito di trattamento illecito, con riferimento specifico alla questione dei danni non patrimoniali.

Per affrontare la questione, dapprima si sono ripercorse le tappe evolutive della giurisprudenza sui danni non patrimoniali: *i*) l'intervento delle sentenze gemelle della Cassazione del 2003 (confermate dalla Corte costituzionale), *ii*) la successiva reinterpretazione offerta dalle decisioni gemelle di San Martino del 2008, *iii*) il recente decalogo di controriforma della Terza Sezione civile della Cassazione del 2018.

Questo quadro generale sul danno non patrimoniale è stato, in seguito, calato all'interno della

responsabilità per illecito trattamento dei dati.

L'analisi ha confermato che per la giurisprudenza maggioritaria, l'illecito trattamento di dati personali, sebbene comportante l'ingiustificata lesione del diritto fondamentale alla protezione dei dati personali, richiede che tale violazione abbia determinato in concreto una lesione che, andando oltre la soglia di tollerabilità, ne renda significativamente apprezzabile la portata e costituzionalmente meritevole il ristoro. Di qui, l'esclusione di ogni forma di automatismo che consideri risarcibile *in re ipsa* il danno di natura immateriale derivante da illecito trattamento di dati personali, dovendo, al contrario, subordinarsi l'accesso alla tutela risarcitoria ai citati parametri-soglia. Non ogni mera violazione dei principi e delle regole di condotta poste dal GDPR determina una lesione ingiusta del diritto tutelato ma unicamente quella che ne offenda in modo sensibile la sua portata effettiva.

Questo orientamento è stato criticato da una parte della dottrina, favorevole al riconoscimento della tutela risarcitoria al verificarsi di ogni condotta realizzata in spregio alle regole conformative previste in materia, a prescindere dalla prova del pregiudizio subito in concreto.

Tuttavia, questo orientamento arriva quasi a sovvertire i principi fondamentali della responsabilità aquiliana, saldamente ancora ad una funzione prettamente compensativa: i tentativi di ampliare la tutela risarcitoria attraverso la totale eliminazione dei requisiti della prova della gravità e serietà del danno sembrano negare totalmente tale funzione compensatoria, per riconoscere una funzione esclusivamente sanzionatoria-punitiva della responsabilità civile. Evidentemente questa tesi si pone l'obbiettivo di trovare una soluzione concreta per un assai difficilmente risolvibile problema, quello della individuazione, quantificazione e prova dei danni non patrimoniali conseguenti alla lesione di un diritto alla personalità.

Si tratta di un'annosa questione che nasce dalla circostanza stessa che, in tale ambito, il danno non è in origine una misura economicamente apprezzabile in modo oggettivo: si tratta, pur sempre, di riconoscere un equivalente monetario ad una lesione "spirituale".

Ciò è chiaramente avvertito anche nella dottrina europea, ove si registrano differenti prese di posizione in ordine al problema della risarcibilità, in termini di definizione e quantificazione, dei danni immateriali derivanti da illecito trattamento.

Questo è dimostrato anche dalla recente domanda di pronuncia pregiudiziale proposta dalla Corte suprema austriaca, che ha[445] chiesto alla Corte di giustizia UE:

1. Se ai fini del riconoscimento di un risarcimento ai sensi dell'articolo 82 del regolamento (UE) 2016/679 (1) (RGPD) occorra, oltre a una violazione delle disposizioni dell'RGPD, che il ricorrente abbia patito un danno, o se sia già di per sé sufficiente la violazione di disposizioni

[445] OBERSTER GERICHTSHOF (Austria), 21.5.2021, causa C-300/21, 2021/C 320/24, *UI v. Österreichische Post AG*.

dell'RGPD per ottenere un risarcimento.

2. Se esistano, per quanto riguarda il calcolo del risarcimento, altre prescrizioni di diritto dell'Unione, oltre ai principi di effettività e di equivalenza.
3. Se sia compatibile con il diritto dell'Unione la tesi secondo cui il presupposto per il riconoscimento di un danno immateriale è la presenza di una conseguenza o di un effetto della violazione di un diritto avente almeno un certo peso e che vada oltre l'irritazione provocata dalla violazione stessa.

Anche l'analisi di alcune sentenze della giurisprudenza di merito tedesca e belga hanno dimostrato che il problema della "soglia di risarcibilità" dei danni immateriali è diffuso a livello europeo.

Si tratta di questioni su cui dovrà attendersi l'opera interpretativa della Corte di giustizia, chiamata, comunque, a dare soluzione ad una questione che non può che essere risolta per approssimazione.

Nella parte conclusiva del lavoro, si è analizzato il contenuto della prova liberatoria, che essenzialmente consiste nella dimostrazione di aver gestito adeguatamente i rischi per i diritti e le libertà degli interessati conseguenti ai trattamenti.

Il GDPR predispone, infatti, un modello di gestione del rischio che impone al titolare di mantenere un approccio proattivo nel prevenire i rischi, dotandosi di una struttura organizzativa che, a tutti i livelli e in tutte le aree di competenza, adotti le necessarie misure per garantire che i dati personali siano trattati sempre in modo lecito. Questo schema di gestione si compone delle seguenti fasi: i) definizione del contesto; ii) identificazione dei rischi; iii) analisi del rischio; iv) valutazione dei rischi; v) controllo dei rischi, fase che a sua volta si divide in due segmenti, il primo dedicato alla preparazione ed approvazione del "piano di azione dei rischio" (*risk action plan*) e nel segmento di esecuzione, controllo e modifica del piano.

Tenendo in considerazione anche le decisioni e i pareri delle autorità di controllo, si sono dunque approfonditi i principali obblighi di *risk management* gravanti sul titolare (la mappatura dei processi, la *privacy by design* e *by default*, la valutazione d'impatto, le violazioni di sicurezza), che possono comportano, nei casi di strutture imprenditoriali particolarmente complesse, la necessità di integrazione della gestione del rischio privacy nei sistemi organizzativi d'impresa (d.lgs. n. 231/2001 e norme ISO 9001 e ISO 27001).

Si tratta, dunque, di un modello di obblighi (e conseguente responsabilità) elastico, che consente di adeguarsi in rapporto alle dimensioni del titolare, nonché alla particolarità dei trattamenti dallo stesso eseguiti: maggiori sono i rischi per i diritti e le libertà degli interessati, più incisive dovranno essere le misure di sicurezza che il titolare dovrà predisporre.

Dall'analisi specifica della prova liberatoria, sembra emergere, dunque, che la responsabilità per illecito trattamento di dati personali deve essere intesa specificamente quale responsabilità da rischio

d'impresa, in quanto tesa a far ricadere sul titolare i rischi conseguenti al trattamento, proprio perché è questo il soggetto che, dall'un lato ricava un'utilità diretta dal trattamento, dall'altro può governare e controllare tali rischi e, pertanto, è specificamente obbligato a farlo.

Questo sistema di tutela fondato sull'*accountability* non sembra, tuttavia, ancora del tutto adeguato. Innanzitutto, l'accountability obbliga a gestire i rischi per i diritti e le libertà degli individui, mentre non considera adeguatamente i rischi sociali/collettivi conseguenti all'utilizzo dei dati personali. Inoltre, la stessa disciplina della responsabilizzazione dovrebbe considerare obblighi di trasparenza notevolmente maggiori per il titolare e prevedere un potere di controllo più persuasivo per l'autorità di controllo. In particolare, il meccanismo della valutazione d'impatto dovrebbe prevedere, in talune ipotesi, il necessario coinvolgimento degli interessati, anche tramite enti o associazioni, e dovrebbe essere imposto l'obbligo di rendere pubblico l'esito delle valutazioni d'impatto nei casi in cui il titolare ritenga di effettuare comunque il trattamento.

Questi risultati dovrebbero, infatti, subire lo scrutinio delle autorità di controllo, le quali dovrebbero verificare la liceità del bilanciamento tra diritti effettuati dal titolare, soprattutto in quei casi in cui il trattamento sia effettuato per finalità di legittimo interesse del titolare.

***

In conclusione, dal lavoro di ricerca sembra essere emerso che, mentre il diritto alla *privacy* è un diritto essenzialmente individualistico, il diritto alla protezione dei dati è, solo parzialmente, un diritto soggettivo. Per poter predisporre strumenti di tutela più efficaci, è necessario abbandonare la concezione prettamente individualista, che comporta un sistema di responsabilità ad azione del singolo: nell'attuale contesto tecnologico, questo rimedio si rivela, in molte ipotesi, di scarso effetto applicativo.

La *data protection* deve essere, più propriamente, considerata quale un insieme di procedure e meccanismi finalizzati ad assicurare agli individui e alla collettività o, comunque, a cerchie determinabili di soggetti, che i dati personali siano trattati secondo principi di liceità, correttezza, responsabilizzazione; quando i trattamenti involgono attività di profilazione e *big data*, dovrebbero essere garantite anche finalità di sviluppo etico e sociale. Il diritto alla protezione dei dati dovrebbe, dunque, considerare maggiormente i rischi collettivi e il sistema di *accountability* essere integrato da obblighi di trasparenza maggiori nonché da un sistema di controlli più penetrante ed incisivo da parte delle autorità di controllo.

Bibliografia

AGABA G. B., AKINDÈS F., BENGTSSON L., COWLS J., GANESH M. I., HOFFMAN N.& OTHERS, *Big data and positive social change in the developing world: a white paper for practitioners and researchers*, in *Rockefeller Foundation Bellagio Centre Conference*, 2014, p. 1;

AL MUREDEN E., *Il futuro del Law and Economics nel pensiero di Guido Calabresi*, in *Riv. dir. civ.*, 2018, p. 778;

ALLEN A. L., *Privacy-as-Data Control: Conceptual, Practical, and Moral Limits of the Paradigm*, in *Connecticut Law Review*, 2000, p. 861;

ALPA G., *Diritto della responsabilità civile,* Laterza, 2003;

ALPA G., *L'identità digitale e la tutela della persona. Spunti di riflessione*, in *Contr. e impr.*, 2017, p. 723;

ALPA G., *La disciplina dei dati personali. Note esegetiche sulla Legge 31 dicembre 1996, n. 675 e successive modifiche,* Seam, 1998;

ALPA G.-BESSONE M., *I fatti illeciti*, in *Trattato di Diritto Privato*, diretto da RESCIGNO P., XIV, Utet, 1982, p. 295;

ALPA G.-BESSONE M., *La responsabilità del produttore*, Giuffrè, 1999;

AMBROSOLI M., *La tutela dei dati personali e la responsabilità civile*, in *Riv. dir. priv*., 1998; p. 297;

ASTONE M. A., *Il danno non patrimoniale nel diritto interno e sovranazionale tra antiche e nuove questioni*, in *Eur. e dir. priv.*, fasc. 4., 1 2018, p. 1183;

BARBIERATO D., *Trattamento dei dati personali e nuova responsabilità civile*, in *Resp. civ. e prev.*, 2019, p. 2151;

BARRA CARACCIOLO F., *La tutela della personalità in Internet*, in *Dir. inform*., 2018, p. 201;

BENN S. I., *Privacy*, *Freedom and Respect for persons*. *Philosophical dimensions of Privacy: an Anthology*, Cambridge University Press, 1984, p. 223;

BENNETT C. J., *Regulating Privacy*, Cornell University Press, Ithace 1992;

BENNETT C. J., *Voter databases, micro-targeting, and data protection law: can political parties campaign* in *Europe as they do in North America?* in *International Data Privacy Law,* Vol. 6, No. 4, 2016, p. 261;

BENTHAM J., *Panopticon ovvero la casa d'ispezione*, a cura di FOUCAULT M.-PERROT M. (traduzione italiana a cura di FORTUNATI V., Marsilio, 1997);

BERGELLI E., *Danno non patrimoniale ed interpretazione costituzionalmente orientata dell'art. 2059,* in *Resp. civ. e prev.,* 2003, p. 691;

BIANCA C. M., *Diritto civile*, *5, La responsabilità*, Giuffrè, 2012;

BIANCA C. M-BUSNELLI F. D., *La protezione dei dati personali. Commentario al D.Lgs. 30 giugno 2003, n. 196*, Cedam, 2007;

BIGO D., *Globalized (in)security: the field and the Ban-opticon,* in SAKAI N.-SOLOMON J., *Traces 4: Translation, Biopolitics, Colonial difference,* Hong Kong, 2006, p. 109;

BILOTTA F., *La responsabilità nel trattamento dei dati personali*, in *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 2016/679 (GDPR) e al novellato d.lgs. n. 196/2003 (Codice Privacy)*, a cura di PANETTA R., Giuffrè, 2019, p. 445;

BINNS R., *Data protection impact assessments: a meta-regulatory approach* in *International Data Privacy Law,* Vol. 7, No. 1, 2017, p. 22;

BISTOLFI C., *Le obbligazioni di compliance in materia di protezione dei dati personali*, in *Il Regolamento Privacy europeo, Commentario alla nuova disciplina sulla protezione dei dati personali*, a cura di BOLOGNINI L.-PELINO E.-BISTOLFI C., Giuffrè, 2016, p. 321;

BLACK E., *L'IBM e l'olocausto. I rapporti fra il Terzo Reich e una grande azienda americana*, Rizzoli, 2001;

BLAND R. L., *Book Notes*, *Washington and Lee Law Review*, Vol. 25, 1968;

BOHM A. S.-GEORGE E. J.-CYPHERS B.-LU S., *Privacy and Liberty in an Always-on, Always-listening World* in *The Columbia Science & Technology Law Review,* 2017, p. 1;

BOLLIER D., *The promise and peril of big data*, The Aspen Institute, 2010;

BOLOGNINI L.-PELINO E.-BISTOLFI C., *Il Regolamento Privacy Europeo. Commentario alla nuova disciplina sulla protezione dei dati personali,* Giuffrè, 2016;

BRANDIMARTE L.-ACQUISTI A.-LOEWENSTEIN G., *Misplaced confidences: Privacy and the control paradox* in *Social psychological and personality science,* 2012;

BRAVO F., *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, Cedam, 2018;

BRAVO F., *Riflessioni critiche sulla natura della responsabilità da trattamento illecito dei dati personali*, in *Persona e mercato dei dati*, a cura di ZORZI N.-GALGANO F., Giuffrè, 2019, p. 383;

BRAVO F., *Software di intelligenza artificiale e istituzione del registro per il deposito del codice sorgente*, in *Contr. e impr.*, 2020, p. 1422;

BRAVO F., *Sul bilanciamento proporzionale dei diritti e delle libertà "fondamentali", tra mercato e persona: nuovi assetti dell'ordinamento europeo*?, in *Contr. e impr.*, 2018, p. 190;

BRAVO F., *Sulla figura del responsabile "interno" del trattamento dei dati personali*, in *Dir. inf. e inform.*, 2019, p. 951;

BUSNELLI F. D., *Le Sezioni Unite e il danno non patrimoniale*, in *Riv. dir. civ*., 2009, p. 105;

BUSNELLI F. D., *Le Sezioni Unite e il danno non patrimoniale*; in *Giur. it*., 2009, p. 259 (nota a CASS. sez. un., 11.11.2008, n. 26972, n. 26973, n. 26974 e n. 26975);

BUSNELLI F. D., voce «*Illecito civile*», in *Enc.giur.*, XV, Treccani, 1989;

BUTTARELLI G., *Banche dati e tutela della riservatezza*, Giuffrè, 1997;

CALABRESI G., *Costo degli incidenti e responsabilità civile. Analisi economico-giuridica*, trad. di DE VITA A.-VARANO V.-VIGORITI V., Giuffrè, 1975;

CALABRESI G., *Ideals, beliefs, attitudes, and the law: private law perspectives on a public law problem*, Syracuse, 1985;

CALABRESI G., *The Cost of Accidents: A Legal and Economic Analysis*, New Haven 1970;

CALABRESI G.., *The Future of Law and Economics*, New Haven, 2016;

CALDERAI V., *Danno da lesione dell'identità e della riservatezza e il trattamento illecito dei dati personali*, in *Il danno non patrimoniale. Principi, regole e tabelle per la liquidazione*, a cura di NAVARRETTA E., Giuffrè, 2010, p. 283;

CAMARDI C., *L'eredità digitale. Tra reale e virtuale*, in *Dir. inf. e inform*., 2018, p. 79;

CARDARELLI F.-SICA S.-ZENO-ZENCOVICH V., *Il codice dei dati personali. Temi e problemi*, Giuffrè, 2004;

CARNELUTTI F., *Il diritto alla vita privata,* in *Riv. trim. dir. pubbl.*, 1955, p. 3;

CARUSI D., *La responsabilità*, in. *La disciplina del trattamento dei dati personali*, a cura di CUFFARO V.-RICCIUTO V., Giappichelli, 1997;

CASO R., *La società della mercificazione e della sorveglianza: dalla persona ai dati. Casi e problemi di diritto civile*, Ledizioni, 2021;

CASSANO G. G.- COLAROCCO V.- GALLUS G. B.- MICOZZI F. P., *Il processo di adeguamento al GDPR aggiornato al D.Lgs. 10 agosto 2018, n. 101*, Giuffrè, 2018;

CASSANO G., *Danno non patrimoniale ed esistenziale: primissime note critiche a Cassazione civile, Sezioni Unite, 11 novembre 2008, n. 25972;* in *Giur. it.,* 2009, p. 317 (nota a CASS., sez. un., 11.11.2008, n. 26972, n. 26973, n. 26974 e n. 26975);

CASTRONOVO C., *La nuova responsabilità civile*, Giuffrè, 2018;

CASTRONOVO C., *Responsabilità civile*, Giuffrè, 2018;

CASTRONOVO C., *Situazioni soggettive e tutela nella legge sul trattamento delle informazioni personali*, in *Eur. e dir. priv*., 1998, I, p. 677;

CECCARELLI V., *La soglia di risarcibilità del danno non patrimoniale da illecito trattamento dei dati personali*, in *Danno e resp*., 2015, p. 339 (nota a CASS., 15.7.2014, n. 16133);

CENDON P., *Anche se gli amanti si perdono l'amore non si perderà. Impressioni di lettura su Cass.,*

8828/2003, in *Resp. civ. e prev*., 2003, p. 675 (note a CASS., 31.5.2003, n. 8827; CASS., 31.5.2003, n. 8828);

CENDON P.-ZIVIZ P., *Risarcimento del danno esistenziale*, Giuffrè, 2003;

CHINÈ G.-ZOPPINI A., *Manuale di diritto civile,* Neldiritto, 2018;

CINQUE A., *Privacy, big-data e contact tracing; il delicato equilibrio fra diritto alla riservatezza ed esigenze di tutela della salute*, in *Nuova. giur. civ. comm*., 2021, p. 957;

CINQUE M., *L'"eredità digitale" alla prova delle riforme*, in *Riv. dir. civ.*, 2020, p. 72;

CLARKE R., *Information technology and dataveillance*, Communications of the ACM, 1988;

CODIGLIONE G., *I dati personali come corrispettivo della fruizione di un servizio di comunicazione elettronica e la "commercializzazione" della privacy*, in *Dir. inf. e inform*., 2017, p. 418 (commento a AGCM, 11.5.2017);

COHEN J. E., *What privacy is for* in *Harward Law Review,* 2013, Vol. 126: 1934, p. 1904;

COLLEY T. C., *A treatise on the Law of Torts or the Wrongs which arise indipendent of Contract*, Callaghan & Company, Chicago, 1889;

COLONNA V., *Il danno da lesione della privacy, in Danno e resp*., 1999, p. 18;

COLONNA V., *Il sistema della responsabilità civile da trattamento dei dati personali*, in *Diritto alla riservatezza e circolazione dei dati personali*, a cura di R. PARDOLESI, Giuffrè, 2003, II, p. 53;

COMANDÈ G., *Commento all'art. 11, l. n. 675/ 1996*, in *La tutela dei dati personali. Commentario alla l. 675/1996*, a cura di GIANNANTONIO E.-LOSANO M.G.-ZENO-ZENCOVICH V., Cedam, 1997, p. 102;

COMANDÈ G., *Sub art. 18,* in *Nuove leggi civ. comm.*, 1999, I, p. 500;

COMMISSIONE UE, *White Paper on Artificial Intelligence: a European approach to excellence and trust* COM(2020) 65 final, 19.2.2020;

COMOGLIO L. P., *L'azione di classe italiana: valutazioni ed efficienza*, in *Dir. pubbl. comp. eur.*, 2012, p. 1114;

CONSOLO C.-ZUFFI B.*, L'azione di classe ex art. 140-bis cod. cons. Lineamenti processuali*, Cedam, 2012;

CONTE G., *Il difficile equilibrio tra l'essere e l'avere: considerazioni critiche sulla nuova configurazione del danno non* patrimoniale, in *Giur. It.,* 2009;

CORBIN A., *Il segreto dell'individuo*, in *La vita privata. L'Ottocento*, collana diretta da ARIÈS P.-DUBY G., Laterza, 1988, p. 333;

CUFFARO V., *Il diritto europeo sul trattamento dei dati personali*, in *Contr. e imp.*, p. 201;

CUFFARO V.-D'ORAZIO R.-RICCIUTO V., *Il codice del Trattamento dei dati personali*, Giappichelli, 2007;

CUFFARO V.-RICCIUTO V., *Il trattamento dei dati personali*, Giappichelli, 1999;

D'ARMONIO MONFORTE A., *La successione nel patrimonio digitale*, Pacini, 2020;

D'OTTAVIO A., *Ruoli e funzioni* privacy *principali ai sensi del regolamento*, in *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, a cura di PANETTA R., Giuffrè, 2019, p. 143;

DAVOLA A.-PARDOLESI R., *In viaggio col robot: verso nuovi orizzonti della r. c. auto ("driverless")?*, in *Danno e resp*., 2017, p. 616;

DE CUPIS A., *Ancora in tema di offesa morale per mezzo della divulgazione cinematografica*, in *Foro it.*, 1952, I, p. 149;

DE CUPIS A., *I diritti della personalità*, in *Trattato di diritto civile e commerciale*, IV, t. 1, diretto da CICU A.-MESSINEO F., Giuffrè, 1959;

DE CUPIS A., *Riconoscimento sostanziale, ma non verbale, del diritto alla riservatezza*, in *Foro it.*, 1963, I, 877, p. 1298 (nota a CASS., 20.4.1963, n. 990);

DE GREGORIO G.-TORINO R., *Privacy, tutela dei dati personali e Big Data*, in AA.VV., *Privacy Digitale*, a cura di TOSI E., Giuffrè, 2019, p. 447;

DE MAURO A.- GRECO M.-GRIMALDI M., *A Formal definition of Big Data based on its essential features*, in *Library Review*, 2016, n. 65, p. 122;

DELEUZE G.-GUATTARI F., *Mille plateaux*, 1980, (ed. italiana *Mille piani, Capitalismo e schizofrenia*, a cura di VIGNOLA P., Orthotes, 2017);

DELL'UTRI M., *Principi generali e condizioni di liceità del trattamento dei dati personali*, in *I dati personali nel diritto europeo*, a cura di V. CUFFARO-R. D'ORAZIO-V. RICCIUTO, Giappichelli, 2019;

DERSHOWITZ A., *The Mueller Report. The final report of the special counsel into Donald Trump, Russia and collusion*, Skyhorse Publishing, 2019;

DI CIOMMO F., *Civiltà tecnologica, mercato e insicurezza: la responsabilità del diritto*, in *Riv. crit. dir. priv*., 2010, p. 590;

DI CIOMMO F., *Il danno non patrimoniale da trattamento dei dati personali*, in *Il "nuovo" danno non patrimoniale*, a cura di G. PONZANELLI, Cedam, 2004, p. 274;

DI CIOMMO F., *La risarcibilità del danno non patrimoniale da illecito trattamento dei dati personali*, in *Danno e Resp.,* 2005, p. 803;

DI CIOMMO F., *Quello che il diritto non dice. Internet e oblio*, in *Danno e resp*., 2014, p. 1101;

DICKENS C., *The life and adventurers of Martin Chuzzlewit*, 1844;

DODGE M.-KITCHIN R., *Code/space: software and everyday life*, MIT Press, 2011;

DONZELLI R., *Art. 140 bis c. cons.*, in *Commentario breve al diritto dei consumatori*, a cura di G. DE

CRISTOFARO G.-ZACCARIA A., Cedam 2013:

FARACE D., *Le persone autorizzate al trattamento dei dati personali*, in *Riv. trim. dir. e proc. civ.*, 2021, p. 423;

FAULKNER W., *Privacy. Il sogno americano: che ne è stato?,* traduzione italiana a cura di MATERASSI M., Adelphi, 2003;

FEDERAL TRADE COMMISSION, *Opinion about Cambridge Analytica*, 9383, 25.11.2019.

FERRI G. B., *Privacy e libertà informatica,* in *Le banche dati in Italia. Realtà normativa e progetti di regolamentazione*, a cura di ZENO-ZENCOVICH V., Jovene, 1985, p. 59.

FINOCCHIARO G., *Il contratto nell'era dell'intelligenza artificiale*, in *Riv. trim. dir. proc. civ*., 2018, p. 441;

FINOCCHIARO G., *Il principio di* accountability*,* in *Giur. it.*, 2019, p. 2777;

FINOCCHIARO G., *Il quadro d'insieme sul Regolamento europeo*, in *La protezione dei dati personali in Italia,* diretto da G. FINOCCHIARO, Zanichelli, 2019, p. 8;

FINOCCHIARO G., *Intelligenza artificiale e protezione dei dati personali*, in *Giur. it.*, 2019, 7, p 1657;

FINOCCHIARO G., *Introduzione al regolamento europeo sulla protezione dei dati*, in *Nuove leggi civ. comm*., 2017, p. 10;

FINOCCHIARO G., *Privacy e protezione dei dati personali. Disciplina e strumenti operativi*, Zanichelli, 2012;

FINOCCHIARO G., voce «*Identità personale* (diritto alla)», in *Digesto, Disc. priv. sez. civ.*, 2010, p. 721;

FOFFA R., *Il caso Vieri: quanto vale la lesione della privacy*, in *Danno e resp*., 2013, p. 55;

FOFFA R., *Illecito trattamento dei dati personali in condominio,* in *Danno e resp*., 2011, p. 131 (nota a TRIB. POTENZA, 27.1.2010);

FOUCAULT M., *Sorvegliare e punire – nascita della prigione*, Einaudi, 1976;

FRANZONI M., *Danno evento, ultimo atto?*, in *Nuova giur civ. comm*., 2018, I (nota a CASS., ord. 27.3.2018, n. 7513);

FRANZONI M., *Dati personali e responsabilità civile*, in *Resp. civ. e prev*., 1998, p. 903;

FRANZONI M., *L'illecito*, in *Trattato della Responsabilità civile*, Giuffrè, 2010;

FRANZONI M., *Responsabilità derivante da trattamento dei dati personali,* in *Dir. inf.*, a cura di FINOCCHIARO G.-DELFINI F., Utet, 2014, p. 831;

FRANZONI M., *Responsabilità per l'esercizio di attività pericolose*, in *La responsabilità civile,* II, 2, a cura di ALPA G.-BESSONE M., Giappichelli, 1987, p. 462;

FROSINI V., *Tecnologie e libertà costituzionali*, in *Dir. inf. e inform.*, 2003;

FROSINI V., *Teoria e tecnica dei diritti umani: i diritti umani nella società tecnologica*, Editori Riuniti,

1993;

FUSARO AR., *Attività pericolose e dintorni. Nuove applicazioni dell'art. 2050 c.c.*, in *Riv. dir. civ.*, 2013, p. 1137;

FUSARO AR., *Quale modello di responsabilità per la robotica avanzata? Riflessioni a margine del percorso europeo*, in *Nuova giur. civ. comm.*, 2020, p. 1344;

GABRIELLI E.-RUFFOLO U., *Intelligenza Artificiale e diritto*, in *Giur. it.*, 2019, p. 1657;

GAETA M. C., *La protezione dei dati personali nell'Internet of Things: l'esempio dei veicoli autonomi*, in *Dir. inf.*, 2018, p. 147;

GAGLIARDI M., *La prova del danno non patrimoniale in caso di trattamento illecito di dati personali*, in *Danno e resp.*, 2016, p. 378;

GALIC M.-TIMAN T.-KOOPS B. J., *Bentham, Deleuze and Beyond: an overview of Surveillance theories from the Panopticon to Participation*, in *Philosophy & Technology*, Berlin, 2016, Vol. 30 no. 1;

GAMBINI M., *Principio di responsabilità e tutela aquiliana dei dati personali*, Esi, 2018;

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Violazioni di dati personali (data breach) in base alle previsioni del Regolamento (UE) 2016/679*, all'indirizzo https://www.garanteprivacy.it/regolamentoue/databreach;

GELLERT R., *Data protection: a risk regulation? Between the risk management of everything and the precautionary alternative*, in *International Data Privacy Law*, 2015, vol 5, n. 1, p. 3;

GELLERT R., *Understanding data protection as risk regulation* in *Journal of Internet Law*, 2015, p. 3;

GELLERT R., *Data protection: a risk regulation? Between the risk management of everything and the precautionary alternative*, in *International Data Privacy Law*, 2015, Vol. 5, No. 1, p. 3;

GERCKE M., *"Hacking an Election". An overview of attacks in the context of democratic elections and the role of criminal law in defending against such attacks* in *Computer Law Review International*, 2017, p. 129;

GIACOBBE G., voce «*Riservatezza* (diritto alla)», in *Enc. dir.*, Giuffrè, 1989, p. 1243;

GIAMPICCOLO G., *La tutela giuridica della persona umana e il c.d. diritto alla riservatezza*, in *Riv. trim. dir. proc. civ.,* 1958, p. 459;

GIANNANTONIO E., voce «*Dati personali* (tutela dei)», in *Enc Dir.*, Giuffrè, 1999;

GIANNANTONIO E.-LOSANO M. G.-ZENO-ZENCOVICH V., *La tutela dei dati personali. Commentario alla l. 675/1996*, Cedam, 1997;

GIUSSANI A., *L'azione di classe: aspetti processuali*, in *Riv. trim. dir. proc. civ.*, 2013, p. 341;

GRAEF I.-CLIFFORD D.-VALCKE P., *Fairness and enforcement: bridging competition, data protection*

and consumer law in *International Data Privacy Law,* Vol. 8, No. 3, 2018, p. 220;

GRECO L., *L'organigramma privacy: i soggetti del trattamento*, in *La protezione dei dati personali in Italia*, a cura di G. FINOCCHIARO, Zanichelli, 2019, p. 321;

GRITTI F., *La responsabilità civile nel trattamenti dei dati personali*, in *Il codice del trattamento dei dati personali*, a cura di CUFFARO V.-D'ORAZIO R.-RICCIUTO V., Giappichelli, 2007, p. 129;

HAGGERTY K. D.-ERICSON R.V., *The surveillant assemblage*, in *British Journal of Sociology*, Vol. No. 51 Issue No. 4, 2000, p. 605;

HERMSTRUWER Y., *Contracting Around Privacy: The (Behavioral) Law and Economics of Consent and Big Data*, in *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 2017, p. 9, all'indirizzo https://www.jipitec.eu/issues/jipitec-8-1-2017/4529;

HILDEBRANDT M.-TIELEMANS L., *Data Protection by Design and Technology Neutral Law*, in *Computer Law & Security Review*, 2013, 29, p. 509;

HOOD C.-ROTHSTEIN H.-BALDWIN R., *The Government of Risk - Understanding Risk Regulation Regimes*, Oxford University Press, Oxford, 2001;

JASMONTAITE L. & OTHERS, *Data Protection by Design and by Default: Framing Guiding Principles into Legal Obligations in the GDPR*, in *European Data Protection Law Review*, 2018, 4, p. 16,

JUDICIAL COLLEGE*, Guidelines for the Assessment of General Damages in Personal Injury Cases*, Oxford, 2019;

KAISER B., *Targeted: My Inside Story of Cambridge Analytica and How Trump and Facebook Broke Democracy*, HarperCollins, 2019;

KAMARINOU D., *Brendan Van Alsenoy, Data Protection Law in the EU: Roles, Responsibilities and Liability* in *International Data Privacy Law,* Vol. 10, No. 4*,* 2020, p. 395;

KNETSCH J., *The compensation of non-pecuniary loss in GDPR infringement cases* in *Eur. J. Privacy L. & Tech.*, 2020, p. 63;

KUNER C.-CATE F. H.-MILLARD C.-SVANTESSON D. J. B.-LYNSKEY O., *Risk management in data protection* in *Data Privacy Law,* Vol. 5, No. 2, 2015, p. 95,

LATHAM & WATKINS, *GDPR Violations in Germany: Civil Damages Actions on the Rise*, 21.12.2020, all'indirizzo https://www.jdsupra.com/legalnews/gdpr-violations-in-germany-civil-84570/;

LAROUCHE P., PEITZ M., PURTOVA N.*, Consumer privacy in network industries. A CERRE Policy Report*, CERRE, 2016;

LEISER M. R.-DECHESNE F., *Governing machine-learning models: challenging the personal data presumption* in *International Data Privacy Law,* Vol. 10 No. 4, 2020, p. 187;

LINCKE K -NOURBAKHSH A.*, An Analysis of the GDPR's Effects on the Future of Cloud Outsourcing. Winds of regulatory change threaten the ubiquity of the cloud,* in *Computer Law Review*

International, 2017, p. 179;

LINTVEDT M. N., *Putting a price on data protection infringement* in *International Data Privacy Law,* Vol. 00, No. 0, 2021, p. 1;

LIONELLO L., *La creazione del mercato europeo dei dati: sfide e prospettive*, in *Dir. comm. int.*, 2021, p. 65;

LIOR A., *AI strict liability vis-à-vis ai monopolization,* in *The Columbia Science & Technology Law Review,* 2020, p. 90;

LLOYD I., *UK: Classification of Software as Goods? UK: Administrators of Cambridge Analytica No Data Controllers* in *Computer Law Review International*, 2019, p. 84;

LUCCHINI GUASTALLA E., *Il nuovo regolamento europeo sul trattamento dei dati personali: i principi ispiratori*, in *Contr. e impr*., 2018, p. 106;

LUCCHINI GUASTALLA E.*, Trattamento dei dati personali e danno alla riservatezza*, in *Resp. civ. e prev*., 2003;

LUGARESI N., *Internet, Privacy e pubblici poteri negli Stati Uniti*, Giuffrè, 2000;

LYON D., *La cultura della sorveglianza*. *Come la società del controllo ci ha reso tutti controllori*, Luiss University Press, 2020;

LYON D., *The culture of Surveillance. Watching as a way of life,* Polity Press, 2018 *(*traduzione italiana a cura di BALBI G.-DI SALVO P., *La cultura della sorveglianza*, Luiss, 2020);

MACARIO F., *La protezione dei dati personali nel diritto privato europeo*, in *Il trattamento dei dati personali*, a cura di V. CUFFARO-V. RICCIUTO, Giappichelli, 1999, p. 48;

MANES P., *Il consenso al trattamento dei dati personali*, Cedam, 2001;

MANIACI A.-D'ARMINIO MONFORTE A., *La prima decisione italiana in tema di "eredità digitale": quale tutela post mortem dei dati personali?,* in *Corr. giur.*, 2021, p. 658 (nota a TRIB. MILANO, 10.2.2021);

MANTELERO A., *Il costo della privacy tra valore della persona e ragione d'impresa*, Giuffrè, 2007.

MANTELERO A., *La gestione del rischio*, in *La protezione dei dati personali in Italia,* diretto da G. FINOCCHIARO, Zanichelli, 2019;

MANTELERO A., *Responsabilità e rischio nel Regolamento UE 2016/679*, in *Nuove leggi civ. comm.*, 2017, p. 144;

MANTELERO A., *Gli autori del trattamento dati: titolare e responsabile*, in *Giur. it*., 2019;

MANTELERO A.-VACIAGO G., *The "Dark Side" of big data: private and public interaction in social surveillance. How data collections by private entities affect governmental social control and how the EU reform on data protection responds* in *Computer law review international*, 2013, p. 161;

MARINO G., *La successione digitale*, in *Oss. dir. civ. e comm*., 2018, p. 180;

MARTIN-FUGIER A., *I riti della vita privata nella borghesia*, in *La vita privata. L'Ottocento*, collana diretta da ARIÈS P.- DUBY G., Laterza, 1988, p. 161;

MASTROPIETRO B., *Il danno da illecito trattamento dei dati personali nel quadro dei recenti orientamenti in materia di danno non patrimoniale*, in *Nuova giur civ. comm*., 2004, I, p. 667;

MASTROPIETRO B., *Il danno da illecito trattamento di dati personali*, in *Nuova giur. civ. comm.,* 2004, p. 679;

MATTERA V., *La successione nell'account digitale*. *Il caso tedesco*, in *Nuova giur. civ. comm.,* 4, 2019, p. 700;

MAYER-SCHONBERGER V.-CUKIER K. N., *Big data. Una rivoluzione che trasformerà il nostro modo di vivere e già minaccia la nostra libertà*, Garzanti, 2013;

MAYER-SCHÖNBERGER V.-PADOVA Y., *Regime change? Enabling big data through Europe's new data protection regulation* in *The Columbia Science & technology law review*, 2016, Vol. XVII, p. 315;

MENGONI L., *Obbligazioni "di risultato" e obbligazioni "di mezzo",* in *Riv. dir. comm*., 1954, p. 185;

MESSINETTI D., *Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali*, in *Riv. crit. dir. priv.*, 1998, p. 350;

MESSINETTI D., *I nuovi danni. Modernità, complessità della prassi e pluralismo della nozione giuridica di danno*, in *Riv. crit. dir. priv*., 2006, p. 552;

MESSINETTI D., *Pluralismo dei modelli risarcitori. Il criterio di ingiustizia "tradito*", in *Riv. crit. dir. priv*., 2007, p. 561;

MESSINETTI R., *La tutela della persona umana* versus *l'intelligenza artificiale. Potere decisionale dell'apparato tecnologico e diritto alla spiegazione della decisione automatizzata*, in *Contr. e impr.*, 2019, p. 891;

MITRAKAS A., *Assessing liability arising from information security breaches in data privacy,* in *International Data Privacy Law*, Vol. 1, No. 2, 2021, p. 29;

MOEREL L., *Big Data Protection. How to Make the Draft EU Regulation on Data Protection Future Proof*, Tilburg University, 2014, p. 3;

MONATERI P. G., *Il pregiudizio esistenziale come voce del danno non patrimoniale,* in *Riv. dir. civ*., 2009, II, p. 97 (nota a CASS., sez. un., 11.11.2008, n. 26972, n. 26973, n. 26974 e n. 26975);

MONTINARO R., *Tutela della riservatezza e risarcimento del danno nel nuovo "codice in materia di protezione dei dati personali"*, in *Giust. civ*., 2004, p. 259;

NAVARRETTA E., *Commento all'art. 9*, in *Commentario alla L. 31 dicembre 1996, n. 675, Tutela della "privacy"*, a cura di C. M. BIANCA-F. D. BUSNELLI, Cedam, 2007;

NAVARRETTA E., *Il calore della persona nei diritti inviolabili e la complessità dei danni non* patrimoniali, in *Riv. dir. civ*., 2009, II, p. 97 (nota a CASS. sez. un., 11.11.2008, n. 26972, n. 26973, n. 26974 e n. 26975);

NAVARRETTA E., Il *contenuto del danno non patrimoniale e il problema della liquidazione*, in *Il danno non patrimoniale. Principi, regole e tabelle per la liquidazione*, a cura di NAVARRETTA E., Giuffrè, 2010, p. 91;

NIGER S., *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, Cedam, 2006;

NIMMER M. B., *The right of Publicity*, in *Law and Contemp. Probs*, 1954, p. 204;

NITTI M., *La valutazione della "gravità della lesione" e della "serietà del danno" nel risarcimento del danno non patrimoniale da violazione della privacy*, in *Danno e resp*., 2015, p. 339 (nota a CASS., 15.7.2014, n. 16133);

NUNZIANTE E., *Big Data. Come proteggerli e come proteggerci. Profili di tutela tra proprietà intellettuale e protezione dei dati personali*, in *Law and Media Working Paper Series*, 2017, p. 6;

O' ROURKE M., *Fencing Cyberspace: drawing borders in a virtual world*, in *Minnesota Law Review*, 82, 1998, p. 620;

O'DELL E., *Compensation for breach of the general data protection regulation,* Dublin ULJ, 2017, p. 97;

O'NEIL C., *Armi di distruzione matematica. Come i big data aumentano la disuguaglianza e minacciano la democrazia*, Bompiani, 2017;

PALLARO P., *Libertà della persona e trattamento dei dati personali nell'Unione Europea*, Giuffrè, 2002;

PANETTA R., *Libera circolazione e protezione dei dati personali*, Giuffrè, 2006;

PARDOLESI R., *Diritto alla riservatezza e circolazione dei dati personali*, Giuffrè, 2003;

PARISI A. G., *Privacy e mercato digitale*, Pacini, 2020;

PASSAGLIA P.-POLETTI D., *Nodi virtuali, legami informali. Internet alla ricerca di regole,* Pisa University Press, 2017*;*

PATTI S., *Il consenso dell'interessato al trattamento dei dati personali*, in *Riv. dir. civ*., 1999, p. 455;

PELLECCHIA E., *La responsabilità civile per trattamento dei dati personali*, in *Resp. civ. e prev*., 2005, p. 232;

PERLINGIERI G., *L'art. 2059 c.c.: uno e bino: una interpretazione che non convince*, in *Rass. dir. civ*., 2003, p. 770 (nota a CORTE COST., 11.6.2003, n. 223);

PERLINGIERI P., *La responsabilità civile tra indennizzo e risarcimento*, in *Rass. dir. civ*., 2004, p.

1066;

PERLINGIERI P., *Privacy digitale e protezione dei dati personali tra persona e mercato*, in *Foro Nap.,* 2018, p. 481;

PERON S., *Ancora sul risarcimento del danno non patrimoniale da violazione della privacy*, in *Resp. civ. prev*., 2016, p. 957;

PERON S., *Sul risarcimento del danno non patrimoniale da violazione della privacy*, in *Resp. civ. prev*., 2013, p. 225;

PERRI P., *Introduzione,* in *Sorveglianza elettronica, diritti fondamentali ed evoluzione tecnologica*, Giuffrè, 2020, p. XI;

PERRI P., *Privacy, diritto e sicurezza informatica*, Giuffrè, 2007;

PERRI P., *Sorveglianza elettronica, diritti fondamentali ed evoluzione tecnologica*, Giuffrè, 2020;

PERROT M., *Introduzione*, in *La vita privata. L'Ottocento*, collana diretta da ARIÈS P.- DUBY G., Laterza, 1988, p. 5;

PHILLIPS G., *The Abuse and Misuse of Technology. A UK Newspaper Lawyer's Perspective*, in *Computer Law Review International*, 2016, p. 43;

PINORI A., *Internet e responsabilità civile per il trattamento dei dati personali*, in *Contr. e impr.*, 2007, p. 1568;

PIRAINO F., *Il regolamento generale sulla protezione dei dati ed i diritti dell'interessato*, in *Nuove leggi civ. comm.*, 2017, p. 369;

PIRAINO F., *Ingiustizia del danno e antigiuridicità,* in *Europa e dir. priv*., 2005, p. 746;

PIZZETTI F., *Privacy e Diritto europeo della protezione dei dati personali. Dalla Direttiva 95/46 al Nuovo Regolamento Europeo, I Diritti nella "rete" della rete,* Giappichelli, 2016;

PIZZETTI F., *Privacy e il diritto europeo alla protezione dei dati personali*, I, Giappichelli, 2016;

PIZZETTI G., *Intelligenza artificiale, protezione dei dati personali e regolazione*, Giappichelli, 2018;

POHLE J., *Data Privacy Legislation In The European Union Member States–A Pratical Overview. How EU Member States have adjusted their domestic data privacy law to the GDPR,* in *Computer Law Review International*, 2018, p. 97;

POLETTI D., *La dualità del sistema risarcitorio e l'unicità della categoria dei danni non patrimoniali*, in *Riv. dir. civ*., 2009, II, p. 97 (nota a CASS., sez. un., 11 novembre 2008, n. 26972, n. 26973, n. 26974 e n. 26975);

POLETTI D., *Le condizioni di liceità del trattamento dei dati personali*, in *Giur. it.*, 2019, p. 2777;

PONZANELLI G. (a cura di), *Il "nuovo" danno non patrimoniale*, Cedam, 2004;

PONZANELLI G., *Danno non patrimoniale: l'abbandono delle Sezioni Unite di San Martino,* in *Danno e resp.*, 2018, p. 456 (nota a CASS., ord. 27.3.2018, n. 7513);

PONZANELLI G., *Il decalogo sul risarcimento del danno non patrimoniale e la pace all'interno della Terza Sezione*, in *Nuova giur civ. comm*., 2018, I (nota a CASS., ord. 27.3.2018, n. 7513);

PONZANELLI G., *Il risarcimento integrale senza danno esistenziale*, Cedam, 2007;

PONZANELLI G., *Limiti del danno esistenziale*, in *Il danno esistenziale. Una nuova categoria della responsabilità civile*, a cura di CENDON P.-ZIVIZ P., Giuffrè, 2000, p. 803;

PONZANELLI G., *Ricomposizione dell'universo non patrimoniale: le scelte della Corte di Cassazione*, in *Danno resp*., 2003, p. 816;

PROSSER W. L., *Privacy*, in *California Law Review*, Vol 48, No. 3, 1960, p. 384;

PUGLIESE G., *Il preteso diritto alla riservatezza e le indiscrezioni cinematografiche*, in *Foro it.*, 1954, p. 116;

QUARTA F., *Risarcimento e sanzione nell'illecito civile*, Esi, 2013;

RADIN M. J., *Compensation and commensurability*, Duke LJ, p. 56;

RAMACCIONI G., *La protezione dei dati personali: il tema/problema del risarcimento del danno non patrimoniale*, in *Danno e resp.*, 2018, p. 665;

RAMIREZ E-BRILL J.-OHLHAUSEN M. K.-WRIGHT J. D.-MCSWEENY T., *Data Brokers. A Call for Transparency and Accountability*, Federal Trade Commission 2014;

RATTI M., *La responsabilità da illecito trattamento dei dati personali nel nuovo Regolamento,* in *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, a cura di FINOCCHIARO G., Zanichelli, 2019, p. 615;

RAVÀ A., *Istituzioni di diritto privato*, Cedam, 1938;

RENNA M., *Sicurezza e gestione del rischio nel trattamento dei dati personali*, in *Resp. civ. e prev.*, 2020, p. 1343;

RESTA G.*, I dati personali oggetto del contratto. Riflessioni sul coordinamento tra la Direttiva (Ue) 2019/770 e il Regolamento*, in *Annuario del diritto dei contratti*, Giappichelli, 2018;

RESTA G., *La successione nei rapporti digitali e la tutela post mortale dei dati personali*, in *Contr. e impr*., 2019, p. 99;

RESTA G.-SALERNO A., *La responsabilità civile per il trattamento dei dati personali*, in *La responsabilità d'impresa*, a cura di P. G. ALPA-G. CONTE, Giuffrè, 2015, p. 684;

RICCI A., *Trattamento di dati sensibili e principio di responsabilizzazione*, in *Giur. it.*, 2018, p. 2639;

RICCI F. M.*, I diritti dell'interessato*, in AA.VV. *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Zanichelli, 2017, p. 185;

RICCIO G. M., *Titolarità e contitolarità nel trattamento dei dati personali tra Corte di Giustizia e Regolamento privacy*, in *Nuova giur. civ. comm.*, 2018, p. 1085 (nota a CORTE GIUST. UE, 5.6.2018, causa C-210/16);

RICCIO G. M., *Diritto all'oblio e responsabilità dei motori di ricerca*, in *Dir. inform.*, 2014, p. 753;

RICCIO G. M.-SCORZA G.-BELISARIO E., *GDPR e Normativa Privacy*. *Commentato*, Ipsoa, 2018;

RICCIUTO V., *Il contratto ed i nuovi fenomeni patrimoniali: il caso della circolazione dei dati personali*, in *Riv. dir. civ.*, 2020, p. 642;

RICCIUTO V., *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione fenomeno*, in *I dati personali nel diritto europeo*, a cura di CUFFARO V.-D'ORAZIO R.-RICCIUTO V., Giappichelli, 2019, p. 23;

RICCIUTO V., *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, in *Dir. inf. e inform.*, 2018, p. 689;

RODOTÀ S., *Elaboratori elettronici e controllo sociale*, Il Mulino, 1973;

RODOTÀ S., *La privacy tra individuo e collettività*, in *Pol. e dir.*, 1974, p. 545;

RODOTÀ S., *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali,* in *Riv. crit. dir. priv.*, 1997, p. 588;

RODOTÀ S., *Prefazione*, in BOCCHIOLA M., *Privacy. Filosofia e politica di un concetto inesistente*, Luiss, 2014, p. 10;

RODOTÀ S., *Relazione 2002*, 20.5.2003;

RODOTÀ S., *Tecnologie e diritti*, Il Mulino, 1995;

RODOTÀ S., *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione,* Laterza, 2005;

RODOTÀ S., *Tra diritti fondamentali ed elasticità della normativa: il nuovo codice della privacy*, in *Eur. e dir. priv.*, 2004, p. 1;

ROTENBERG SCHWARTZ S., *Information privacy law*, Aspen Publishers, 2005;

RUBINSTEIN I. S.-GOOD N., *The trouble with Article 25 (and how to fix it): the future of data protection by design and default,* in *International Data Privacy Law*, Vol. 10, No. 1, 2020, p. 37;

RUFFOLO U.-AMIDEI A., *Intelligenza artificiale e diritti della persona: le frontiere del "transumanesimo"*, in *Giur. it.*, 2019, p. 1657;

SALAMI E., *Autonomous transport vehicles versus the principles of data protection law: is compatibility really an impossibility?,* in *International Data Privacy Law,* Vol. 10, No. 4, 2020, p. 330;

SALVI C., *Il risarcimento integrale del danno non patrimoniale, una missione impossibile*. *Osservazione sui criteri per la liquidazione del danno non patrimoniale*, in *Eur. e dir. priv.*, 2014, p. 517;

SALVI C., *La responsabilità civile*, Giuffrè, 1998;

SARTOR G., *Intelligenza artificiale e diritto. Un'introduzione*, Giuffrè, 1996;

SARTOR G., *Le applicazioni giuridiche dell'intelligenza artificiale: la rappresentazione della*

conoscenza, Giuffrè, 1990;

SCALISI A., *Il diritto alla riservatezza*, Giuffrè, 2002;

SCALISI V., *Danno alla persona e ingiustizia*, in *Riv. dir. civ*., 2007, p. 152;

SCALISI V*., Illecito civile e responsabilità: fondamento e senso di una distinzione*, in *Riv. dir. civ*., 2009, p. 657;

SCARCHILLO G., *Responsabilità e tutela dei diritti. Percorsi di diritto privato comparato*, Jovene, 2018;

SCOGNAMIGLIO C., *Danno morale soggettivo*, in *Nuova giur. civ. comm.,* 2010, p. 327;

SCOGNAMIGLIO C., *Il sistema del danno non patrimoniale dopo le decisioni delle Sezioni Unite*, in *Resp. civ. prev*. 2009, p. 261;

SCOGNAMIGLIO R., *Il danno morale. Contributo alla teoria del danno extracontrattuale*, in *Riv. dir. civ.,* 1957, I, p. 277;

SCOGNAMIGLIO C., *La Cassazione delinea presupposti e limiti di risarcibilità del danno non patrimoniale contrattuale nell'azione di classe*, in *Nuova giur. civ. comm.*, 2019, p. 993;

SERAFINELLI L., *Ancora sulla tutela del consumatore, anche in chiave collettiva*, in *Nuova giur. civ. comm.*, 2019, p. 612;

SICA S.- D'ANTONIO V.-RICCIO G. M., *La nuova disciplina europea della privacy*, Cedam, 2016;

SICA S., *Commento sub artt. 11-22,* in *La nuova disciplina della privacy (d.lgs. 30 giugno 2003, n. 196)*, a cura di SICA S.-STANZIONE M. G, Le riforme del diritto italiano, 2005, p. 8;

SICA S., *Danno e nocumento nell'illecito trattamento di dati personali*, in *Dir. inf. e inform.*, 2004, p. 721;

SICA S., *Il consenso al trattamento dei dati personali: metodi e modelli di qualificazione giuridica*, in *Riv. dir. civ.*, 2001, p. 621;

SICA S., *La libertà fragile. Pubblico e privato al tempo della rete*, Esi, 2014;

SOLOVE D. J., *Introduction: privacy self-management and the consent dilemma* in *Harward Law Review*, 2013, Vol. 126, 1934, p. 1880;

SORO A., *Democrazia e potere dei dati*, BaldiniCastoldi, 2019;

SPANGARO A., *L'ambito di applicazione materiale della disciplina del Regolamento*, in *La protezione dei dati personali in Italia,* diretto da G. FINOCCHIARO, Zanichelli, 2019, p. 28;

STANZIONE M. G., *Il regolamento europeo sulla privacy: origine e ambito di applicazione*, in *Eur. e dir. priv.*, 2016, p. 1249;

STANZIONE P., *Tecnica, protezione dei dati e nuove vulnerabilità,* 2.7.2021, all'indirizzo https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9676499;

STRUGAŁA R., *Art. 82 GDPR: strict liability or liability based on fault?,* in *European Journal of*

Privacy Law & Technologies Special issue, 2020, p. 71;

TAMPIERI M., *Il patrimonio digitale oltre la vita: - quale destino?*, in *Contr. e impr.*, 2021, p. 543;

THIENE A., *Segretezza e riappropriazione di informazioni di carattere personale: riserbo e oblio nel nuovo Regolamento europeo*, in *Nuove leggi civ*., 2017, p. 443;

THOBANI S., *Il danno non patrimoniale da trattamento illecito dei dati personali*, in *Dir. inform*., 2017, p. 427;

THOBANI S., *Invio di comunicazioni indesiderate: il risarcimento del danno non patrimoniale*, in *Giur. it.*, 2017, p. 1537;

THOMPSON M., *'Beyond Gatekeeping: The Normative Responsibility of Internet Intermediaries*, in *Vand J. Ent. & Tech L*., 2016, Vol. 18:4, p. 783, p. 783;

TINCANI P., *Sorveglianza e potere. Disavventure dell'asimmetria cognitiva*, in *Ragion pratica*, 2018, I, p. 63;

TOMARCHIO V., *L'unitarietà del danno non patrimoniale nella prospettiva delle Sezioni unite*; in *Resp. civ. e prev*., 2009, p. 38 (nota a CASS., sez. un., 11.9.2008, n. 26972, n. 26973, n. 26974 e n. 26975);

TORMEN L., *La linea dura della Cassazione in materia di responsabilità dell'*Hosting Provider *(attivo e passivo)*, in *Nuova giur. civ. comm.*, 2019, p. 1039 (nota a CASS. 19.3.2019, n. 7708);

TOSI E., *Illecito trattamento dei dati personali, responsabilizzazione, responsabilità oggettiva e danno nel GDPR: funzione deterrente-sanzionatoria e rinascita del danno morale soggettivo*, in *Contr. e impr.*, 2020, p. 1115;

TOSI E., *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale*, Giuffrè, 2020;

TOSI E., *Trattamento illecito dei dati personali, responsabilità oggettiva e danno non patrimoniale alla luce dell'art. 82 del GDPR UE,* in *Danno e resp.*, 2020, p. 434;

TRILATERAL RESEARCH & CONSULTING, *Privacy impact assessment and risk management – Repost for the Information Commissioner's Office*, 4.5.2013;

TRIMARCHI P., *La responsabilità civile: atti illeciti, rischio, danno*, Giuffrè, 2017;

TRIMARCHI P., *Rischio e responsabilità oggettiva*, Giuffrè, 1961;

UNGER W., *How the Poor Data Privacy Regime Contributes to Misinformation Spread and Democratic Erosion* in *The Columbia Science & Technology Law Review,* 2021, p. 308*;*

VAN ALSENOY B., *Liability under EU Data Protection Law. From Directive 95/46 to the General Data Protection Regulation*, JIPITEC, 2016, p. 271;

VAN ALSENOY B., *Data Protection Law in the UE: Roles, Responsibilities and Liability*, Cambridge, 2019, p. 47;

VAN DAM C., *European Tort Law*, OUP, Oxford 2013;

VERSACI G., *La contrattualizzazione dei dati personali dei consumatori*, Esi, 2020;

WARREN S.-BRANDEIS L., *The right to Privacy*, in *Harvard Law Review,* Vol. 4, No. 5, 1890, p. 193;

WATERMAN K.-BRUENING P. J., *Big Data analytics: risks and responsibilities* in *International Data Privacy,* Vol. 4, No. 2, 2014, p. 89;

WESTIN A., *Privacy and Freedom*, Atheneum New York, 1967;

WESTIN A., *Entering the Era of Databank Regulation and How We Got There*, in *Policy Issues in Data Protection and Privacy*, *Principles and Perspectives*, OECD, Paris, 1976;

WOLTERS P. T. J., *The security of personal data under the GDPR: a harmonized duty or a shared responsibility?* in *International Data Privacy Law,* Vol. 7, No. 3, p. 165;

WONG B., *Problems with controller-based responsibility in EU data protection law* in *International Data Privacy Law,* Vol. 11, No 4, 2021, p. 375;

WRIGHT D., *A framework for the ethical impact assessment of information technology* in *Ethics and Information Technology,* 2011, p. 199;

WRIGHT D.-WADHWAK.-LAGAZIO M.-RAAB C.-CHARIKANE E., *Integrating privacy impact assessment in risk management,* in *Data Privacy Law,* Vol. 4, No. 2*,* 2014, p. 155;

WU J.-WANG J.-NICHOLAS S.-MAITLAND E.-FAN Q., *Application of Big Data Technology for COVID-19 Prevention and Control in China: Lessons and Recommendations*, in *J. Med. Internet Res*. 2020, vol. 22, iss. 10, p. 1;

ZACCARIA A., *La successione* mortis causa *nei diritti di disporre di dati personali digitalizzati*, in *Studium Iuris*, 2020, p. 1368;

ZENO ZENCOVICH V., *La quantificazione del danno alla reputazione e ai dati personali: ricognizione degli orientamenti 2013 del Tribunale di Roma*, in *Dir. inf*., 2014, p. 405;

ZENO-ZENCOVICH V., *I diritti della personalità*, *I, Le fonti e i soggetti*, a cura di LIPARI N.-RESCIGNO P., Giuffrè, 2009;

ZICCARDI G., *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica*, Raffaello Cortina Editore, 2015;

ZICCARDI G., *Resistance, liberation technology and human rights in the digital age,* Springer, 2013, all'indirizzo https://www.springer.com/gp/book/9789400752757;

ZIVIN P., *E poi non rimase nessuno*, in *Resp. civ. e prev*., 2003, p. 675, con note di F. D. BUSNELLI, *Chiaroscuri di estate. La Corte di Cassazione e il danno alla persona*;

ZIVIZ P., *I "nuovi danni" secondo la Cassazione,* in *Resp. civ. e prev*., 2001, p. 1177 (nota a CASS., 10.5.2001, n. 6507);

ZIVIZ P., *Il danno non patrimoniale: istruzioni per l'uso,* in *Riv. dir. civ*., 2009, II, p. 38 (nota a CASS.,

sez. un., 11.11.2008, n. 26972, n. 26973, n. 26974 e n. 26975);

ZORZI GALGANO N., *Persona e mercato dei dati. Riflessioni sul GDPR*, Cedam, 2019;

ZUBOFF S., *The age of surveillance capitalism, the fight for a human future at the new frontier of poweri*, Pubblic affairs, 2019 (ed. italiana *Il capitalismo della sorveglianza*. *Il futuro dell'umanità nell'era dei nuovi poteri*, Luiss, 2019);

ZUBOFF S., *The Secrets of Surveillance Capitalism,* Frankfurter Allgemeine, Feuilleton, 2016, all'indirizzo https://www.faz.net/aktuell/feuilleton/debatten/the-digital-debate/shoshana-zuboff-secrets-of-surveillance-capitalism-14103616.html.