Università degli Studi di Padova

Dipartimento di Diritto Pubblico, Internazionale e Comunitario

Corso di Laurea in Diritto e Tecnologia

a.a. 2022/2023

Titolo tesi: I rimedi giustiziali previsti in Italia per la tutela della privacy

Relatore: Professoressa Beatrice Zuffi

Studente: Riccardo Faggian

INDICE

INTRODUZIONE

Il diritto fondamentale della privacy ha subito una notevole trasformazione nel corso della storia dovuta principalmente dal cambiamento digitale e dall'inarrestabile interconnessione tra individui privati e pubblici. Questo diritto ha le sue radici nell'ordinamento statunitense ma la sua diffusione nell'ordinamento europeo e di conseguenza italiano era prevedibile e il primo capitolo, verterà proprio su questa sua evoluzione. Si partirà analizzando le prime riflessioni elaborate dalle corti statunitensi, fondamentali in quanto hanno rappresentato la base per la disciplina del diritto alla riservatezza, giungendo fino allo studio dell'attuale quadro normativo europeo e italiano. Si potrà vedere la metamorfosi che questo diritto ha subito con l'avvento delle nuove tecnologie, trasformandosi in diritto alla protezione dei dati personali. Inizialmente, all'interno del diritto alla riservatezza si faceva rientrale anche la *data protection* ma si vedrà come in realtà questi siano differenti tra di loro. Questo cambiamento ha dimostrato la flessibilità del diritto, in quanto è riuscito a adattarsi alle nuove tecnologie modificando le norme già esistenti e introducendone di nuove.

Il secondo capitolo è rivolto invece all'analisi della figura del Garante per la protezione dei dati personali, autorità amministrativa indipendente autorizzata a verificare la correttezza dei trattamenti dei dati personali e il rispetto dei principi presenti nel Regolamento 679/2016. Verranno analizzati in modo dettagliato i poteri e le funzioni di questa figura e, in particolare, come li ha esercitati nei provvedimenti emanati contro Google Analytics, INPS e il sistema di intelligenza artificiale ChatGPT. Questi tre casi sono molto importanti perché dimostrano la forte collaborazione che c'è tra diritto e tecnologia. Verranno inoltre approfondite le modalità con cui un soggetto può rivolgersi a questa figura per tutelarsi da una violazione della propria privacy.

Il terzo capitolo si basa invece, sullo studio del ricorso al giudice civile come rimedio giustiziale in caso di violazione. Verrà messo in luce la possibilità per l'individuo di ottenere un risarcimento del danno e quali siano i presupposti per ottenerlo.

Attraverso l'analisi di questi due differenti percorsi di tutela sarà possibile vedere quanto la privacy e la *data protection* siano fondamentali all'interno della nostra società e quanto sia importante, per il cittadino, conoscere i suoi diritti e le sue tutele. Diritto e tecnologia sono ormai un binomio consolidato e questo richiede, da parte del diritto, un continuo

aggiornamento per garantire protezione dalle nuove tecnologie che non rappresentano esclusivamente un problema ma, se usate in modo responsabile, diventano un grande alleato.

CAPITOLO PRIMO

DAI PRIMI SVILUPPI STATUNITENSI AL GDPR

1.1 The right to be let alone: origine del diritto alla privacy

Il diritto alla privacy nasce alla fine del diciannovesimo secolo negli Stati Uniti d'America, grazie, a gli avvocati Samuel Warren e Louis D. Brandies, autori del famoso articolo "*The right to privacy*", pubblicato sulla rivista dell'Università di Harward nel 1980. L'opera rappresenta una delle fondamenta in quanto, "è la prima monografia giuridica a riconoscere l'esistenza di un autonomo diritto alla privacy" ([1]). All'interno dell'articolo il diritto alla privacy veniva definito come "*the right to be let alone*" ([2]) e "il merito di Warren e Brandeis è di aver sostenuto, contro il corrente indirizzo giurisprudenziale, che la tutela di tale diritto non era da esso completamente garantito." ([3]) Di fatto, prima dell'uscita di questo fondamentale contributo, il diritto ad essere lasciati soli non aveva, in effetti, una valenza distinta dai diritti alla reputazione e all'onere. I due constatarono che le nuove fotocamere sviluppate in quell'epoca, erano in grado di violare la sfera privata senza l'ausilio della persona violata in quanto capaci di "*take picture surreptitiously, the doctrines of contract and of trust are inadequate to support the required protection*" ([4]). Di fatto, prima del 1890, la fotografia "non poteva essere scattata senza un consapevole *sitting* della persona interessata" ([5]). Grazie alla *Kodak snap Camera,* la stampa fu in grado di sviluppare un nuovo tipo di giornalismo, *yellow journalism,* basato sui pettegolezzi e sulla violazione della vita privata degli individui. Il focus dell'articolo ([6]) riguardava la differenza tra il "diritto ad informare e ad essere

---

[1] MIGLIETTI, *Profili storico-comparativi del diritto alla privacy, Diritti comparatati Comparare i diritti fondamentali in Europa,* 4 dicembre 2014, p. 3. https://www.dirittocomparati.it/profili-storico-comparativi-del-diritto-alla-privacy/.

[2] WARREN e BRANDEIS, *The right to privacy*, *Harward Law Rewiev*, 1890, p.193.

[3] PAGANO, *Tutela dei dati personali: evoluzione della legislazione europea e stato del dibattito, Torino, 1983, p. 68.*

[4] WARREN e BRANDEIS, *The right to privacy*, *Harward Law Rewiev*, 1890, p.211.

[5] PAGANO, *Tutela dei dati personali: evoluzione della legislazione europea e stato del dibattito*, Torino, 1983, p. 68-69.

[6] L'avvocato Warren, insieme alla moglie, aveva una vita molto mondana e organizzava diverse feste all'interno della sua abitazione. Warren era molto noto all'interno della società e la stampa cominciò a seguirlo e pubblicare articoli riguardante il suo stile di vita. La goccia che fece traboccare il vaso fu un articolo contenente foto della moglie durante un dei party organizzato all'interno della propria abitazione.

informati" ([7]). Diritti che non subiscono limitazione nel caso in cui il loro oggetto sia un personaggio pubblico, mentre nel caso di una persona privata, la stampa è tenuta a rispettare il diritto all'essere lasciati soli. Molto interessati sono le parole che vengono utilizzate dai due avvocati per concludere l'articolo: "il diritto comune ha sempre riconosciuto che la casa di un uomo è il suo castello, spesso inaccessibile anche a coloro che sono incaricati di eseguire i suoi stessi ordini. Vorranno forse i tribunali sbarrare l'ingresso principale alle autorità costituita per poi spalancare le porte di servizio alla curiosità oziosa e pruriginosa?" ([8]).

Warren e Brandeis fecero riferimento agli emendamenti Primo, Quarto e Quinto del *Bill of rights* per "affermare l'esistenza, all'interno dell'ordinamento giuridico americano, di un autonomo diritto alla privacy" ([9]). Le nuove tecnologie utilizzate dalla stampa in quegli anni, stavano creando un forte squilibrio tra il diritto di informare ed essere informati e il diritto alla riservatezza facendo prevalere i primi due. Lo scopo che veniva perseguito con il "*The right to privacy*" era di "offrire protezione, attraverso la tutela del diritto alla privacy, agli aspetti più intimi e spirituali dell'uomo" ([10]). L'articolo risulta essere cruciale in quanto viene introdotta una prima visione in cui "si abbandonano le logiche materiali ed utilitaristiche e si tutela non soltanto il valore preminente della proprietà privata ma, anzitutto, quello supremo della inviolabilità personale" ([11]).

È noto che all'interno della Costituzione americana un riferimento al diritto ad essere lasciati soli non sussiste e per poter sostenere la loro tesi, i due giuristi hanno dovuto svolgere una gran lavoro di interpretazione della legislazione americana. Il loro lavoro di interpretazione partì dall'analisi dell'ordinamento di *common law*, che tutelava l'individuo da pubblicazioni illecite di opere grazie al riconoscimento del diritto al copyright e il diritto di inedito. Come messo in luce dai due avvocati, questi due diritti

---

Dopo aver pubblicato l'articolo, Warren e Brandeis avviarono un'azione legale contro l'invadenza della stampa ma per il riconoscimento al diritto alla privacy bisognerà attendere diversi anni.

[7] ALONGI e POMPEI, *Diritto della privacy e protezione dei dati personali Il GDPR alla prova della data driven economy, Roma*, 2021, p. 15.

[8] FROSINI, *Privacy: diritto fondamentale oppure no, Federalismi.it, 6 agosto 2008, p. 2.* https://www.federalismi.it/nv14/articolo-documento.cfm?Artid=10767&content=&content_author=.

[9] MIGLIETTI, *Profili storico-comparativi del diritto alla privacy, Diritti comparatati Comparare i diritti fondamentali in Europa,* 4 dicembre 2014, p. 4. https://www.dirittocomparati.it/profili-storico-comparativi-del-diritto-alla-privacy/.

[10] *Op.ult.cit.*

[11] *Op.ult.cit.*

permettevano all'individuo di stabilire "in quale misura i suoi pensieri, i suoi sentimenti e le sue emozioni devono essere comunicati ad altri" ([12]). Il diritto al copyright e il diritto di inedito tutelavano la forma esterna dell'idea dell'individuo, l'espressione artistica. I due giuristi arrivarono alla conclusione che questi due diritti non erano gli strumenti adatti per tutelare un soggetto da una pubblicazione o da una descrizione di un suo fatto privato: c'era insomma un vuoto di tutela, dal momento che il danno provocato da una pubblicazione illecita di un fatto privato non dava luogo alla tutela risarcitoria, accordata solo per le violazioni dei diritti di copyright e di inedito. Anche il diritto di proprietà non era in grado di fornire una protezione adeguata, in quanto si opinava che inerisse solo beni materiali, Warren e Brandies consideravano infatti che la privacy implicasse "non solo la protezione degli scritti personali, ossia della corrispondenza, ma anche nel diritto di chi non è soggetto pubblico di impedire che la stampa riporti affari privati" ([13]). Tuttavia, i due giuristi non consideravano il diritto ad essere lasciati soli come un diritto assoluto, in quanto vi erano delle limitazioni che ne circoscrivevano la portata ([14]). Una di queste consisteva nel fatto che tale diritto non poteva condurre a vietare o a prevenire la pubblicazione di fatti e avvenimenti di interesse pubblico.

Il riconoscimento del diritto alla privacy all'interno dell'ordinamento statunitense ha richiesto naturalmente tempo, ma l'articolo di Warren e Brandies è stato fondamentale perché ha avviato un cambiamento epocale nel sistema giuridico statunitense. Un ruolo decisivo venne comunque giocato anche dai giudici che, con una serie di decisioni ([15]) e mediante un'attenta interpretazione degli Emendamenti contenuti nella Carta dei Diritti americana, riuscirono ad individuare il fondamento costituzionale della privacy. Tuttavia, sulla natura di tale diritto non mancavano dubbi e si dibatteva animatamente all'interno della società civile. La minoranza della popolazione e un ristretto numero di giudici della Corte Suprema spingeva per l'adozione di un approccio difensivo della privacy, mentre la maggioranza dei giudici della Corte Suprema erano ostili verso un atteggiamento più liberale e verso il riconoscimento di un autonomo diritto alla privacy. Le due tesi si scontrano per diversi anni creando incertezza e vuoti di tutela e "lasciando così alla mercè

---

[12] WARREN e BRANDEIS, *The right to be let alone*, *Harward Law Rewiev*, 1890., p 198.
[13] *Op. ult. cit.,* p. 213.
[14] *Op. ult. cit.,* p. 214
[15] Olmstead v. United States 277 U.S. 438 (1928), Griswold v. Connecticut 381 U.S. 479 (1965), Roe v. Wade 410 U.S. 113 (1973), Katz v. United States 389 U.S. 347 (1967).

degli oscillanti orientamenti giurisprudenziali che si alternarono nel tempo" ([16]). Solo nel 1928, con la sentenza Olmstead v. United States ([17]) incominciò il lungo percorso di riconoscimento del diritto alla privacy e l'avanzare della tesi di minoranza. Questa sentenza risulta fondamentale in quanto da essa si sviluppò, se pur in forma ridotta, la cossidetta *constitutional penumbral theory* che "riconosceva nel testo costituzionale la possibilità di aperture a maggiori tutele" ([18]). Il termine penombra richiama i concetti di vaghezza e di indeterminatezza e l'interpretazione svolta dai giuristi è "sempre necessitata dall'indeterminatezza di tutte le norme, derivante a sua volta dalla vaghezza di ogni linguaggio" ([19]). Di conseguenza, i predicati del linguaggio giuridico hanno una penombra "di casi in cui l'applicabilità della norma è opinabile" ([20]).

Olmstead venne accusato di essere un contrabbandiere di alcolici e di violare il "*Prohibition Act*" sulla base di prove acquisite mediante strumenti di *wiretapping* installati nel suo ufficio e sulle linee di comunicazione della strada accanto la sua abituazione. Il convenuto fece ricorso lamentando la violazione del Quarto emendamento ([21]) ma la Corte Suprema ritenne non applicabile tale emendamento in quanto non si era verificata alcuna violazione fisica nell'abitazione e nell'ufficio di Olmstead. Tuttavia, il giudice Holmes, membro della Corte Suprema dal 1902 al 1935, nella sua *disenting opinion* affermò che "*The protection guaranteed by the Amendments is much broader in scope. The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings, and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as*

---

[16] MIGLIETTI, *Profili storico-comparativi del diritto alla privacy, Diritti comparatati Comparare i diritti fondamentali in Europa,* 4 dicembre 2014, p. 4. https://www.dirittocomparati.it/profili-storico-comparativi-del-diritto-alla-privacy/.

[17] Olmstead v. United States 277 U.S. 438 (1928).

[18] GUARDA e BINCOLETTO, *Diritto comparato della privacy e della protezione dei dati personali, Milano, 2023, p.25.*

[19] VIGGIANI, *Il penumbral reasoning nella giurisprudenza nordamericana, Jura Gentium,* 2011, p. 3. https://www.juragentium.org/topics/rights/it/viggiani.pdf.

[20] *Op.ult.cit.*

[21] Bill of Rights, Quarto Emendamento: "*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".*

against the Government, the right to be let alone -- the most comprehensive of rights, and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment. And the use, as evidence in a criminal proceeding, of facts ascertained by such intrusion must be deemed a violation of the Fifth" ([22]).

Uno dei *leading case* che avallò la *constitutional penumbral theory*, affermando la possibilità di applicare in via estensiva il Primo e il Quattordicesimo Emendamento è Griswold v. Connecticut ([23]). In quegli anni, nello Stato del Connecticut veniva punito ogni utilizzo di contraccettivi e chi ne agevolasse l'utilizzo: due medici, arrestati e multati per averne promosso l'uso, decisero però di impugnare il provvedimento, ritenendolo in contrasto con gli emendamenti Primo ([24]) e alla clausola del *Due process* del Quattordicesimo emendamento ([25]). Il caso venne portato di fronte alla Corte Suprema il quale, facendo riferimento a due importanti casi ([26]), ricostruì e rifedì le garanzie del Primo emendamento, stabilendo che tutti gli articoli del *Bill of Rights,* comprendono "garanzie le quali si estendono oltre quanto specificatamente enunciato, andando a ricomprendere una penombra nella quale sono presenti diritti e libertà senza i quali quanto garantito nel *Bill of Rights* sarebbe svuotato di gran parte del proprio significato" ([27]). Con questa sentenza si verificò un primo riconoscimento al diritto alla privacy, non del singolo individuo ma della coppia sposata che ha diritto a poter compiere le proprie scelte in materia di contraccezione senza subire ingerenze dello Stato, in quanto questo rappresenta un elemento della loro vita privata. In seguito a questa sentenza, si sviluppa

---

[22] Olmstead v. United States, 277 U.S. 479 (1928), https://www.law.cornell.edu/supremecourt/text/277/438.

[23] Griswold v. Connecticut, 381 U.S 479 (1965).

[24] Bill of Rights, Primo Emendamento: "*Il Congresso non potrà emanare leggi per il riconoscimento di una religione o per proibirne il libero culto, o per limitare la libertà di parola o di stampa o il diritto dei cittadini di riunirsi in forma pacifica e d'inviare petizioni al governo per la riparazione dei torti subiti*".

[25] Bill of Rights Quattordicesimo Emendamento Sezione I:" *Tutte le persone nate o naturalizzate negli Stati Uniti e soggette alla loro sovranità sono cittadini degli Stati Uniti e dello Stato in cui risiedono. Nessuno Stato porrà in essere o darà esecuzione a leggi che disconoscano i privilegi o le immunità di cui godono i cittadini degli Stati Uniti in quanto tali; e nessuno Stato priverà alcuna persona della vita, della libertà o delle sue proprietà, senza due process of law, né rifiuterà ad alcuno, nell'ambito della sua sovranità, la equal protection of the laws*".

[26] Meyer v. Nebraska, 262 US 390 (1923) e Pierce v. Society of Sisters, 268 US 510 (1925).

[27] Fabiano, *Tanto tuonò che piovve: l'aborto, la polarizzazione politica e la crisi democratica nell'esperienza federale statunitense, BioLaw Journal*, 2022, p. 7. *https://teseo.unitn.it/biolaw/article/view/2377/2302*.

una nuova idea di privacy che consiste nel diritto del singolo di autodeterminarsi nelle scelte che rientrano nella sua sfera privata. Nel caso Roe v. Wade ([28]) la Corte Suprema fece rientrare all'interno di questa nuova concezione anche il diritto di una donna a terminare una gravidanza, azione che lo Stato del Texas vietava.

Ulteriore caso dove la Corte ha esteso l'interpretazione del Quarto Emendamento ([29]) è Katz v. United States ([30]). La vicenda riguardava l'utilizzo da parte del *Federal Bureau of Investigation* (FBI) di uno strumento inserito in una cabina telefonica a fini investigativi. La Corte Suprema si è espressa dichiarando illegittimo l'utilizzo di tale strumento sulla base del fatto che il Quarto Emendamento tutela la privacy delle persone dalle ingerenze dello Stato senza un legittimo mandato.

La tutela della privacy ottenuta grazie all'opera dei giudici riguardava in particolare la protezione del privato da violazioni compiute da autorità pubbliche. A livello federale una delle leggi più importanti in materia emanata dal Congresso nel 1970, è il *Privacy Act,* che regola appunto i rapporti tra privato e pubblico in quest'ambito. A livello statale, invece, sono state adottate numerose leggi, volte a disciplinare il versante privatistico ossia le lesioni della privacy poste in essere da soggetti diversi dalle Istituzioni. Negli USA tuttora difetta una legge federale che regola i rapporti tra privati in materia di privacy: i vari testi normativi ([31]) emanati dagli stati statunitensi hanno confermato la privacy come un diritto del consumatore che deve essere bilanciato con gli interessi delle imprese, invece che come un diritto fondamentale dell'individuo. Questo perché gli Stati Uniti "consultarono esclusivamente le aziende e la conseguente regolamentazione fu basata su una bozza preparata dall'industria delle telecomunicazioni" ([32]). In questo modo, la normativa statunitense in materia di *data protection* tutela maggiormente gli interessanti aziendali, mentre a livello europeo, dove invece vennero interpellate le

---

[28] Roe v. Wade 410 U.S. 113 (1973).

[29] *Bill of Rights, Quarto Emendamento:" 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 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*".

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

[31] *California Consumer Privacy Act, Virginia Consumer Data Protection Act, Colorado Privacy Act, Connecticut Data Privacy Act.*

[32] SAETTA, *Privacy negli Usa, Protezione dati personali,* 2016. https://protezionedatipersonali.it/privacy-negli-usa#:~:text=Negli%20Usa%20non%20esiste%20una,tutelano%20la%20protezione%20dei%20dati.

diverse autorità nazionali, la regolamentazione si concentra maggiormente sulla tutela dei cittadini. È noto che negli Stati Uniti, il centro del sistema giuridico è l'autonomia individuale e la libertà personale e l'ordinamento segue un approccio utilitaristico e autoregolamentante. Il diritto alla privacy è affidato all'equilibrio del mercato e le aziende, consapevoli di questo, tutelano i consumatori inserendo delle clausole di protezione dei dati personali all'interno dei loro termini di servizio. Sulla base di questa impostazione, la *Federal Trade Commission* ([33]) è incaricata di garantire la *data protection,* integrandola con la tutela dei consumatori, e l'integrità delle transazioni commerciali. L'approccio americano sicuramente risulta efficacie e adattabile rispetto le nuove tecnologie; tuttavia, rischia di considerare la privacy come un prodotto scambiale all'interno del mercato, andando così a ridurne l'importanza. Come si potrà vedere invece, l'Unione europea, il quale si basa su di un approccio generalista e centralizzato, considera la privacy come diritto fondamentale dell'individuo riconoscendone la giusta importanza.

1.2 Dal diritto alla privacy statunitense al diritto alla riservatezza europeo

Nel 1948 con l'entrata in vigore della Dichiarazione universale dei diritti dell'uomo dell'Organizzazione delle Nazioni Unite è stato affermato in modo universale il valore fondamentale dell'uomo, riconoscendo che ogni persona è titolare di diritti e libertà che devono essere tutelati e che deve essere protetta da "interferenze arbitrarie nella vita privata, nella famiglia, nella casa, e nella corrispondenza" ([34]). Due anni più tardi, nel 1950, attraverso la Convenzione Europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali è stato riconosciuto il diritto al rispetto della vita privata e famigliare, del domicilio e della corrispondenza. L'articolo 8 della CEDU così recita: «1. Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza. 2. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui». Con la Convenzione Europea per la salvaguardia dei diritti

[33] Agenzia governativa statunitense istituita nel 1914. Il suo compito principale è quelli di promuovere la tutela dei consumatori e l'eliminazione e prevenzione di pratiche commerciali anticoncorrenziali.
[34] *Dichiarazione universale dei diritti dell'Uomo dell'Organizzazione delle Nazioni Unite*, Articolo 12.

dell'uomo e delle libertà fondamentali insieme anche all'attività della giurisprudenza della Corte di Giustizia, è stata riconosciuta una prima tutela del diritto al rispetto della propria vita privata evitando così un vuoto di tutela. Questo ha rappresentato l'avvio del lungo processo di riconoscimento del diritto alla riservatezza. In seguito al Trattato di Mastricht del 1993, nel 1995 entrò in vigore la Direttiva 95/46/CE "relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione dei dati", il quale stabilì confini precisi per la raccolta, conservazione e trattamento dei dati personali. L'obbiettivo principale fu quello di emanare una normativa armonica di tutela dei dati personali, nonostante la discrezionalità lasciata agli Stati membri essendo un atto non direttamente applicabile. La Direttiva è considerata fondamentale in quanto dimostrò, per la prima volta, che un forte livello di protezione dai trattamenti dei dati personali è doveroso al fine di consentire e garantire una libera circolazione, all'interno dell'Unione, dei dati stessi. Protezione e libera circolazione sono necessariamente legati e la Direttiva ne fu la prova; all'interno della normativa venivano disciplinati tutti gli aspetti del trattamento, come la liceità, le finalità, i ruoli. Subito dopo l'emanazione della Direttiva, negli anni 2000, è stata emanata la Carta dei Diritti Fondamentali dell'Unione Europea che ha rappresentato un cambio di direzione perché si è passati dal concentrarsi esclusivamente sull'aspetto economico e di integrazione ad un focus sui diritti fondamentali. La Carta disciplina sia il diritto al rispetto della vita privata sia il diritto alla protezione dei dati personali. Come si potrà vedere all'interno di questo elaborato, questi due diritti sono differenti. In generale si può affermare che nel diritto al rispetto della vita privata l'obiettivo è quello di impedire interferenze illecite mentre il diritto alla protezione dei dati personali si manifesta in poteri di intervento e lo Stato e i responsabili del trattamento devono attivarsi per far che il trattamento sia lecito. Il diritto alla riservatezza rientra nei diritti della personalità e troviamo un suo riconoscimento sia nell'art. 8 della CEDU sia, successivamente, nell'art. 7 della Carta di Nizza. L'articolo 7 prevede che: «Ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni».

Mentre il diritto alla protezione dei dati è previsto dall'articolo 8 della Carta dei Diritti Fondamentali che così cita: «1. Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano. 2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di

accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica. 3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente». L'articolo 8 va "riferito ad ogni informazione relativa ad una persona fisica identificata o identificabile*"* ([35]), salvo che si "tratti di informazioni che incidono sulla vita privata dell'individuo*"* ([36]).

La Carta dei Diritti Fondamentali dell'Unione Europea, prevedendo due articoli differenti che disciplinano il rispetto alla vita privata e familiare e il diritto alla protezione dei dati personali, si distacca dall'approccio adottato dalla CEDU e permette di dedurre che questi due diritti siano situazioni giuridiche soggettive diverse. Inizialmente la Carta di Nizza non aveva un valore giuridico vincolante ma solo politico, sulla base del suo "carattere meramente declaratorio e simbolico" ([37]) ma, con l'entrata in vigore nel 2009 del Trattato di Lisbona ([38]), le è stata conferito la qualifica di fonte del diritto primario dell'Unione. L'articolo 8 della Carta di Nizza ha sostanzialmente recepito i principi previsti dalla cit. Direttiva, con la quale si è cercato di trovare un equilibro tra la libera circolazione dei dati e il rispetto dei diritti fondamentali dell'uomo, tra cui appunto quello alla riservatezza e alla protezione dei dati personali. Inoltre, un riconoscimento del diritto alla protezione dei dati è presente nell'articolo 16 del TFUE ([39]) e secondo la Commissione europea esso rappresenta "una base giuridica specifica" ([40]).

1.2.1 Il diritto alla riservatezza in Italia

Nell'ordinamento italiano si iniziò a discutere di diritto alla riservatezza e tutela della vita privata solamente a partire dagli anni Cinquanta del Novecento. In mancanza di norme che menzionassero o implicassero il diritto alla riservatezza, emersero due diverse correnti di pensiero. Una parte della dottrina mostrava ancora una certa ritrosia a

---

[35]Corte di Giustizia dell'Unione Europea, Joined Cases Volker und Markus Schecke (C–92/09) ed Eifert (C–93/09), [2010] ECR I-11063, p. 52.

[36] J. KOKOTT, C. SOBOTTA, *The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR*, International Data Privacy Law, Volume 3, Issue 4, novembre 2013, p. 222–228.

[37] CHIARELLO, *Il valore costituzionale della Carta di Nizza: un problema ancora aperto anche alla luce della sentenza n. 269/2017 della Corte costituzionale, Consulta online, 2018,* p. 378. https://giurcost.org/contents/giurcost/studi/chiariello.pdf.

[38] Articolo 6 Trattato di Lisbona, comma primo: "1. L'Unione riconosce i diritti, le libertà e i principi sanciti nella Carta dei diritti fondamentali dell'Unione europea del 7 dicembre 2000, adattata il 12 dicembre 2007 a Strasburgo, che ha lo stesso valore giuridico dei trattati".

[39] Articolo 16 TFUE, comma primo: "1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano".

[40] Relazione alla proposta di Regolamento 2012/11, Commissione europea, p. 2. https://www.europarl.europa.eu/meetdocs/2009_2014/documents/com/com_com(2012)0011_/com_com(2012)0011_it.pdf.

considerarlo una situazione giuridica autonoma, ritenendo che la sua tutela rientrasse all'interno del diritto d'autore e di copyrights; altrui autori si mostravano invece decisamente propensi a riconoscere in esso un distino diritto soggettivo. Il dibattito, nel silenzio del legislatore, rese il ruolo della giurisprudenza decisivo. Subito dopo la Seconda Guerra Mondiale i giudici civili incominciarono in effetti ad occuparsi del diritto alla riservatezza in relazione alla protezione della vita privata delle persone dotate di una certa notorietà. Tra le sentenze più importanti, bisogna sicuramente citare il caso Caruso c. Tirrena Asso Film ([41]). Il signor Caruso era un famoso cantante e all'interno di un film vennero rappresentati alcune vicende della sua vita privata come il fatto che era incline all'ubriachezza e che aveva contratto diversi debiti. Anche se le vicende erano raccontate in modo romanzato, la famiglia chiamò in causa la casa produttrice ritenendo che il film violasse la riservatezza del cantante, e ne ledesse la memoria e l'onore. La sentenza di primo grado rigettò la richiesta di sequestro cautelativo, adducendo «l'esistenza di un interesse pubblico alla conoscenza delle vicende, anche private, di persone celebri» ([42]). Gli eredi fecero ricorso e il Tribunale di Roma ritenne «lecito rievocare in un film, anche senza il consenso degli aventi diritto, la vita di una persona celebre», con estromissione di quegli avvenimenti privati la cui narrazione, «non essendo giustificata dalle esigenze della valutazione della personalità e della conoscenza delle circostanze che hanno concorso alla formazione alla formazione di essa», appaga solo il desiderio «di indiscrezione del pubblico, e con esclusione, comunque, di quei fatti, anche se veri, dalla divulgazione dei quali possa derivare un pregiudizio all'onere, al decoro o alla reputazione della persona rappresentata »([43]). Tale decisione venne fortemente criticata dalla dottrina e ribaltata successivamente dalla Corte di Cassazione la quale statuì che non c'era alcuna norma atta a costituire il fondamento di un autonomo diritto alla protezione della vita privata: per offrire tutela nei casi di specie bastava applicare il precetto generale del *neminem laedere*, stabilito nell'articolo 2043 del Codice civile.

Un altro caso degno di menzione è rappresentato dalla vicenda Petacci c. Palazzi del 1963, che originava, dalla pubblicazione di un libro concernente gli eventi personali della

---

[41] Caruso c. Tirrena Asso Film, n. 4487, 1953.
[42] Pretore di Roma, 19 novembre 1951, *Foro it., 1952, p. 149 e ss.*
[43] Tribunale di Roma, 14 settembre 1953, Foro.it, 1953, p. 115. Richiamata in SIMONE, *Enrico Caruso e il diritto alla riservatezza. Una difficile costruzione giuridica, Teoria e storia del diritto privato, 2021.* https://www.teoriaestoriadeldirittoprivato.com/wp-content/uploads/2021/12/2021_Contributi_Simone.pdf.

Signora Petacci e della sua famiglia. In secondo grado, la Corte d'Appello di Milano riconobbe la presenza di un diritto al "riserbo, come facoltà giuridica di escludere ogni invadenza estranea dalla sfera della propria intimità personale e familiare". I giudici, richiamando l'articolo 8 della CEDU, argomentarono l'esistenza "diritto alle vicende", riconducibile a "una serie di atti umani storicamente individuati" ([44]), come diritto alla personalità differente dal diritto all'onore ([45]), meritevole di ricevere autonoma tutela giuridica ([46]). Il caso giunse fino alla Corte di Cassazione ([47]) che, attraverso una sentenza epocale, cambiò la propria iniziale presa di posizione statuendo che: «Sebbene non sia ammissibile il diritto tipico alla riservatezza, viola il diritto assoluto di personalità, inteso quale diritto erga omnes alla libertà di autodeterminazione nello svolgimento della personalità dell'uomo come singolo, la divulgazione di notizie relative alla vita private, in assenza di un consenso almeno implicito, ed ove non sussista, per la natura dell'attività svolta dalla persona e del fatto divulgato, un preminente interesse pubblico di conoscenza».

In questo modo, la Corte di Cassazione accolse l'idea di un diritto inalienabile della personalità, anche se non riconobbe ancora completamente autonomia al diritto di riservatezza. La decisione risultò non molto soddisfacente, sia per coloro che riconoscevano l'esistenza del diritto in questione sia per coloro che ne negavano il fondamento giuridico.

Per giungere al pieno riconoscimento del diritto alla riservatezza bisognerà attendere il 1975 con il caso Soraya Esfandiari c. Rusconi Editori. L'attrice chiamò in causa la casa editrice in seguito alla pubblicazione, in una rivista, di alcune foto ritraenti alcuni suoi momenti intimi all'interno del suo domicilio. La principessa Soraya lamentava una violazione del proprio domicilio e della sua riservatezza: richiese quindi il risarcimento per i danni subiti. Nell'attesa della pronuncia di merito domandò pure l'adozione di un sequestro conservativo. La principessa ottenne il provvedimento cautelare e poi vinse nel merito. Il convenuto impugnò tuttavia la decisione di prime cure dinanzi alla Corte di

---

[44] CARNELUTTI, *Diritto alla vita privata, Rivista trimestrale di diritto pubblico,* 1955, Vol. 1, p. 3 e ss.
[45] RAVÀ, *Sul diritto alla riservatezza, in Foro padano,* 1955, Vol. *1,* p. 467 ss.
[46] DE CUPIS, *Sul limite della tutela della riservatezza, in Foro padano,* 1955, Vol. 1, pp. 471 ss.
[47] Cass. Civ., Sentenza n. 990 del 20 aprile 1963, massima reperibile al seguente link: https://www.altalex.com/documents/news/2021/05/11/diritto-ad-essere-dimenticati.

Appello di Milano ([48]), che confermò il risarcimento del danno, dal momento che la principessa aveva subito un danno d' immagine, ma non ritenne di accordare alcuna compensazione per la violazione del diritto alla riservatezza, visto che non poteva ancora essere considerato un autonomo diritto della personalità. La Corte di Cassazione, investita della questione con il ricorso proposto dalla principessa, riconobbe l'esistenza di un fondamento del diritto alla riservatezza grazie ad un'interpretazione evolutiva ([49]) dell'articolo 2 della Costituzione eliminando così ogni dubbio sull' autonomia del diritto in questione. Secondo la celeberrima pronuncia, i giudici di legittimità misero in chiaro che l'articolo 2 della Costituzione ha come obiettivo una tutela "a tutto tondo" della persona, che non è limitata ai soli diritti della personalità contemplati espressamente, ma è aperta e interpretabile in modo da comprendere tutti gli aspetti della persona, anche se non sono oggetto di esplicite tutele o tipizzazioni legislative. La S.C descrisse il diritto alla riservatezza in questi termini: «tale diritto consiste nella tutela di quelle situazioni e vicende strettamente personali e familiari, le quali, anche se verificatesi fuori del domicilio domestico, non hanno per i terzi un interesse socialmente apprezzabile, contro le ingerenze che, sia pure compiute con mezzi leciti, per scopi non esclusivamente speculativi e senza offesa per l'onere, la reputazione e il decoro, non siano giustificate da interessi pubblici preminenti» ([50]).

Grazie a questa sentenza, si è raggiunto un riconoscimento costituzione del diritto alla privacy. Tuttavia, sono presenti diverse tesi su quale sia l'articolo costituzionale a sostegno di questo riconoscimento. Una prima corrente di pensiero condivide la scelta fatta dalla Corte nell' individuare l'articolo 2 come base giuridica di suddetto diritto. La clausola "la Repubblica riconosce e garantisce i diritti inviolabili dell'uomo" può essere estesa per far rientrare anche gli aspetti della persona umana che non vengono previsti direttamente nella Costituzione ma che sono comunque meritevoli di tutela come la riservatezza. Ulteriore tesi, invece, vede l'articolo 13 come fondamento in quanto nella concezione di libertà personale vi rientra sia l'elemento corporale sia quello morale della persona umana. In questo modo, anche la dignità umana rientrerebbe nella nozione di libertà personale e sarebbe quindi inviolabile. La terza e ultima tesi invece, trova il

---

[48] App. Milano 19 gennaio 1971.
[49] PAGALLO, IL *diritto nell'età dell'informazione. Il riposizionamento tecnologico degli ordinamenti giuridici tra complessità sociale, lotta per il potere e tutela dei diritti,* Torino, 2014, p 231-232.
[50] Cass. Civ. Sentenza n. 2129 27 maggio 1975, *JStor,* p. 2896. https://www.jstor.org/stable/23173994.

fondamento nell'articolo 21. Secondo questa impostazione, la libertà di pensiero di una persona si manifesterebbe anche nel limitare i destinatari della manifestazione di pensiero se questa contiene informazioni private. In realtà, la tesi che prevale è quella che vede il fondamento del diritto alla riservatezza nell'insieme delle interpretazione di tutti gli articoli sopra citati. Interessante risulta essere il punto di vista del celeberrimo giurista Stefano Rodotà ([51]), il quale sostiene che non occorre cercare un generale diritto alla riservatezza ma interpretare i diritti fondamentali in modo che vi possa rientrare la riservatezza.

Dalla decisione della Corte nel caso Soraya Esfandiari c. Rusconi Editori fino all'emanazione della Direttiva 95/46/CE, la dottrina faceva rientrare nella nozione di riservatezza "non solo il diritto di respingere le invasioni della sfera privata, ma soprattutto il diritto di controllare il flusso di informazioni riguardanti un determinato soggetto" ([52]). In realtà, come sarà possibile vedere all'intero dell'elaborato, il diritto alla riservatezza e il diritto alla protezione dei dati personali sono differenti.

1.3 Cambiamento tecnologico: lo sviluppo del diritto alla protezione dei dati

Il cambiamento tecnologico è stato decisivo affinché maturasse all'interno dell'ordinamento dell'Unione Europea (e quindi del sistema italiano) l'evoluzione normativa che determinò il passaggio dal diritto alla riservatezza al diritto per la protezione dei dati. Ai nostri fini possono essere individuate tre fasi della rivoluzione digitale, che incisero in maniera significativa sul fenomeno in parola. La prima iniziò negli anni Settanta, quando vennero prodotti i primi calcolatori: si trattava di dispositivi molto costosi e di notevoli dimensioni, per cui solamente le grandi imprese pubbliche potevano acquistarli. Negli anni Ottanta cominciarono ad essere immessi nel mercato calcolatori più piccoli ed economici, che divennero così appetibili anche per le piccole e medie imprese private. L'ultima fase iniziò negli anni Novanta, quando i computer iniziarono ad essere acquistati in massa anche dai consumatori, soprattutto grazie alle vaste potenzialità di connessione che si determinano con l'avvento di Internet.

Attraverso i computer si potevano memorizzare grandi quantità di informazioni, ma soprattutto accedervi facilmente e condividere moli di dati fino ad allora impensabili. Non

---

[51] RODOTÀ, *Intervista su privacy e libertà,* Roma-Bari, 2005, p. 13.
[52] RODOTÀ, *Elaboratori elettronici e controllo sociale,* Bologna, 1973, p.130.

ci volle molto per capire l'importanza di garantire una tutela adeguata, che andasse ben al di là dell'inviolabilità del domicilio e della vita intima, per proteggere il titolare di dati personali rispetto al trattamento operato sugli stessi da parte di altri soggetti. In Europa i primi provvedimenti che adottarono questo approccio furono la Direttiva 95/46/CE, relativa alla tutela della protezione delle persone fisiche con riguardo al trattamento dei dati personali, cui seguiranno poi la Direttiva 97/66 CE sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni e la Direttiva 2002/58/CE, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche. La Direttiva 95/46 è stata la più importante in quanto rappresentò il primo intervento normativo di ampio respiro sul trattamento dei dati personali, che si poneva l'obbiettivo di bilanciare i diritti e le libertà delle persone con la libera circolazione dei dati personali e lo sviluppo tecnologico. In Italia, la Direttiva venne recepita attraverso la legge n. 675 del 31 dicembre 1996, che istituì la figura del Garante per la protezione dei dati personali. La legge n. 675/1996 verrà poi abrogata dal Codice in materia di protezione dei dati personali emanato con il D.LGS n.196/2003, il quale introduce nel nostro ordinamento, accanto al diritto alla riservatezza, un autonomo diritto alla protezione dei dati personali. La Direttiva 95/46 costituì il quadro normativo di riferimento per la protezione dei dati personali per un lungo periodo, fino al 2016, quando fu adottato il Regolamento Generale sulla Protezione dei Dati Personali.

1.4 General Data Protection Regulament (GDPR)

Il Regolamento Generale per la Protezione dei Dati (GDPR) è stato approvato il 27 aprile 2016 ed è divenuto applicabile il 25 maggio 2018. Uno dei motivi che ha portato all'emanazione di questo atto era la necessità di uniformare la normativa in materia di tutela dei dati personali all'interno dell'Unione Europea. Il legislatore europeo ha voluto adottare un regolamento per armonizzare il quadro normativo che con la Direttiva 95 si era frammentato in seguito alle differenti modalità di attuazione adottate dagli Stati in sua recezione. Il GDPR ha permesso di creare un "diritto comune in materia di privacy" ([53]). Il Regolamento riprende gran parte dei principi e disposizioni previste dalla Direttiva, rispetto alla quale viene tuttavia complessivamente rafforzata e resa più efficacie la tutela

[53] COLAPIETRO, IANNUZZI, *I principi generali del trattamento dei dati personali e i diritti dell'interessato, Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679,* Napoli, 2017, p. 90.

dei dati personali. La necessità di emanare un regolamento in materia di *data protection* è sorta principalmente per due fattori. In primo luogo, la Direttiva del 1995 non era più in grado di fornire una tutela adeguata rispetto alle nuove tecnologie, che tra il 1995 e il 2016 hanno avuto uno sviluppo esponenziale. Inoltre, in quel periodo si è avuto un rinnovo della cornice costituzionale e un cambiamento ([54]) degli obiettivi dell'Unione europea con la consacrazione della tutela della persona fisica. Un ruolo particolarmente importante all'interno del GDPR è svolto dai considerando. Nonostante non siano dotati di una forza giuridica vincolante sono necessari per interpretare il Regolamento in modo corretto, in quanto esplicitano i "principi ispiratori dell'intervento normativo" ([55]) e la sua "motivazione giuridica." ([56]).

1.4.1 Ambito materiale e territoriale del GDPR

L'ambito materiale di applicazione del GDPR è delineato nell'articolo 2, il quale stabilisce che le disposizioni in esso contenute trovano applicazione al "trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi*"* ([57]). Il GDPR ha ampliato la definizione dei dati personali rispetto alla Direttiva 95/46/CE: in base all'articolo 4 reg.cit. ([58]). In particolare, vengono previsti nuovi aspetti identificativi della persona, aumentano così "il novero di elementi attribuibili ad un soggetto e definibili dati personali" ([59]). In questo modo, all'interno dell'ambito di applicazione del GDPR, rientrano anche i dati pseudonimizzati in quanto in grado di identificare il titolare e quindi diventare personali.

---

[54] "L' approccio delle istituzioni europee è passato da una configurazione prevalentemente market-driven a una fundamental rights-oriented". M. BASSINI, *la svolta della privacy europea: il nuovo pacchetto sulla tutela dei dati personali, in QC,* 2016, p. 588.

[55] C. COLAPIETRO, *I principi ispiratori del Regolamento UE 2016/679 sulla protezione dei dati personali e la loro incidenza sul contesto normativo nazionale*, Federalismi.it, 2018, p. 4.

[56] F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali*, Torino, 2016, p. 8-10.

[57] Articolo 2 GDPR:" Ambito *di applicazione materiale*".

[58] Articolo 4 GDPR :*"* «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, 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;".*

[59] DI CIOLLO, *L'ambito di applicazione della normativa privacy: analisi comparata tra GDPR e direttiva 95/46/CE, Iusintinere.it,* 2019, p. 2, https://www.printfriendly.com/p/g/sKdbNA.

Il GDPR tutela i dati personali dal trattamento ([60]) automatizzato e manuale, ma esulano dal suo campo applicativo i trattamenti di cui articolo 2, ove sono ad esempio menzionati quelli compiuti da autorità competenti a fini di indagine, prevenzione o accertamento oppure i trattamenti compiuti da persone fisiche per scopi personali e non commerciali.

In base all'articolo 3 il GDPR opera per i "trattamenti dei dati personali effettuati nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione." ([61]) Questo significa che il GDPR si applica ad esempio nel caso in cui una società che possiede uno stabilimento all'interno dell'Unione processi i dati, ma il loro trattamento avvenga in un paese non Europeo. L'articolo specifica poi che il reg. si applica anche "al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano: l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione" ([62]). Grazie a quest'articolo, il GDPR riesce a fornire una notevole tutela al *data subject* ([63]), visto che la maggior parte dei soggetti fornitori di servizi e titolari del trattamento dovranno rispettare le disposizioni previste anche nei casi in cui quest'ultimi non siano situati all'interno dell'Unione Europea.

1.4.2 I ruoli all'interno del trattamento dei dati personali

L'articolo 4 del GDPR definisce tutti i soggetti che ricoprono un ruolo durante il trattamento dei dati personali. La prima figura da analizzare è il titolare del trattamento (data processor) che può essere una persona fisica, giuridica, una pubblica autorità o un diverso organismo, che, in autonomia oppure cooperando con altri, individua quelle che sono le finalità e i mezzi del trattamento. Il titolare stabilisce le modalità e le misure

---

[60] Articolo 4 GDPR : *"*«trattamento»: *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;".*

[61] Articolo 3 GDPR:" *Ambito di applicazione territoriale*".

[62] Articolo 3 GDPR:" *Ambito di applicazione territoriale*".

[63] Soggetto titolare dei dati e interessato del trattamento.

tecniche con cui deve essere realizzato il trattamento dei dati personali e ne è responsabile. Il titolare può delegare ad un soggetto dei compiti e tale viene definito, nell'articolo 4, come responsabile (data controller). Anche questo soggetto può essere una persona fisica o giuridica, un'autorità pubblica oppure altro organismo delegato dal titolare. Il responsabile deve essere in grado di garantire misure tecniche adeguate a rispettare i principi e le norme previste dal GDPR e è responsabile nel caso in cui non rispetti le indicazioni del titolare. Il GDPR ha altresì introdotto la possibilità per il responsabile di nominare un sub-responsabile, ma con una previa autorizzazione scritta del titolare. L'articolo 29 ([64]) invece regola la figura dell'autorizzato, ovvero la persona fisica che materialmente tratta i dati e che agisce sotto l'autorità del titolare o del responsabile.

Una novità che è stata introdotta dal GDPR è la figura del *Data Protection Officer* (DPO). Si tratta di un soggetto esperto di protezione dei dati personali che si occupa di valutare e organizzare la gestione del trattamento dei dati personali svolto dalle diverse organizzazioni. Il DPO funge da consigliere per il titolare e il responsabile e valuta se la normativa viene rispettata e applicata correttamente. Rappresenta una sorta di intermediario tra titolare e interessato del trattamento e in certi casi la sua nomina è obbligatoria ([65]). Infine, l'ultima figura del trattamento è l'interessato, cioè la persona fisica titolare dei dati personali che vengono trattati (*data subject*).

1.4.3 I principi del GDPR

Il GDPR prevede una serie di principi che devono essere rispettati al fine di garantire un trattamento dei dati personali lecito e sicuro. Il Regolamento riprende quanto già sancito dalla Direttiva introducendo alcune novità. La conferma e l'introduzione di nuovi principi, ribadisce l'importanza e la necessità di porre delle limitazioni ai titolari del trattamento. Quest'ultimo non è libero nello scegliere le modalità del trattamento ma è

---

[64] Articolo 29 GDPR:*" Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri".*

[65] Articolo 37 GDPR paragrafo 1:*" Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogni qualvolta: 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 trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; oppure c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categoria particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10".*

tenuto a rispettare suddetti principi. È evidente che questa condizione di conformità rappresenta una sorta di primo livello di tutela per il data subject. Nel caso in cui l'interessato si renda conto di subire un trattamento illecito, può adire ad un secondo livello di tutela, la presentazione di un reclamo a Garante oppure mediante ricorso all'autorità giudiziaria. Secondo l'articolo 5 i dati devono "essere trattati in modo lecito, corretto e trasparente". Affinché il trattamento sia considerato lecito, è necessario che abbia una base legale legittima, che può essere l'espressione del consenso oppure una delle condizioni previste nell'articolo 6 del GDPR.

La correttezza invece, consiste nel divieto di abuso della posizione del titolare e responsabile del trattamento e che l'acquisizione e utilizzo dei dati avvengano in modo corretto e coerente con quanto stabilito nell'informativa del trattamento dei dati personali. Inoltre, le informazioni non devono essere trattate in modo pregiudizievole e discriminatorio. Questo principio è fortemente legato al principio di trasparenza, una delle novità rispetto alla Direttiva 95/46. Quest'ultimo impone che le informazioni destinate al pubblico o al titolare dei dati siano accessibili e comprensibili. Per rendere comprensibile all'interessato l'intero contesto, particolarmente chiare devono essere le informazioni che riguardano il titolare e il responsabile del trattamento dei dati e le finalità che questi ultimi vogliono perseguire. Questo principio si traduce nella creazione dell'informativa che è "funzionale alla formazione ed espressione di un consenso al trattamento autenticamente libero e consapevole, nonché all'eventuale esercizio di tutti i diritti dell'interessato" ([66]).

In seguito, l'articolo introduce uno dei concetti fondamentali del GDPR, la limitazione delle finalità. Questo principio sancisce che i dati possono essere trattati solamente per gli scopi previsti e comunicati dal titolare del trattamento all'interessato e per i quali quest'ultimo ha fornito il suo consenso. Qualsiasi tipologia di trattamento svolto per finalità differenti da quelle stabilite è illecito.

Ulteriore principio è la minimizzazione dei dati secondo cui il titolare del trattamento deve utilizzare solamente i dati personali che sono adeguati, pertinenti e limitati a quanto necessario. Non è possibile raccogliere dall'interessato dati ulteriori non inerenti alle finalità del trattamento. I dati devono essere esatti e aggiornati e il titolare del trattamento deve adottare misure idonee per cancellare o rettificare i dati. Inoltre, devono essere

[66] CALIFANO, *Privacy: affermazione e pratica di un diritto fondamentale,* Napoli, 2016, p.63.

"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". Questo è il principio della limitazione della conservazione, che può però subire delle eccezioni nei casi in cui i dati vengono conservati per fini di interesse pubblico o di ricerca.

Il titolare e il responsabile del trattamento sono tenuti a rispettare il principio di responsabilizzazione che trova il suo fondamento nell'articolo 25 del Regolamento. Si tratta di una delle novità introdotte dal GDPR in quanto il precedente modello della Direttiva 95/46 legato alla sola prestazione del consenso dell'interessato, non era sufficientemente adeguato per tutelare l'interessato. Con l'intervento del legislatore europeo, è stato previsto l'obbligo per i gestori del trattamento di valutare attentamente tutti i rischi che possono derivare dalle loro attività. In particolare, questo principio "consiste nell'assumere comportamenti proattivi, tali da dimostrare la concreta adozione di adeguate misure di carattere preventivo finalizzate ad assicurare l'applicazione del Regolamento e la tutela dei diritti e delle libertà dei soggetti interessati e delle persone" ([67]).

Un altro articolo molto importante è il 25, che prevede i cosiddetti principi di "protezione della vita privata fin dalla progettazione (by design) e protezione per impostazione predefinita (by default)". La norma impone due obblighi generali al titolare del trattamento e il mancato rispetto è soggetto a sanzione, secondo gli articoli 82 e 83 del medesimo Regolamento. Il dovere di adottare misure di data protection by design e by default deve essere rispettato anche dalle Autorità competenti, come il Garante per la protezione dei dati personali, che trattano i dati a fini investigativi, di accertamento e di prevenzione ([68]).

1.4.4 Obblighi di sicurezza: articolo 32 del GDPR

In questo elaborato analizzeremo quelle che sono le tutele e i diritti che l'interessato può esercitare in caso di violazione della sua privacy e i due diversi percorsi di tutela, giurisdizionale e amministrativo. Il GDPR prevede, negli articoli 32 e seguenti, una serie

---

[67] Università degli studi di Catania, *Trattamento dei dati personali,* 2019, p. 11. https://web.dmi.unict.it/sites/default/files/files/guida_lettura_regolamento_gdpr.pdf.

[68] Direttiva 2016/680 *"relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati"*.

di obblighi che il titolare del trattamento deve rispettare e che riguardano la sicurezza del trattamento stesso e che tutelano maggiormente l'interessato. Come esaminato in precedenza, l'articolo 5 prevede che il titolare sia tenuto a adottare delle misure di sicurezza al fine di garantire l'integrità e la riservatezza dei dati. Questo principio viene ripreso anche dall'articolo 32 che introduce alcuni obblighi di sicurezza. In particolare, si stabilisce che il titolare e il responsabile del trattamento devono considerare il rischio del loro trattamento e adottare "misure tecniche e organizzative" per mitigare tale rischio. Al fine di rispettare questo obbligo devono essere presi in considerazione "lo stato dell'arte e dei costi di attuazione, nonché della natura dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche" ([69]). La norma, inoltre, fa riferimento ad alcune misure tecniche e organizzative come la pseudonimizzazione e la cifratura dei dati, che il titolare e il responsabile possono adottare per mitigare il rischio del trattamento. Oltre all'articolo 32, all'interno del GDPR, è possibile trovare altre disposizioni che impongono alcuni obblighi al titolare del trattamento e tutelano l'interessato. L'artico 33 stabilisce che in caso di un *data breach* ([70]) che metta a repentaglio la libertà e i diritti della persona fisica, il titolare deve notificare la violazione all'autorità entro settantadue ore dal momento in cui ne è venuto a conoscenza. Al paragrafo quinto del medesimo articolo viene stabilito inoltre che il titolare deve documentare qualsiasi tipo di violazione "comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio" ([71]). La notifica all'autorità di controllo deve contenere una breve descrizione della violazione, il numero dei soggetti interessati, i recapiti del soggetto che l'interessato può contattare per aver più informazioni sulla violazione, le conseguenze e le "*misure adottate da parte del titolare per porre rimedio alla violazione dei dati personali*" ([72]). Inoltre, secondo l'articolo 34, il titolare del trattamento è tenuto a informare la persona fisica titolare dei dati violati nel caso in cui la violazione è suscettibile di presentare un

[69] Articolo 32 GDPR "Sicurezza del trattamento".
[70] Una 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. Una violazione dei dati personali può compromettere la riservatezza, l'integrità o la disponibilità di dati personali. (Garante per la protezione dei dati personali).
[71] Articolo 33 GDPR: *"Notifica di una violazione dei dati personali all'autorità di controllo"*.
[72] Articolo 33 GDPR: *"Notifica di una violazione dei dati personali all'autorità di controllo".*

rischio elevato per i diritti e le libertà delle persone fisiche. Tuttavia, sono previsti dei casi in cui non è necessario comunicare all'interessato la violazione ([73]).

In alcune situazioni, il titolare del trattamento effettua una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali (*Data Protection Impact Assesment*, d'ora innanzi: DPIA) ([74]). Questa valutazione preventiva viene fatta per i trattamenti che, considerati la natura, l'oggetto, il contesto e le finalità, possono presentare un rischio elevato per i diritti e le libertà delle persone fisiche. All'interno della DPIA dev'essere presente una descrizione delle operazioni del trattamento e le sue finalità, compreso l'interesse legittimo ([75]) del titolare, una valutazione sulla necessità e sulla proporzionalità del trattamento e infine, la valutazione del rischio per i diritti e le libertà del *data subject*, nonché le misure per mitigare tale rischio.

Il titolare del trattamento, infine, ha il dovere di consultare l'autorità di controllo prima di un trattamento se la valutazione del trattamento ha dimostrato che esso porterebbe un elevato rischio ai diritti e alle libertà dell'interessato. Questa consultazione preventiva, prevista dall'articolo 36 del GDPR, permette al titolare di capire quali misure tecniche può adottare per tutelare l'interessato ed evitare che il trattamento violi il GDPR.

1.5 Diritto alla riservatezza e diritto alla protezione dei dati non sono sinonimi

La protezione dei dati viene confusa con la definizione di riservatezza in senso stretto e in molti casi non le viene riconosciuta la giusta importanza. Ogni volta che un utente

---

[73] Articolo 34 GDPR paragrafo 3 :*"Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni: a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura; b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1; c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia"*.

[74] Articolo 35 GDPR: *"Valutazione d'impatto sulla protezione dei dati".*

[75] Saetta, *Trattamenti basati sui legittimi interessi del titolare, Protezione dati personali,* 2018, definisce così legittimo interesse: "beneficio che il titolare può ottenere dal trattamento dei dati personali altrui. L'interesse deve essere legittimo, cioè, occorre che sia perseguito secondo modalità conformi alle normative**.** In sostanza deve essere: lecito (ossia conforme al diritto nazionale e unionale applicabile); articolato in maniera sufficientemente chiara, ossia sufficientemente specifico da consentire di eseguire il test comparativo valutando l'interesse legittimo del titolare del trattamento rispetto agli interessi o ai diritti fondamentali dell'interessato; appresentare un interesse concreto ed effettivo (ossia non deve essere teorico e quindi corrispondere alle attività in corso)". *https://protezionedatipersonali.it/trattamenti-basati-su-legittimi-interessi*.

accede ad un sito oppure scarica una nuova app, acconsente a lunghe informative senza darvi la giusta importanza e senza interessarsi troppo a quello che potrebbe succedere ai dati che condividerà tramite la navigazione nel sito o l'accesso all'app. Per capire a pieno l'importanza della data protection è doveroso concentrarsi sulla differenza che sussiste tra la stessa e il concetto di tutela della privacy. All'interno del GDPR viene evidenziata questa distinzione e i relativi strumenti di tutela, ma queste disposizioni non sono ancora percepite nella loro esatta portata dai titolari dei diversi trattamenti dei dati e dagli utenti, nonostante l'approvazione del Regolamento risalga a diversi anni fa. Questa distinzione tra diritto alla riservatezza e diritto alla protezione dei dati è d'interesse comune, non solo per gli esperti del settore e per i titolari del trattamento ma è importante per chiunque interagisca con il mondo digitale.

Il diritto alla privacy permette di rivendicare l'esclusiva disponibilità di informazioni che appartengono al titolare di tale diritto, il quale di conseguenza può decidere se condividerle oppure no. All'interno di questo diritto viene riconosciuta la possibilità, per il titolare, di escludere o limitare l'accesso alle sue informazioni e ai suoi dati da parte di soggetti terzi. Una volta condivise queste informazioni, che possono anche essere sensibili, il solo diritto alla riservatezza non è più sufficiente per tutelare il soggetto. La privacy rappresenta un primo scudo di protezione delle nostre informazioni private perché ci permette di averne la piena disponibilità e di impedire che altri vi accedano ma, una volta che quei dati sono condivisi non ci tutela da un loro illegittimo utilizzo da parte di un soggetto terzo. Il diritto alla protezione dei dati mira a fornire un secondo scudo capace di offrire riparo. L'esclusiva disponibilità delle nostre informazioni è fondamentale tanto quanto la protezione delle stesse, che comunicate, volontariamente o non, necessitano di tutele per rendere la condivisione governabile e sicura.

Ogni soggetto è in possesso di informazioni che riguardano la propria sfera privata e per tutelarsi da una dannosa esposizione, non andrebbero condivise con chiunque. Di fatto però spesso dati sensibili vengono condivisi per compiere i più disperati e banali gesti della quotidianità: quando ci abboniamo ad un servizio online e viene richiesto un metodo di pagamento, quando si ordina un prodotto e è necessario inserire l'indirizzo per la spedizione. Chi riceve queste informazioni deve garantire in concreto che utilizzerà queste informazioni in modo corretto e adotterà misure di sicurezza per proteggerle.

La *data protection* accordata dal Reg. riesce a tutelare maggiormente il dato rispetto alla privacy, perché stabilisce in astratto le garanzie necessarie perché sia accettabile la sua condivisione e in concreto fornisce i mezzi giuridici e tecnici per proteggerlo. La protezione dei dati personali rappresenta un mezzo indispensabile per permette la realizzazione della personalità individuale. La sua manifestazione si esterna mediante i diritti dell'interessato, che rappresentano strumenti di tutela ([76]) e dall'insieme degli obblighi imposti al titolare del trattamento dei dati personali. Bisogna però evidenziare che sovente gli utenti e i titolari del trattamento tendono a sottovalutare e ad ignorare la loro responsabilità in materia di protezione dei dati personali.

La distinzione tra diritto alla privacy e *data protecion* non è presente solamente nel GDPR, ma anche all'interno della Carta dei diritti fondamentali dell'Unione europea dove l'articolo 7 disciplina il "Rispetto per la vita privata e familiare*"* mentre l'articolo 8 riguarda la "Protezione dei dati personali". Come detto in precedenza, la vita privata e familiare rappresenta l'oggetto della tutela della privacy, tesa per lo più a reprimere e a negare intrusioni, mentre la protezione dei dati personali si configura per così dire in positivo, come situazione giuridica soggettiva tesa ad assicurare che i dati siano trattati in un certo modo al fine di tutelare il soggetto interessato. La giurisprudenza della Corte di Giustizia dell'Unione europea ([77]) e della Corte europea dei diritti dell'Uomo ha aiutato a eliminare la confusione che si era creata attorno a questi due diversi concetti. Dal riconoscimento di questa distinzione, è nato il dibattito sulla natura del diritto alla protezione dei dati, in particolare se anche esso abbia rango costituzionale. La maggioranza della dottrina adotta una visione negativa ritendo gli articoli costituzionali a sostegno del diritto alla riservatezza non idonei per poter essere una base giuridica per la *data protection.* Sulla base di ciò, tale diritto si fonderebbe sulla normativa europea, acquisendo così esclusivamente rango legislativo e non costituzionale. Tuttavia, una parte

---

[76] COLAPIETRO, IANNUZZI, *I principi generali del trattamento dei dati personali e i diritti dell'interessato, Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679,* Napoli*,* 2017, p. 128-129*.*

[77] Sentenza della Corte (Grande Sezione) dell'8 aprile 2014. Digital Rights Ireland Ltd contro Minister for Communications, Marine and Natural Resources e a. e Kärntner Landesregierung e a. Cause riunite C-293/12 e C-594/12.
Sentenza della Corte (Grande Sezione) del 13 maggio 2014. Google Spain SL e Google Inc. contro Agencia Española de Protección de Datos (AEPD) e Mario Costeja González. Causa C-131/12.
Per maggiori informazioni si rimanda a POLLICINO, *Interpretazione o manipolazione? La Corte di giustizia definisce un nuovo diritto alla privacy digitale, Feredalismi.it, 2014.*

della dottrina minoritaria, considera che il diritto alla protezione dei dati personali sia dotato di rilevanza costituzionale. Anche in questo caso, a sostegno di questa tesi, vi è l'interpretazione evolutiva degli articoli 2, 13 e 21. Con l'innovazione tecnologica, ognuno di no è dotato di un "corpo elettronico" ([78]) formato da tutte le informazioni digitali che ci riguardano. Il controllo di suddetto corpo elettronico, secondo questa tesi, rientrerebbe nelle libertà dell'uomo e di conseguenza risulterebbe inviolabile. Sicuramente il diritto alla *data protection* trova fondamento nel diritto europeo e in quello nazionale, si parla a tal proposito di una configurazione multilivello. Per quanto riguarda invece il riferimento costituzionale, vi è ancora incertezza all'interno della dottrina.

La tutela del dato personale, potenzialmente capace di rilevare informazioni sensibili e private, è diventata molto più rilevante e delicata rispetto alla tutela della vita privata e a dimostrazione di tale importanza lo stesso Trattato sul Funzionamento dell'Unione europea, all'articolo 16, prevede che "ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano". Bisogna tuttavia riconoscere che tra gli utenti della rete, più in generale il cittadino, difetta di una consapevolezza reale dell'importanza dei propri dati che si traduca in congruenti comportamenti di autotutela: si tratta del cosiddetto "paradosso della privacy". Con questa espressione si intende il divario che sussiste tra le preoccupazioni che gli utenti della rete mostrano di possedere in materia di privacy/protezione dei dati e le loro condotte effettive all'interno della rete. La maggior parte dei soggetti che utilizzano internet ritiene che la *data protection* sia fondamentale e rilevante, ma analizzando i loro atteggiamenti si nota, in realtà, una diffusa superficialità, che si manifesta nella disinvoltura con i dati vengono condivisi con soggetti terzi non affidabili, che non garantiscono le dovute protezioni, ovvero nell'accettazione di qualsiasi tipologia di informativa. In molti casi, va detto, però l'utente viene ingannato dai titolari dei diversi trattamenti, che adottano strumenti poco sicuri e/o elaborano informative poco chiare. Molto spesso questo è dovuto al fatto che garantire misure di sicurezza adeguate ed elaborare informative e siti in modo chiaro e intuitivo richiede un costo in certi casi molto elevato, che non tutti i *provider* sono in grado di sostenere. Il Garante per la protezione dei dati personali, in questo contesto, svolge un ruolo fondamentale sanzionando i soggetti che non rispettano le normative vigenti e tutelando così gli utenti della rete. Il secondo capitolo di questo elaborato verterà sulla figura del Garante e sui

[78] RODOTÀ, *Intervista su privacy e libertà,* Roma-Bari, 2005, p. 119.

rimedi che il soggetto che ha subito una violazione del proprio diritto alla privacy può esperire per proteggersi.

CAPITOLO SECONDO

IL PERCORSO DI TUTELA NON GIURISDIZIONALE E IL RUOLO DEL GARANTE

2.1 Le disposizioni previste dal GDPR in caso di violazione

Il soggetto che subisce un trattamento illecito ha la possibilità di adottare due diversi percorsi di tutela, il percorso amministravo e il percorso giurisdizionale. In questo secondo capitolo verrà analizzato il percorso di tutela non giurisdizionale e la figura del Garante per la protezione dei dati personali (d'ora innanzi Garante e/o Autorità), che nel nostro ordinamento svolge un ruolo centrale. Al Capo VIII del GDPR sono previste le disposizioni che vengono applicate nei casi di trattamenti illeciti dei dati personali. Una prima disposizione fondamentale è quella contenuta nell'art. 77, ove si prevede la possibilità per l'interessato di presentare un reclamo al Garante. All'interessato viene riconosciuta la facoltà di scegliere l'Autorità Garante tra quelle eventualmente competenti dello Stato membro in cui egli lavora o risiede abitualmente oppure in cui si è verificata la violazione. In via generale, il soggetto legittimato a presentare il reclamo è colui che ha subito la violazione. Tuttavia, l'articolo 80 del GDPR prevede il diritto per l'interessato di *"*dare mandato a un organismo, un'organizzazione o un'associazione senza scopo di lucro*"* legalmente costituito in uno Stato membro, purché gli obbiettivi di tale ente abbiano ad oggetto un interesse pubblico e siano rivolti alla protezione dei diritti e delle libertà nel campo della *data protection*. Le norme appena richiamate permettono, ad esempio, a un soggetto che ha subito una violazione dei propri dati personali all'interno dell'Unione europea, ma che non è residente né lavora in uno Stato membro, di accedere agli strumenti di tutela previsti dal GDPR. Questo ampia notevolmente l'ambito di applicazione territoriale della tutela fornita mediante il reclamo al Garante.

Dopo l'avvio del procedimento, l'interessato dovrà essere informato dall'Autorità dello stato e dell'esito del reclamo e della sua facoltà di impugnare avanti al giudice il provvedimento del Garante. Il reclamo al Garante non è, comunque, l'unica possibilità di tutela offerta dinanzi alle violazioni delle norme sul trattamento dei dati personali: il GDPR prevede anche differenti strumenti, che verranno analizzati successivamente in questo elaborato.

2.2 Autorità amministrative Indipendenti: private e public enforcement

Il Garante per la protezione dei dati personali è un'Autorità amministrativa indipendente del nostro ordinamento. L'articolo 51 del GDPR prevede la possibilità per ogni Stato membro di poterne costituire o indicare diverse per *"*sorvegliare l'applicazione del presente regolamento al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento e di agevolare la libera circolazione dei dati personali all'interno dell'Unione*"*. Le Autorità amministrative indipendenti diventano sempre più rilevanti nell'attuazione delle disposizioni a tutela della *data protection* e dei soggetti che operano nel mercato e contribuiscono in modo concreto alla tutela dei diritti e delle libertà fondamentali degli individui. Inoltre, rappresentano una soluzione alternativa per la risoluzione di controversie tra privati rispetto alla tutela giurisdizionale civile. Le Autorità amministrative indipendenti sono enti pubblici preposti dalla legge alla regolazione, sorveglianza, controllo di determinati settori dell'economia e al raggiungimento di specifici interessi pubblici. Sono dotate di una competenza tecnica superiore rispetto alle altre pubbliche amministrazioni e sono appunto indipendenti dal potere esecutivo. Difatti, l'articolo 52 del GDPR stabilisce che *"*ogni autorità di controllo agisce in piena indipendenza nell'adempimento dei propri compiti e nell'esercizio dei propri poteri conformemente al presente regolamento*."* Inoltre, i membri delle autorità di controllo, nello svolgere i loro rispettivi compiti, non subiscono alcun tipo di "pressione esterna" e non possono *"*esercitare alcuna attività incompatibile*"* con quelle prevista dalla legge. Inoltre, possono esercitare le loro funzioni anche in relazione ai trattamenti di dati personali compiuti da enti pubblici o soggetti privati che agiscono per un interesse pubblico. La loro indipendenza rispetto al potere esecutivo si traduce in neutralità e terzietà rispetto agli interessi in gioco. In particolare, l'Autorità Garante "ha il dovere di assicurare il giusto equilibro tra i numerosi diritti ed interessi, individuali e collettivi, pubblici e privati, in tensione tra loro" ([79]).

All'interno del nostro sistema giuridico, oltre al Garante per la protezione dei dati personali, operano altre autorità con funzioni e poteri differenti. Una di queste è l'Autorità per le garanzie nelle comunicazioni (AGCOM) che tutela il diritto d'autore sulle reti di comunicazioni elettroniche e garantisce l'applicazione del Regolamento 2019/1150.

[79] F.B. ROMANO, *Le tutele dinanzi al Garante della privacy. Reclami, Segnalazioni e Sanzioni,* Pisa, 2022, pag. 34.

Importante è anche l'Autorità Garante della concorrenza e del mercato (AGCM) che opera per proteggere la concorrenza del mercato e tutelare i soggetti deboli da abusi di posizioni dominanti e da pratiche concorrenziali sleali. In via generale, i compiti che svolgono queste autorità possono essere raggruppati in tre categorie: interventi sanzionatori e ripristinatori, composizione di liti tra privati e funzioni di regolazione. È doveroso sottolineare che, nonostante venga loro demandata anche la risoluzione di controversie, le Autorità amministrative non sono giudici.

La Corte costituzionale è stata chiamata a pronunciarsi sulla natura di queste Autorità, per le quali ha escluso che si tratti di organi giurisdizionali, in ragione della *"*ontologica incompatibilità tra la posizione di giudice e di parte processuale nel giudizio avverso i propri provvedimenti*"* ([80]). Anche la Corte di giustizia ([81]), qualche anno prima, si era espressa in senso conforme, dichiarando che le Autorità amministrative, non essendo giudici, non possono compiere rinvii pregiudiziali alla Corte, in ragione del potere di avocazione esercitabile dalla Commissione UE. Di conseguenza, gli atti e i provvedimenti delle Autorità rispettano il regime proprio degli atti amministrativi e sono sempre soggetti al *"*controllo di un giudice*"* ([82]), con la conseguenza che a ciascuna delle due parti coinvolte nel conflitto attinente il trattamento dei dati personali la possibilità di *"*rivolgersi ad un giudice deve essere sempre garantita*"* ([83]).

2.3 Il Garante per la protezione dei dati personali (D.LGS 20/06/2003 N.196)

Il Garante per la protezione dei dati personali venne istituito dalla legge 31 dicembre 1996, n. 675, successivamente rifluita nel Codice Privacy, emanato con il decreto legislativo n. 196 del 30 giugno 2003. Nel 2018, il decreto legislativo n. 101/2018 ha modificato tale Codice, attualizzandone il contenuto rispetto alle disposizioni previste nel GDPR. L'autorità è un organo collegiale costituito da quattro membri nominati dal Parlamento, che rimangono in carica per un mandato di sette anni non rinnovabile. Il lavoro del Garante si esplica nella pubblicazione di atti di varia natura, come provvedimenti collegiali prescrittivi e/o sanzionatori, pareri, ordinanze aventi ad oggetto

[80] Corte costituzionale, sentenza n. 13, 31 gennaio 2019, punto 6.1 pag. 32. È possibile consultarla al seguente link: https://www.cortecostituzionale.it/actionSchedaPronuncia.do?anno=2019&numero=13.
[81] Corte di Giustizia UE, Epitropi Antagonismou v. Syfait, c-53/03, 31 maggio 2005. È possibile consultarla al seguente link: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:62003CJ0053.
[82] Articolo 113 della Costituzione Italiana.
[83] Articolo 24 della Costituzione Italiana.

l'obbligo per coloro cui siano state addebitate delle violazioni di conformarsi alle norme vigenti in materia. Può inoltre presentare segnalazioni all'autorità giudiziaria nel caso in cui venga a conoscenza di reati. In seguito all'emanazione del Decreto legislativo 101/2018, il sistema normativo in materia di *data protection* in Italia è divenuto più complesso rispetto al passato. La disciplina consta di due livelli, il primo dei quali è costituito dal Regolamento europeo (GDPR), che fonte di rango superiore rispetto al Codice italiano della Privacy ([84]). È compito del Garante e dell'autorità giudiziaria ordinaria applicare il GDPR ed interpretare le norme interne in maniera consonante, eventualmente disapplicando quelle che siano in contrasto con esso.

Il decreto legislativo 101/2018 è fortemente innovativo rispetto al decreto 196/2003, ma il procedimento che ha portato alla sua emanazione è stato particolarmente sofferto. L'idea iniziale era quella di abrogare l'intero vecchio Codice della Privacy, al fine di semplificare la disciplina del settore, ma alla fine è prevalso un approccio di modifica ed integrazione. Una prima novità ha riguardato l'abrogazione dell'articolo 2 ([85]) e l'emanazione di un nuovo articolo in cui si specifica che "il presente Codice reca disposizioni per l'adeguamento dell'ordinamento nazionale alle disposizioni del Regolamento". Questa nuova disposizione riprende sostanzialmente il titolo del decreto legislativo n. 101/2018. Il legislatore ha voluto riprendere il concetto per specificare, anche nel quadro del sistema normativo del Codice, che l'unica finalità del Codice è adeguare le disposizioni nazionali al GDPR. Lo scopo di questo nuovo articolo 2 è ricordare che" l'intera normativa italiana in materia di protezione dati si basa sulla competenza del legislatore italiano derivante dal GDPR e, di conseguenza, deve essere

---

[84] La gerarchia delle fonti è così costituita nel nostro ordinamento: Costituzione, fonti internazionali, fonti primarie del diritto (legge, decreti legge, decreti legislativi, referendum abrogativo, leggi regionali), fonti secondarie, usi e consuetudini. La fonte di rango superiore prevale su quella inferiore e la supremazia del diritto europeo rispetto le fonti primarie e secondarie del nostro ordinamento è riconosciuta a livello costituzionale sia dall'articolo 10 che stabilisce che "l'ordinamento giuridico italiano si conforma alle norme del diritto internazionale generalmente riconosciute" sia dall'articolo 11 che stabilisce che l'Italia "consente, in condizioni di parità con gli altri Stati, alle limitazioni di sovranità necessarie ad un ordinamento che assicuri la pace e la giustizia fra le nazioni".

[85] Articolo 2 Codice Privacy prima dell'entrata in vigore del GDPR: "*1. Il presente testo unico, di seguito denominato "codice", garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.*
2. Il trattamento dei dati personali è disciplinato assicurando un elevato livello di tutela dei diritti e delle libertà di cui al comma 1 nel rispetto dei principi di semplificazione, armonizzazione ed efficacia delle modalità previste per il loro esercizio da parte degli interessati, nonché per l'adempimento degli obblighi da parte dei titolari del trattamento".

interpretata e applicata alla luce del nuovo Regolamento europeo" ([86]). Si tratta di un concetto che può risultare ovvio ma molto spesso sono proprio gli aspetti più ovvi che vengono trascurati. Con il decreto legislativo 101/2018 sono stati aggiunti diversi articoli come l'articolo 2-undecies che risulta particolarmente rilevante in quanto limita l'esercizio dei diritti previsti nel GDPR dall'articoli 15 al 22. In particolare, suddetti diritti *"*non possono essere esercitati con richiesta al titolare del trattamento ovvero con reclamo ai sensi dell'articolo 77 del Regolamento qualora dall'esercizio di tali diritti possa derivare un pregiudizio effettivo e concreto su interessi*"* tutelati dalla legge. Il decreto ha inoltre introdotto la possibilità dell'interessato di avere il binario di tutela, amministrativa e giurisdizionale e ha rafforzato i poteri dell'Autorità.

2.3.1 Funzioni e poteri del Garante

Gli articoli 57 e successivi del GDPR definiscono i compiti e i poteri del Garante per la protezione dei dati personali. Uno dei primi compiti è, senza dubbio, la supervisione e l'assicurazione della corretta applicazione del regolamento, nonché la promozione della responsabilizzazione degli utenti riguardo ai rischi della rete, attraverso l'informazione sulle norme che disciplinano il trattamento dei dati personali, nonché sui diritti e sulle garanzie di cui godono gli utenti titolari dei dati. Promuove la *"*consapevolezza dei titolari del trattamento e dei responsabili del trattamento riguardo agli obblighi imposti loro dal presente regolamento.*"* Se richiesto, inoltre, informa l'interessato *"*in merito all'esercizio dei propri diritti*"*. Ulteriore compito fondamentale consiste nel trattare i reclami presentati da un *"*interessato, o da un organismo, un'organizzazione o un'associazione*"* e compie le opportune indagini per verificarne l'oggetto e la fondatezza. Al fine di garantire una corretta applicazione del Regolamento, il Garante collabora con le diverse Autorità di controllo per le violazioni che coinvolgono più Stati membri. Viste le sue competenze tecniche, il Garante è in grado di fornire consulenze ([87]) per trattamenti che hanno un elevato rischio di ledere i diritti e le libertà fondamentali degli utenti. Inoltre, è

---

[86] PIZZETTI, *Codice privacy italiano dopo il GDPR: come leggerlo e applicarlo ex decreto 101/2018, Agenda Digitale,* 2018. https://www.agendadigitale.eu/sicurezza/privacy/gdpr-pizzetti-i-consigli-per-leggere-e-applicare-bene-il-decreto-101-2018-dal-19-settembre/.

[87] Articolo 36 comma 1, GDPR, Consultazione preventiva: "*il titolare del trattamento, prima di procedere al trattamento, consulta l'autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 indiche che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio".*

tenuto a incoraggiare *"*l'elaborazione di codici di condotta, e fornire pareri su tali codici*"* e approvarli quando *"*forniscono garanzie sufficienti*"*.

L'articolo 58 del Regolamento conferisce al Garante poteri di indagine, correttivi, autorizzativi e consultivi, mentre l'articolo 83 disciplina il potere sanzionatore ovvero il potere di infliggere sanzioni di natura amministrativa pecuniaria. Il Garante è legittimato a richiedere al titolare del trattamento qualsiasi informazione al fine di poter esercitare i propri poteri d'indagine. Di fatto, può ottenere dal titolare del trattamento *"*l'accesso a tutti i dati personali e a tutte le informazioni necessarie per l'esecuzione dei suoi compiti*"*. I poteri correlativi, invece, riconoscono al Garante la possibilità di stabilire limitazioni, temporanee o definitive al trattamento oppure di ordinare la *"*rettifica, la cancellazione di dati personali*"*. Può inoltre ordinare al titolare del trattamento di *"*soddisfare le richieste dell'interessato di esercitare i diritti loro derivanti dal presente regolamento*"*.

I poteri autorizzativi e consultivi invece, sono legati a tutte quelle attività di consulenza e di autorizzazioni che sono previsti dall'articolo 57 del Regolamento, come la possibilità di rilasciare pareri, consulenze e autorizzazioni. Le disposizioni normative a livello europee vengono riprese, a livello nazionale, dal Codice della Privacy all'articolo 154. Dall'analisi di questi articoli, si può notare quanto ampi siano i poteri e i compiti del Garante e di conseguenza capire l'ampiezza del suo raggio d'azione. Sempre di più, risulta essere una figura forte e fondamentale per la tutela della *data protection.*

2.4 Rimedi in caso di violazione dei dati personali

I rimedi che possono essere esercitati da un soggetto che ha subito una violazione dei propri dati personali sono diversi. Il primo consiste nella possibilità di presentare un'istanza al titolare o al responsabile del trattamento per far valere i propri diritti previsti dagli articoli 15 e seguenti del GDPR, come i diritti di rettifica, di accesso e cancellazione. Il titolare che riceve un'istanza è tenuto a rispondere, senza ingiustificati ritardi, entro 30 giorni dal ricevimento della medesima. Sussiste però la possibilità di prorogare tale periodo di tempo di 60 giorni nel caso in cui il titolare abbia ricevuto un gran numero di istanze. Nel caso in cui, in seguito alla presentazione di un'istanza, il titolare non abbia risposto entro i termini previsti oppure il trattamento risulti ancora non conforme al GDPR, l'interessato può rivolgersi al Garante per la protezione dei dati personali mediante lo strumento del reclamo previsto dall'articolo 77 del GDPR. Subito dopo la presentazione del reclamo, il Garante avvia la fase istruttoria che, se si conclude con esito

positivo porta all'avvio di un procedimento amministrativo, il quale può portare all'adozione di uno dei provvedimenti previsti dall'articolo 58 del GDPR. Se l'interessato non è in grado di presentare un reclamo, può rivolgersi al Garante attraverso la segnalazione che risulta essere meno vincolante rispetto al reclamo in quanto, secondo l'articolo 144 del Codice della Privacy, *"*chiunque può rivolgere una segnalazione che il Garante può valutare ai fini dell'emanazione dei provvedimenti di cui all'articolo 58 del Regolamento*"*. L'articolo 79 del GDPR riconosce all'interessato la possibilità di impugnare il provvedimento dell'Autorità di fronte al giudice civile, mentre l'articolo 78 garantisce al soggetto interessato di adottare il percorso di tutela giurisdizionale attraverso un ricorso effettivo. Come detto in precedenza, l'introduzione delle autorità amministrative indipendenti ha permesso all'interessato di poter avere un doppio binario di tutela per far valere i propri diritti. Per quanto riguarda le violazioni dati personali il percorso di tutela amministrativa ha diversi vantaggi come la celerità nell'emanare il provvedimento, la gratuità nel presentare un reclamo e/o una segnalazione e la possibilità di giovarsi dei poteri ispettivi del Garante. Tuttavia, sono presenti anche alcuni svantaggi come l'impossibilità per l'Autorità amministrativa di condannare l'autore della violazione al risarcimento del danno e la possibilità di un'archiviazione ([88]) del reclamo presentato dall'interessato. Quest'ultimo svantaggio però non pregiudica la possibilità per l'interessato di presentare un ricorso all'autorità giudiziaria, dal momento che "tutti possono agire in giudizio per la tutela dei propri diritti e interessi legittimi" ([89]).

2.5 Il reclamo: il rimedio principale

La Direttiva del 95/46 ha introdotto un obbligo per gli Stati membri di istituire delle Autorità amministrative indipendenti dotate di poteri di controllo, obbligo che, come citato nel paragrafo 2.2 del medesimo capitolo, è stato ripreso dal GDPR all'interno

---

[88] Articolo 11 Delibera 1/2019, Chiusura dell'istruttoria preliminare: "*Al termine dell'istruttoria preliminare, il dipartimento, servizio o altra unità organizzativa competente può concludere l'esame archiviandolo, quando: a) la questione prospettata con il reclamo non risulta riconducibile alla protezione dei dati personali o ai compiti demandati al Garante; b) non sono ravvisati, allo stato degli atti, gli estremi di una violazione della disciplina rilevante in materia di protezione dei dati personali; c) si tratta di una richiesta eccessiva, in particolare per il carattere pretestuoso o ripetitivo anche ai sensi dell'articolo 57, paragrafo 4, del GDPR*; *d) la questione prospettata con il reclamo è stata già esaminata dall'Autorità, in particolare con un provvedimento collegiale di carattere generale, o può essere esaminata richiamando provvedimenti o questioni già affrontate dal Garante ovvero esprimendo un prudente avviso su questioni che non presentano particolare rilevanza sul piano generale. 2. Nei casi di cui al comma 1 del presente articolo è fornito all'istante un riscontro indicando succintamente le ragioni per le quali, ai sensi del medesimo comma, non è promossa l'adozione di un provvedimento del Collegio*".

[89] Articolo 24 Costituzione Italiana.

dell'articolo 51. Tuttavia, la Direttiva non prevedeva in modo formale un diritto al reclamo, ma lasciava discrezionalità agli Stati membri nella scelta del miglior strumento di garanzia per la protezione dei dati personali. Nel nostro ordinamento, la legge n. 675 del 1996, all'interno dell'articolo 30, ha introdotto la figura del Garante per la protezione dei dati personali e la possibilità per l'interessato di far valere i propri diritti "dinanzi all'autorità giudiziaria o con ricorso al Garante" ([90]). Da qui si può vedere che la legge n.675 ha introdotto un primo strumento di tutela amministrativa, il ricorso, che l'interessato poteva esercitare, in alternativa al ricorso giurisdizionale, quando riteneva di aver subito una violazione dei diritti legati al trattamento e previsti dalla legge stessa ([91]). La legge, tuttavia, individuò solamente il ricorso come strumento di tutela per l'interessato, bisognerà attendere l'entrata in vigore del Codice in materia di protezione dei dati personali, attraverso il decreto legislativo n. 196 del 30 giugno 2003, il quale ha abrogato la legge n. 675/1996 e ha ampliato i rimedi a protezione del soggetto interessato. Analizzando l'articolo 141 ([92]) del Codice si può vedere come il legislatore abbia aggiunto

---

[90] Articolo 29 della Legge 31 dicembre 1996 n. 675, *Tutela.*

[91] Articolo 13 della Legge 31 dicembre 1996 n. 675, *Diritti dell'interessato: "1. In relazione al trattamento di dati personali l'interessato ha diritto: a) di conoscere, mediante accesso gratuito al registro di cui all'articolo 31, comma 1, lettera a), l'esistenza di trattamenti di dati che possono riguardarlo;*
b) di essere informato su quanto indicato all'articolo 7, comma 4, lettere a), b) e h); c) di ottenere, a cura del titolare o del responsabile, senza ritardo: 1) la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la comunicazione in forma intelligibile dei medesimi dati e della loro origine, nonché della logica e delle finalità su cui si basa il trattamento; la richiesta può essere rinnovata, salva l'esistenza di giustificati motivi, con intervallo non minore di novanta giorni; 2) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati; 3) l'aggiornamento, la rettificazione ovvero, qualora vi abbia interesse, l'integrazione dei dati; 4) l'attestazione che le operazioni di cui ai numeri 2) e 3) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si riveli impossibile o comporti un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato; d) di opporsi, in tutto o in parte, per motivi legittimi, al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta; e) di opporsi, in tutto o in parte, al trattamento di dati personali che lo riguardano, previsto a fini di informazione commerciale o di invio di materiale pubblicitario o di vendita diretta ovvero per il compimento di ricerche di mercato o di comunicazione commerciale interattiva e di essere informato dal titolare, non oltre il momento in cui i dati sono comunicati o diffusi, della possibilità di esercitare gratuitamente tale diritto".

[92] Articolo 141 Codice della Privacy prima della modifica del D.lgs. n 101/2018: "*L'interessato può rivolgersi al Garante: a) mediante reclamo circostanziato nei modi previsti dall'articolo 142, per rappresentare una violazione della disciplina rilevante in materia di trattamento di dati personali; b) mediante segnalazione, se non è possibile presentare un reclamo circostanziato ai sensi della lettera a), al fine di sollecitare un controllo da parte del Garante sulla disciplina medesima; c) mediante ricorso, se intende far valere gli specifici diritti di cui all'articolo 7 secondo le modalità e per conseguire gli effetti previsti nella sezione III del presente capo*".

due diversi rimedi: il reclamo e la segnalazione. Rappresentavano strumenti di denuncia informali, mentre il ricorso aveva un carattere, per così dire, più formale. Come evidenziato nel primo capitolo, nel 2016 è stato approvato il General Data Protection Regolament, il quale a differenza della Direttiva ha introdotto, nell'articolo 77, il *"*diritto di proporre un reclamo", eliminando così la discrezionalità che la Direttiva aveva riconosciuto. *"*Tutti i principali aspetti sostanziali del reclamo sono ora disciplinati dal diritto all'Unione, mentre gli Stati, nel dare esecuzione al GDPR, hanno il compito di stabilire regole procedurali che forniscano garanzie adeguate*"* ([93]).

Con il D.lgs. 101/ 2018 però, il Codice Privacy ha subito ulteriori modifiche, in particolare, è stato abrogato il ricorso, configurando così il reclamo e le segnalazioni come unici strumenti di tutela amministrativa. L'articolo 141 ora prevede il diritto dell'interessato di "rivolgersi al Garante mediante reclamo ai sensi dell'articolo 77 del Regolamento", mentre l'articolo 140 bis ne prevede l'alternatività con il ricorso al giudice stabilendo che "il reclamo al Garante non può essere proposto se, per il medesimo oggetto e tra le stesse parti, è stata già adita l'autorità giudiziaria". La natura amministrativa del reclamo rende obbligatorio l'applicazione dell'articolo 41 della Carta dei Diritti Fondamentali dell'Unione Europea quale stabilisce che "ogni persona ha diritto a che le questioni che la riguardano siano trattate in modo imparziale ed equo ed entro un termine ragionevole dalle istituzioni, organi e organismi dell'Unione*"*.

2.5.1 La fase introduttiva del reclamo

Vista la discrezionalità riconosciuta agli Stati membri nell'individuare le regole procedimentali del reclamo, all'interno del nostro ordinamento, gli articoli 142 e 143 del Codice della Privacy disciplinano il reclamo. Si tratta di un insieme di regole "minimaliste" per rendere il più lineare possibile il procedimento, lasciando un certo margine di flessibilità all'Autorità Garante. Sotto il profilo della semplificazione, la presentazione del reclamo avviene mediante l'utilizzo di fascicoli elettronici, che rendono molto più agevole e celere il deposito degli atti. Con riguardo, invece, allo spazio di autonomia riservato all'Autorità indipendente, va rilevato che l'ultimo comma dell'articolo 142 attribuisce al Garante la possibilità di disciplinare "con proprio regolamento il procedimento relativo all'esame dei reclami." Di fatto, il 4 aprile 2019 il

[93] ROMANO, *Le tutele dinanzi al Garante della privacy. Reclami, Segnalazioni e Sanzioni,* Pisa, 2022, p. 27.

Garante ha emanato il Regolamento n. 1/2019 per aggiornare le procedure interne in seguito all'entrata in vigore del GDPR.

La legittimazione attiva spetta al soggetto interessato, che ritiene di aver subito un trattamento illecito; secondo il comma secondo dell'articolo 142, è però possibile che egli conferisca mandato ad "un ente del terzo settore che sia attivo nel settore della tutela dei diritti e delle libertà degli interessati". La legittimazione passiva invece ricade sul titolare o sul responsabile del trattamento. Proseguendo con l'analisi dell'articolo 142, è possibile capire quali siano i requisiti sostanziali e formali che il reclamo deve possedere. In particolare, esso deve contenere "gli estremi identificativi del titolare o del responsabile del trattamento, ove conosciuto" e il reclamante deve illustrare i fatti, le circostanze e le disposizioni che ritiene essere state violate nel modo più dettagliato possibile. Il reclamo non si può limitare ad una semplice denuncia, ma deve essere analitico per permettere al titolare del trattamento di presentare le sue difese. Nel caso in cui il reclamo sia incompleto o risulti impreciso, secondo quanto previsto dal Regolamento 1/2019, l'Autorità Garante può richiedere al reclamante di integrare l'atto introduttivo entro 15 giorni: la mancata regolarizzazione porta all'archiviazione del reclamo.

Per quanto riguarda le modalità di deposito del reclamo, il Codice Privacy non prevede particolari formalità. Presso il sito internet ([94]) dell'Autorità Garante, oltre a poter presentare un reclamo oppure una segnalazione, è possibile anche informarsi su quelle che sono le modalità per presentare tali atti.

Si è già evidenziato come il GDPR, all'articolo 77, preveda due diversi criteri alternativi per l'individuazione dell'Autorità competente, potendo il soggetto interessato presentare reclamo "nello Stato membro in cui lavora o risiede abitualmente oppure nello Stato in cui si è verificata la violazione". Il primo criterio tutela la parte debole del rapporto, cioè l'interessato che subisce l'illecito trattamento, mentre il secondo riguarda il luogo in cui l'evento dannoso si è verificato o potrebbe verificarsi. Più complicata è l'individuazione dell'Autorità nel caso di trattamenti che coinvolgono più Stati membri ovvero Stati

[94] È possibile visionare il sito internet presso questo indirizzo: https://www.garanteprivacy.it/. I reclami e le segnalazioni devono essere inviati mediante raccomandata oppure PEC sottoscritti con firma autenticata del reclamante. Il sito, inoltre, contiene collegamenti ipertestuali al GDPR e al Codice Privacy e grazie alla sua newsletter, permette ad un soggetto di rimanere costantemente aggiornato sulla normativa in materia di privacy.

dell'Unione e Stati extraeuropei. In tale circostanza il GDPR, nell'articolo 60 ([95]) ha previsto il cosiddetto "sportello unico", formato da tutte le Autorità interessate più un'Autorità detta capofila ([96]) il quale "coopera con le altre autorità di controllo per raggiungere un consenso" circa la gestione del procedimento. Nel caso in cui le diverse Autorità non riescano a trovare un accordo, secondo quanto riportato dall'articolo 68 ([97]) del GDPR, la decisione viene affidata al Comitato europeo per la protezione dei dati. Una volta presentato il reclamo, l'Autorità Garante avvia la fase istruttoria per verificarne l'ammissibilità.

2.5.2 La fase istruttoria del reclamo

Nella disciplina delle fasi istruttoria e decisoria il GDPR ha lasciato ampia discrezionalità agli Stati membri. Secondo quanto stabilito dal comma 4 dell'articolo 58 "l'esercizio da parte di un'autorità di controllo dei poteri è soggetto a garanzie adeguate", riconosciute a entrambe le parti coinvolte. All'interno del Codice Privacy, l'articolo che disciplina la fase istruttoria è il 143, nel quale si nota come questa venga preceduta da un'istruttoria preliminare, nel corso della quale l'Autorità Garante verifica la fondatezza dell'istanza e la presenza dei presupposti per l'adozione del provvedimento finale che consistono nella competenza dell'Autorità, la legittimazione nell'istanze, l'interesse e la presenza dei requisiti formali del reclamo. Durante la fase istruttoria viene svolto un attento esame dei fatti rappresentati dal reclamante: l'Autorità procede naturalmente all'acquisizione dei documenti allegati al reclamo. Il Cod. Privacy, agli articoli 157 ([98]) e seguenti, prevede,

---

[95] Per maggior informazioni sul procedimento di cooperazione tra le diverse autorità di controllo si richiama l'articolo 60 del GDPR.

[96] Secondo l'articolo 56 del GDPR salvo deroghe, "l'autorità di controllo dello stabilimento principale o dello stabilimento unico del titolare e del trattamento o responsabile del trattamento è competente ad agire in qualità di autorità di controllo capofila per i trattamenti transfrontalieri.

[97] Articolo 68 GDPR*: "1. Il comitato europeo per la protezione dei dati («comitato») è istituito quale organismo dell'Unione ed è dotato di personalità giuridica. 2. Il comitato è rappresentato dal suo presidente. 3. Il comitato è composto dalla figura di vertice di un'autorità di controllo per ciascuno Stato membro e dal garante europeo della protezione dei dati, o dai rispettivi rappresentanti. 4. Qualora, in uno Stato membro, più autorità di controllo siano incaricate di sorvegliare l'applicazione delle disposizioni del presente regolamento, è designato un rappresentante comune conformemente al diritto di tale Stato membro. 5. La Commissione ha il diritto di partecipare alle attività e alle riunioni del comitato senza diritto di voto. La Commissione designa un rappresentante. Il presidente del comitato comunica alla Commissione le attività del comitato. 6. Nei casi di cui all'articolo 65, il garante europeo della protezione dei dati ha diritto di voto solo per decisioni che riguardano principi e norme applicabili a istituzioni, organi, uffici e agenzie dell'Unione che corrispondono nella sostanza a quelli del presente regolamento"*.

[98] Articolo 157 Codice Privacy, *Richiesta di informazioni e di esibizioni di documenti*: *"1. Nell'ambito dei poteri di cui all'articolo 58 del Regolamento, e per l'espletamento dei propri compiti, il Garante può richiedere al titolare, al responsabile, al rappresentante del titolare o del responsabile, all'interessato o*

innanzitutto, il potere dell'Autorità di adottare "la richiesta di informazione e di esibizione di documenti" ([99]). Il destinatario degli ordini in parola dev'essere una persona fisica identificata, che si espone a sanzioni in caso di inottemperanza. Secondo l'articolo 168 Cod. Privacy, infatti, "chiunque, in un procedimento o nel corso di accertamenti dinanzi al Garante, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi, è punito con la reclusione da sei mesi a tre anni". Inoltre, ai sensi dell'art. 166 Cod. Privacy, la mancata risposta alle richieste del Garante costituisce un illecito amministrativo ([100]). L'esercizio dei mezzi istruttori può avvenire solo se sono state applicate le "garanzie adeguate" previste dall'articolo 58 del GDPR. In particolare, il Garante può richiedere informazioni se queste sono strettamente legate all'oggetto del reclamo. Durante l'esame del reclamo il Garante inoltre, "può disporre di accessi a banche di dati, archivi o altre ispezioni e verifiche nei luoghi ove si svolge il trattamento o nei quali occorre effettuare rilevazioni comunque utili al controllo del rispetto della disciplina in materia di trattamento dei dati personali." ([101]) L'accertamento di fatti mediante ispezioni e verifiche può essere fatto di sorpresa oppure mediante un preavviso e può svolgersi anche attraverso la collaborazione con altri organi dello Stato. Se gli accertamenti devono essere svolti all'interno di una abitazione l'articolo 158 richiede "l'assenso informato" del titolare o del responsabile del trattamento. In caso di mancato consenso del titolare, l'Autorità deve essere autorizzata dal "presidente del tribunale

---

anche a terzi di fornire informazioni e di esibire documenti anche con riferimento al contenuto di banche di dati".

[99] La richiesta d'informazioni è "un'attività volta a verificare che i dati personali di cui l'organizzazione è in possesso, siano trattati secondo quanto previsto dal Regolamento Europeo 2016/679 (GDPR). Quello che viene richiesto al titolare in sede ispettiva è comprovare l'accountability, ovvero l'attuazione di misure tecniche e organizzative opportune, efficaci e adeguate per la salvaguardia dei dati personali". NUCARA, *Ispezione privacy: regole fondamentali per affrontare un controllo della GdF (e dell'Autorità Garante), Cybersecurity360,* 2020. https://www.cybersecurity360.it/legal/privacy-dati-personali/ispezione-privacy-regole-fondamentali-per-affrontare-un-controllo-della-gdf-e-dellautorita-garante/.
Inoltre, l'autorità di controllo può "richiedere ad ogni player dell'ecosistema privacy di esibire documenti anche con riferimenti al contenuto di banche dati". ALVERONE, *Norme procedurali privacy: il procedimento dinanzi al Garante per l'adozione di provvedimenti correttivi e sanzionatori, Diritto.it,* 2022. https://www.diritto.it/norme-procedurali-privacy-il-procedimento-dinanzi-al-garante-per-ladozione-di-provvedimenti-correttivi-e-sanzionatori/.
Essendo un'autorità amministrativa indipendente e dotata di ampie competenze, il Garante è legittimato a adottare questi strumenti sulla sola base dell'articolo 58 del GDPR e dell'articolo 157 del Codice Privacy. Queste due basi giuridiche sono sufficienti a garantire la legittimità dell'attività di ispezione e di esibizione.

[100] L' Articolo 166 comma 2 del Codice Privacy richiama l'articolo 83 paragrafo 5 del GDPR, dove è stabilito che per questo tipo di violazione, si può subire una sanzione amministrativa pecuniaria fino a 20.000.000 EUR, o per le imprese, fino al 4% del fatturato annuo dell'esercizio precedente, se superiore.

[101] Articolo 158 Codice Privacy "*Accertamenti*".

competente per territorio" mediante un decreto motivato. È possibile notare la presenza di alcune differenze rispetto a quanto viene stabilito per l'ordine d'ispezione di persone e di cose disciplinato dall'articolo 118 del Codice di procedura civile. All'interno dell'articolo si può vedere che l'ispezione, richiesta dal giudice durante un processo civile, deve essere rivolta a "fatti che appaiono indispensabili per conoscere i fatti della causa, purché ciò possa compiersi senza grave danno per la parte o per il terzo". Inoltre, se la parte o il terzo si rifiutano di sottoporsi all'ordine di ispezioni, il giudice può sanzionarli e "desumere argomenti di prova". Da queste differenze, si potrebbe dedurre che l'ispezione effettuata dal Garante risulti essere meno vincolata rispetto l'ispezione richiesta dal giudice civile sulla base dell'articolo 118. Rimangono comunque strumenti differenti che vengono applicati in contesti diversi. Di fatti l'articolo 158 del Codice Privacy è specificatamente volto a regolamentare la protezione dei dati personali in conformità con il GDPR.

È stato visto come il Decreto 101/2018 abbia modificato il Cod. Privacy andando, in particolare ad ampliare i poteri dell'Autorità e le garanzie a tutela di coloro che ne subiscono l'esercizio. Una delle maggiori novità introdotte è la possibilità per il Garante di emanare dei provvedimenti d'urgenza. Quando viene presentato un reclamo, l'emanazione del provvedimento finale non è istantanea, in quanto il Garante necessita di tempo per poter acquisire tutte le informazioni necessarie e durante questo intervallo i diritti del soggetto interessato hanno spesso necessità di essere protetti. Sull'importanza dei provvedimenti d'urgenza in seno al procedimento dinanzi all'Autorità si tornerà più avanti quando analizzeremo il Caso ChatGPT, in cui il Garante ha interrotto il trattamento dei dati di utenti italiani prima della conclusione della fase istruttoria. Lo stesso articolo 58 del GDPR prevede in effetti, come potere correttivo, la possibilità di "imporre una limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento." Successivamente all'acquisizione delle informazioni rilevanti e all'esame delle stesse, si può ritenere conclusa la fase istruttoria e il Garante può emanare il provvedimento a chiusura del procedimento, che può contenere prescrizioni rivolte al titolare e al responsabile del trattamento oppure dimostrare la mancata violazione della normativa da parte di questi soggetti. Sulla base di quanto stabilito dal Codice Privacy e dal GDPR, i provvedimenti del Garante per la protezione dei dati non hanno efficacia erga omnes ma sono specifici e hanno valore solamente nei confronti dei soggetti coinvolti all'interno del trattamento.

2.5.3 La fase decisoria del reclamo

Il Garante, grazie alla potestà di autoregolamentazione riconosciutagli dal legislatore europeo, ha previsto delle procedure molto articolate per la fase conclusiva del procedimento. Sia il GDPR sia il Codice Privacy sono particolarmente laconici ([102]) sul punto: di qui la pregnanza del Regolamento 1/2019, adottato dal Garante per dettagliare e integrare, ove opportuno, la disciplina della procedure avanti ad esso avviate. La fase decisoria del procedimento può portare all'emanazione di un provvedimento che permette l'esercizio dei poteri correttivi ([103]) e sanzionatori da parte dell'Autorità. Nel caso in cui il procedimento si concluda con una sanzione nei confronti del titolare del trattamento, il Garante è tenuto a informare quest'ultimo dei motivi fondativi della sanzione. Il provvedimento finale, così come per l'archiviazione, viene adottato attraverso una deliberazione motivata del Collegio che viene notificata sia al titolare del trattamento sia al reclamante.

Tuttavia, un reclamo può avere come oggetto la violazione dei diritti previsti dagli articoli 15 a 22 ([104]) del GDPR. In questo caso, il reclamante chiede al Garante di "accogliere una richiesta non soddisfatta dal titolare del trattamento" ([105]). In questo modo, il Garante

---

[102] Si richiama l'articolo 143 del Codice Privacy e l'articolo 77 del GDPR per maggiori chiarimenti.

[103] L'articolo 58 comma 2 del GDPR stabilisce che: "*Ogni autorità di controllo ha tutti i poteri correttivi seguenti: a) rivolgere avvertimenti al titolare del trattamento o al responsabile del trattamento sul fatto che i trattamenti previsti possono verosimilmente violare le disposizioni del presente regolamento; b) rivolgere ammonimenti al titolare e del trattamento o al responsabile del trattamento ove i trattamenti abbiano violato le disposizioni del presente regolamento; c) ingiungere al titolare del trattamento o al responsabile del trattamento di soddisfare le richieste dell'interessato di esercitare i diritti loro derivanti dal presente regolamento;* d) ingiungere al titolare del trattamento o al responsabile del trattamento di conformare i trattamenti alle disposizioni del presente regolamento, se del caso, in una determinata maniera ed entro un determinato termine; e) ingiungere al titolare del trattamento di comunicare all'interessato una violazione dei dati personali; f) imporre una limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento; g) ordinare la rettifica, la cancellazione di dati personali o la limitazione del trattamento a norma degli articoli 16, 17 e 18 e la notificazione di tali misure ai destinatari cui sono stati comunicati i dati personali ai sensi dell'articolo 17, paragrafo 2, e dell'articolo 19; h) revocare la certificazione o ingiungere all'organismo di certificazione di ritirare la certificazione rilasciata a norma degli articoli 42 e 43, oppure ingiungere all'organismo di certificazione di non rilasciare la certificazione se i requisiti per la certificazione non sono o non sono più soddisfatti; i) infliggere una sanzione amministrativa pecuniaria ai sensi dell'articolo 83, in aggiunta alle misure di cui al presente paragrafo, o in luogo di tali misure, in funzione delle circostanze di ogni singolo caso; e j) ordinare la sospensione dei flussi di dati verso un destinatario in un paese terzo o un'organizzazione internazionale".

[104] I diritti che gli articoli 15 a 22 del GDPR sono i seguenti: Diritto di accesso dell'interessato, Diritto di rettifica, Diritto alla cancellazione, Diritto di limitazione di trattamento, Diritto alla portabilità dei dati, Diritto di opposizione, diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato. Per maggiori informazioni si richiama il suddetto Regolamento consultabile al seguente link: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32016R0679.

[105] ROMANO, *Le tutele dinanzi al Garante della privacy. Reclami, Segnalazioni e Sanzioni,* Pisa, 2022, p. 81.

svolge essenzialmente "la funzione di dirimere una controversia tra l'interessato ed il titolare, adottando provvedimenti ove non raggiunga una definizione bonaria della questione tra le parti" ([106]). L'articolo 15 del Regolamento 1/2019 disciplina questa tipologia di provvedimento stabilendo che la prima fase del procedimento è il cosiddetto "interpello preventivo". Fase necessaria per verificare che il reclamante abbia effettivamente fatto valere i propri diritti, ma il responsabile o titolare del trattamento non ha accolto suddetto richiesta. Una volta riscontrato questo scenario, viene valutata l'ammissibilità e la fondatezza del reclamo. Se si ottiene un risultato positivo, il Garante andrà ad inoltrare la richiesta del reclamante, entro 20 giorni, al titolare e/o responsabile del trattamento. Da questo punto in poi la normativa può causare confusione poiché, anche se il titolare del trattamento aderisce volontariamente alla richiesta, l'Autorità avvia automaticamente un procedimento sanzionatorio. Questa procedura potrebbe sembrare inefficiente, poiché il ruolo principale del Garante in questi casi è risolvere dispute, e se ciò è già avvenuto con l'accettazione volontaria, l'avvio del procedimento potrebbe non avere senso. Inoltre, tale procedura si limiterebbe all'accertamento da parte dell'Autorità dell'accettazione della richiesta del titolare e non comporterebbe l'esercizio di poteri correttivi da parte del Garante.

Tuttavia, si possono verificare alcuni casi di archiviazione del reclamo, che chiudono il procedimento in maniera non satisfattiva per l'istante. L'archiviazione ([107]) può essere disposta subito dopo la conclusione della fase istruttoria preliminare con decisione motivata. L'articolo 11 del Regolamento 1/2019 prevede quattro diversi ipotesi. La prima è nel caso in cui "la questione prospettata con il reclamo non risulta riconducibile alla protezione dei dati personali o ai compiti demandati al Garante". Questo significa che l'Autorità non possiede la competenza per poter gestire detta questione e non può quindi emanare alcun provvedimento. Seconda ipotesi è quando "non sono ravvisati gli estremi di una violazione della disciplina rilevante in materia di protezione dei dati personali" e quindi il reclamo risulta infondato. Terzo caso è rappresentato da "una richiesta eccessiva, in particolare per il carattere pretestuoso o ripetitivo anche ai sensi dell'art. 57, paragrafo

[106] *Op.ult.cit.*

[107] Secondo l'articolo 14 del Regolamento 1/2019, l'archiviazione può avvenire anche dopo la conclusione della fase istruttoria. Per maggiori chiarimenti si richiama il medesimo articolo.

4, del GDPR". Infine, l'archiviazione può essere disposta quando "la questione prospettata con il reclamo è stata già esaminata dall'Autorità".

In precedenza, è stato evidenziato come il reclamante debba essere preciso e analitico nell'allegazione dei fatti rilevanti. Quest'onere consente al Garante di valutare in modo immediato se proseguire con il procedimento oppure archiviare l'istanza dell'interessato. Se il reclamo è vago e non circostanziato rischia di incorrere nell'archiviazione.

Va detto che il Garante, nel proprio sito istituzionale, mette a disposizione moduli fac-simile e precise istruzioni per la stesura del reclamo, oltre che informative di ampio raggio per far sì che gli utenti del web siano più consapevole dei pericoli che possono derivare da uno scorretto utilizzo della rete.

L'articolo 12 del Regolamento 1/2019 si occupa della fase introduttiva del procedimento. Il Garante è tenuto a comunicare al titolare del trattamento l'avvio del procedimento fornendo una "sintetica descrizione dei fatti e delle presunte violazione della disciplina rilevante in materia di protezione dei dati personali, l'indicazione dell'unità organizzativa competente presso la quale può essere presa visione ed estratta copia degli atti, l'indicazione che entro trenta giorni dal ricevimento della comunicazione è possibile inviare al Garante scritti difensivi o documenti e chiedere di essere sentito dalla medesima Autorità". ([108])

In riferimento ai termini per la conclusione del procedimento, l'articolo 77 del GDPR prevede che il reclamante venga informato dell'esito e dello stato del procedimento "entro un termine ragionevole". Il legislatore italiano ha interpretato suddetto articolo, stabilendo, nell' articolo 143 del Codice Privacy, un termine ([109]) di nove mesi per l'adozione del provvedimento, con possibilità di proroghe nel caso di particolari esigenze istruttorie motivate.

2.6 Le segnalazioni al Garante

Ulteriore strumento che si può utilizzare al fine di denunciare una violazione al Garante per la protezione dei dati personali è la segnalazione. Si tratta di un rimedio di natura informale, che si distingue dal reclamo, permettendo a chiunque di presentare un fatto

[108] Articolo 12 comma 2 Regolamento 1/2019.
[109] Si evidenza che in caso di attuazione del sistema di cooperazione tra diverse Autorità Garanti previsto dall'articolo 60 del GDPR, il termine viene prorogato fino alla conclusione della cooperazione.

lesivo della riservatezza all'Autorità. È doveroso precisare che la segnalazione non è contemplata dal diritto dell'Unione europea (né dalla Direttiva 95/46 né dal GDPR), pur se la funzione di sorveglianza attribuita al Garante secondo l'articolo 57 del GDPR include "anche il potere di ricevere esposti, denunce, o notizie informali relative a presunte violazione" ([110]). La segnalazione è una novità introdotta con il D.lgs. 196/2003, e prima della riforma del 2018, veniva considerata come uno strumento accessibile principalmente dall'interessato nel caso in cui non fosse in grado di presentare un reclamo. Difatti il previgente articolo 141 del Codice Privacy riconosceva all'interessato questa possibilità, se non possedeva sufficienti informazioni per proporre un reclamo circostanziato. In seguito all'entrata in vigore del D.lgs. 101/2018, la facoltà di segnalazione è stata estesa a chiunque voglia denunciare una presunta violazione della normativa in materia di protezione dei dati, anche a chi non ha subito direttamente il trattamento illecito. Ora, nel nuovo Codice Privacy, l'articolo che disciplina la segnalazione è il 144 ([111]): lo scopo principale di tale previsione, in comune con il reclamo, è fare in modo che il Garante eserciti i propri poteri per censurare la violazione denunciata. Nonostante la presenza del cit. articolo, il Codice non fornisce tuttavia una definizione di segnalazione, sicché il Garante, in virtù della propria autonomia di Autorità indipendente, è intervenuto con regolamento. Così, secondo l'articolo 19 del Regolamento 1/2019 "sono qualificabili come segnalazioni gli atti, diversi dalle richieste di parere e dai quesiti, che non presentano le caratteristiche del reclamo e sono volti a sollecitare un controllo da parte del Garante sulla disciplina rilevante in materia di trattamento dei dati personali." La segnalazione deve essere presentata da un soggetto identificato, salvo eccezioni ([112]) previste dal medesimo articolo. Il segnalante non possiede gli stessi diritti del reclamante: il Garante non è tenuto a rispettare alcun obbligo informativo nei suoi riguardi e nemmeno ad avviare un procedimento dopo aver ricevuto la segnalazione.

---

[110] ROMANO, *Le tutele dinanzi al Garante della privacy. Reclami, Segnalazioni e Sanzioni,* Pisa, 2022, p. 93.

[111] Articolo 144 Codice Privacy: "*Chiunque può rivolgere una segnalazione che il Garante può valutare anche ai fini dell'emanazione dei provvedimenti di cui all'articolo 58 del Regolamento. 2. I provvedimenti del Garante di cui all'articolo 58 del Regolamento possono essere adottati anche d'ufficio*".

[112] Articolo 19 Regolamento 1/2019 del Garante per la protezione dei dati personali: "*L'Autorità può utilizzare le notizie indicate in eventuali segnalazioni che provengono da un soggetto non identificato, qualora ritenga di dover avviare controlli su casi nei quali ravvisa il rischio di seri pregiudizi o di ritorsioni ai danni di soggetti interessati dal trattamento, oppure ricorre comunque un caso di particolare gravità*".

2.7 Le sanzioni del Garante

L'utilizzo di sanzioni amministrative per punire le violazioni di norme comunitarie non è di certo recente. Il tema venne affrontato dalla Corte di Giustizia nel 1989 ([113]) e, in Italia, discusso anche da autorevole dottrina a partire dal 1994 ([114]). La Direttiva 95/46 prevedeva una prima disciplina in materia di sanzioni nell'articolo 24, dove veniva stabilito che "gli Stati membri adottano le misure appropriate per garantire la piena applicazione della presente direttiva". Si trattava di un vincolo molto generale, che riconosceva agli Stati membri ampia discrezionalità e che diede luogo ad un sistema sanzionatorio assai frammentato. Tra i motivi che portarono all'adozione del GDPR vi era in effetti anche la necessità di istituire un quadro normativo uniforme e armonizzato in materia di sanzioni. Il GDPR però non si è limitato a stabilire un sistema sanzionatorio comune, ma ha riconosciuto ([115]) alle sole Autorità amministrative indipendenti la facoltà di adottare i provvedimenti a tal fine previsti. Evidentemente, tali istituzioni sono state ritenute le uniche in grado di garantire la competenza tecnica e la neutralità decisoria doverose per esercitare in maniera adeguata le funzioni di controllo in parola.

In base a quanto affermato nel Considerando n. 129 del GDPR, le Autorità devono esercitare i poteri loro attribuiti in modo "imparziale, equo ed entro un termine ragionale"; inoltre, nei relativi procedimenti deve sempre essere rispettato il principio di proporzionalità ([116]). La possibilità di emanare sanzioni nei confronti di soggetti trasgressori rientra tra i poteri correttivi previsti dall'articolo 58 del GDPR, il quale sottopone l'esercizio di tali poteri a garanzie procedurali adeguate. La funzione principale delle sanzioni è sicuramente quella di rendere maggiormente effettiva la normativa nel

---

[113] Corte di Giustizia, Sentenza 21 settembre 1989, causa 68/88.

[114] Si richiama l'attenzione all' intervento di G. GRASSO, *Nuove prospettive in tema di sanzioni amministrative comunitarie, Rivista trimestrale diritto pubblico, 1994, p. 870 e ss.*

[115] In particolare, l'articolo 58 del GDPR riconosce all'Autorità poteri d'indagine, correttivi, autorizzativi e consultivi.

[116] Il principio di proporzionalità è illustrato nell'articolo 5, paragrafo 4, del trattato sull'Unione europea. Esso mira a inquadrare le azioni delle istituzioni dell'Unione europea (Unione) entro certi limiti.
In virtù di tale principio, le misure dell'Unione: devono essere idonee a conseguire il fine desiderato, devono essere necessarie per conseguire il fine desiderato, e non devono imporre alle persone un onere eccessivo rispetto all'obiettivo che si intende raggiungere (proporzionalità in senso stretto). Il principio di proporzionalità viene ripreso anche dal GDPR nel considerando 4 dove viene stabilito che: "Il trattamento dei dati personali dovrebbe essere al servizio dell'uomo. 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 ossequio al principio di proporzionalità". Si è visto che nonostante i considerando non abbiano forza di legge, ricoprono un ruolo fondamentale all'interno della normativa della *data protection.*

campo della *data protection*. Le sanzioni vanno comunque comminate in aggiunta o in sostituzione agli altri strumenti a disposizione dell'Autorità. In certi casi, come visto precedentemente dall'analisi dell'articolo 58 del GDPR, quest'ultima può in effetti limitarsi a rivolgere un avvertimento oppure un ammonimento al titolare o responsabile del trattamento. Un avvertimento del Garante viene emesso quando si sospetta una possibile violazione della normativa della *data protection.* Questo significa che il Garante ha riscontrato che un titolare di un trattamento sta operando in modo rischioso, mettendo a repentaglio la protezione dei dati dei soggetti coinvolti. L'Autorità, in questo modo, va a informare il titolare di essere più attendo e di ridurre i rischi connessi alla sue attività. L'avvertimento è considerato un "mezzo di tutela anticipata" ([117]) in quanto il Garante anticipa una possibile violazione futura che potrebbe verificarsi, tuttavia, in concreto la violazione non si è ancora verificata e di conseguenza non risulta essere un provvedimento vincolante. L'ammonimento, invece, è adottato per le violazioni minori ([118]) laddove l'irrogazione di una pena pecuniaria risulterebbe sanzione eccessiva per il titolare del trattamento, se questo è una persona fisica.

Il sistema sanzionatorio prevede pene pecuniarie molto severe, con importo massimo fino a 20 milioni di euro. "Si tratta di sanzioni formalmente amministrative, ma sostanzialmente penali" ([119]). Secondo la Corte EDU ([120]) nella materia penale rientrano non solo gli illeciti definiti come criminali dagli ordinamenti nazionali, ma anche gli illeciti che per la natura del precetto violato e per la severità delle sanzioni irrogate risultino sostanzialmente di natura punitiva. Le sanzioni del GDPR hanno questa natura: le multe pecuniarie sono particolarmente elevate e sono quindi in grado di incidere in maniera significativa nella sfera giuridica del destinatario. Presentando natura afflittiva, esse vanno assoggettate alle garanzie sancite per la materia penale dalla CEDU e dalla

---

[117] ROMANO, *Le tutele dinanzi al Garante della privacy. Reclami, Segnalazioni e Sanzioni,* Pisa, 2022, p. 108.
[118] Le violazioni minori sono quelle che non presentano un elevato rischio per i diritti e le libertà delle persone fisiche, creano comunque un disagio per la persona ma non così gravoso da far sì che il titolare del trattamento subisca una sanzione amministrativa pecuniaria. Tuttavia, un elenco che identifica se la violazione sia minore oppure no non sussiste; generalmente spetta al Garante per la protezione dei dati personali, in base allo stato dell'arte, durata della violazione, tipi di dati trattati, avvenuta collaborazione del titolare, decidere se si tratta di una violazione minore.
[119] ROMANO, *Le tutele dinanzi al Garante della privacy. Reclami, Segnalazioni e Sanzioni,* Pisa, 2022, p. 109.
[120] Engels e altri c. Paesi Bassi, Corte EDU, Application no. 5100/71; 5101/71; 5102/71; 5354/72; 5370/72. https://hudoc.echr.coe.int/tur#{%22itemid%22:[%22001-57478%22]}.

Carta dei diritti fondamentali dell'Unione europea, quali quelle inerenti il diritto di essere ascoltato, il diritto ad un ricorso effettivo e il principio di presunzione di innocenza.

Oltre alla possibilità di emanare sanzioni pecuniare, all'Autorità Garante vengono riconosciuti poteri reintegrativi ([121]), come quello di ordinare la limitazione provvisoria o definitiva di un trattamento dei dati che è, ad es., stato adottato contro la società OpenAI per la vicenda relativa a ChatGPT (su cui v. *infra*). Grazie all'esercizio di questi poteri reintegrativi il Garante emana provvedimenti giuridicamente vincolanti e sanzionatori, nei quali è prevalente però la funzione ripristinatoria (invece che quella punitiva): di conseguenza non si tratta di misure assoggettate alle garanzie difensive previste per la materia penale.

Ancora: il Codice Privacy prevede alcune sanzioni accessorie come, ad esempio, l'inutilizzabilità dei dati, che porta uno svantaggio economico al titolare del trattamento oppure la pubblicazione dell'ordinanza d'ingiunzione presso il portale del Garante.

Le sanzioni devono essere effettive e secondo l'articolo 83, § 2, GDPR, devono essere inflitte in funzione delle circostanze di ogni singolo caso e sulla base di una serie di criteri stabiliti dalla disposizione stessa ([122]). Inoltre, il GDPR ha riconosciuto agli Stati membri

---

[121] All'interno dell'articolo 58 del GDPR sono presenti i diversi poteri reintegrativi che l'Autorità Garante può esercitare che consistono nell'ingiunzione di soddisfare le richieste dell'interessato, ingiunzione di conformare i trattamenti alle disposizioni del Regolamento in una certa misura e entro un determinato termine, ingiunzione di comunicare all'interessato una violazione dei suoi dati persoli, un ordine di cancellazione oppure rettifica del trattamento, revoca della certificazione e ordine di sospensione di un trasferimento di dati.

[122] L'articolo 83 del GDPR distingue due diverse tipologie di sanzioni amministrative: "le violazioni cosiddette di minore gravità, per le quali sono previste le sanzioni amministrative pecuniarie di importo fino a 10 milioni di euro o, per le imprese fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente; le violazioni più gravi in considerazione della maggiore gravità delle fattispecie a cui sono ricondotte, ammontano fino a 20 milioni di euro o, per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore." La scelta della sanzione spetta al Garante il quale, sulla base di quanto stabilito dall'articolo 83, deve valutare: la natura, la gravità e la durata della violazione; il carattere doloso o colposo della violazione; le misure adottate dal titolare del trattamento o dal responsabile del trattamento; il grado di responsabilità del titolare del trattamento o del responsabile del trattamento; eventuali precedenti violazioni pertinenti commesse dal titolare del trattamento; il grado di cooperazione con l'autorità di controllo; le categorie di dati personali interessate dalla violazione; la maniera in cui l'autorità di controllo ha preso conoscenza della violazione, in particolare se e in che misura il titolare del trattamento o il responsabile del trattamento ha notificato la violazione; qualora siano stati precedentemente disposti provvedimenti di cui all'articolo 58, paragrafo 2, nei confronti del titolare del trattamento o del responsabile del trattamento in questione relativamente allo stesso oggetto, il rispetto di tali provvedimenti; l'adesione ai codici di condotta approvati ai sensi dell'articolo 40 o ai meccanismi di certificazione approvati ai sensi dell'articolo 42; eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso, ad esempio i benefici finanziari conseguiti o le perdite evitate, direttamente o indirettamente, quale conseguenza della violazione. Si richiama il seguente articolo: STEFANELLI e ASTI, Le

la possibilità di prevedere sanzioni diverse per violazioni particolarmente gravi sempre però che esse siano "effettive, proporzionate e dissuasive" ([123]). Principio che viene ripreso nell'articolo 84 del Regolamento stesso dove è stabilito che gli Stati membri possono stabilire "le norme relative alle altre sanzioni per le violazioni del presente regolamento, in particolare per le violazioni non soggette a sanzioni amministrative pecuniarie a norma dell'articolo 83, e adottano tutti i provvedimenti necessari per assicurarne l'applicazione".

Si è visto che il Garante per la protezione dei dati personali venne istituito, all'interno dell'ordinamento italiano, con la legge n.675 del 1996. Nel corso degli anni, è stato sempre attivo e numerosi sono stati gli atti emanati. Nei paragrafi successivi verranno analizzati tre casi particolarmente rilevanti in quanto forniscono un quadro dettagliato e preciso del ruolo essenziale del Garante all'interno del sistema giuridico italiano. Con il caso di ChatGPT si potrà vedere come l'Autorità sia sempre pronta a intervenire e valutare le nuove tecnologie che possono mettere a repentaglio i diritti dei cittadini. Nel provvedimento contro l'INPS invece, verrà evidenziata la competenza del Garante di gestire i trattamenti dei dati personali il cui titolare è una società che opera per conto dello Stato perseguendo così un interesse pubblico. In questo si dimostrerà la dinamicità del Garante nel tutelare sia interessi privati sia pubblici. Nell'ultimo caso, contro il servizio Google Analystic gestito da Google LLC, verrà vista l'attenzione che l'Autorità ha nei confronti dei trattamenti transfrontalieri dei dati personali.

---

sanzioni della nuova disciplina privacy, Stefanelli & Stefanelli studio legale, 2020. *https://www.studiolegalestefanelli.it/it/approfondimenti/le-sanzioni-della-nuova-disciplina-privacy/*.

[123] Considerando 152 GDPR: "*Se il presente regolamento non armonizza le sanzioni amministrative o se necessario in altri casi, ad esempio in caso di gravi violazioni del regolamento, gli Stati membri dovrebbero attuare un sistema che preveda sanzioni effettive, proporzionate e dissuasive.*
La natura di tali sanzioni, penali o amministrative, dovrebbe essere determinata dal diritto degli Stati membri".

2.8 Il caso di ChatGPT

Una delle ultime evoluzioni dell'intelligenza artificiale ([124]) e che ha fatto molto scalpore è ChatGPT. Si tratta di una *chatbot* ([125]), basata su IA capace di rispondere agli input degli utenti: più precisamente consiste in un ″modello linguistico in grado di produrre elaborati testuali con un linguaggio intuitivo e naturale″ ([126]). La possibilità di accedere ad un elevatissimo numero di informazioni presenti nella rete da parte di ChatGPT può "incidere sulla sfera individuale di ciascuno" ([127]), ove si dimostri che parte di quei dati sono dati personali raccolti per trattamenti aventi finalità diverse? Questa è la domanda che la Dottrina si è posta in riferimento al rapporto tra intelligenza artificiale e diritti fondamentali del singolo individuo. Il caso di ChatGpt è utile anche per capire l'importanza del potere di controllo del Garante per la protezione dei dati personali.

Con il comunicato stampa del 31 marzo 2023, il Garante per la protezione dei dati personali comunicò di aver adottato un provvedimento d'urgenza contro ChatGPT limitando così il trattamento dei dati personali degli utenti italiani. In data 20 marzo, la

---

[124] Nel 1956 venne coniata l'espressione intelligenza artificiale (d'ora innanzi IA) dal matematico John McCarthy. Il parlamento europeo, presso il portale *Società,* la definisce con questi termini: "*"L'intelligenza artificiale (IA) è l'abilità di una macchina di mostrare capacità umane quali il ragionamento, l'apprendimento, la pianificazione e la creatività. L'intelligenza artificiale permette ai sistemi di capire il proprio ambiente, mettersi in relazione con quello che percepisce e risolvere problemi, e agire verso un obiettivo specifico. Il computer riceve i dati (già preparati o raccolti tramite sensori, come una videocamera), li processa e risponde. I sistemi di IA sono capaci di adattare il proprio comportamento analizzando gli effetti delle azioni precedenti e lavorando in autonomia*". I primi esperimenti nel campo dell'IA risalgono agli Sessanta e riguardavano principalmente tentativi di creazione di sistemi digitali in grado di imitare il ragionamento umano. Grazie allo sviluppo tecnologico, l'IA si è notevolmente evoluta diventando uno strumento molto potente e utile in diversi campi come quello sanitario, bancario e manufatturiero. L'intelligenza artificiale "automatizza l'apprendimento continuo e la scoperta attraverso i dati"; essa "aggiunge intelligenza a prodotti già esistenti", rendendoli più automatizzati e precisi. Si richiama il seguente articolo: [124] SAS, *Perché l'intelligenza artificiale è importante?* In *IA Che cos'è l'intelligenza Artificiale,* presso il seguente link https://www.sas.com/it_it/insights/analytics/what-is-artificial-intelligence.html.
L'IA è in grado di auto-apprendere dai dati che processa mediante il cosiddetto *machine learning*, che permette all'intelligenza artificiale di automatizzare la costruzione di modelli analitici da utilizzare per prendere decisioni future. La Treccani definisce il *machine learning* come "*branca dell'Intelligenza Artificiale che si occupa dello sviluppo di algoritmi e tecniche finalizzate all'apprendimento automatico mediante la statistica computazionale e l'ottimizzazione matematica*". Per maggiori informazioni si richiama il seguente sito: https://www.treccani.it/vocabolario/machine-learning_%28Neologismi%29/.
[125] Definizione di Chatbot presso REDAZIONE OSSERVATORI DIGITAL INNOVATION, *Cosa sono i chatbot e come possono essere sfruttati dalle aziende: "Con Chatbot si intende un agente software in grado di eseguire azioni per un interlocutore umano, basandosi su comandi ricevuti dall'utente in linguaggio naturale".*
[126] C. NEGRI, *Chat GPT, come funziona e cosa può fare: limiti e opportunità*, *BLOG.*
[127] L. CALIFANO, ChatGPT e Meta EDI: spunti problematici su profili regolatori e ruolo delle autorità di controllo di protezione dati, Federalismi, 3 maggio 2023, p. V.

società Open AI ([128]) subì una *data breach* riguardante le "conversazioni degli utenti e le informazioni relative al pagamento degli abbonati al servizio a pagamento" ([129]). Dopo aver ricevuto un reclamo su questo, il Garante avviò la fase istruttoria nel quale riscontrò diverse violazioni. Il Garante emanò il provvedimento senza interpellare le altre autorità dei diversi Stati Membri e il Comitato europeo e questo fece particolare clamore nonostante quanto previsto dall'articolo 60 § 11 ([130]).

Il Garante, compiute le dovute verifiche, ha affermato che all'interno di ChatGPT non veniva «fornita alcuna informativa agli utenti, né agli interessati i cui dati siano stati raccolti da OpenAI e trattati tramite il servizio di ChatGPT»; inoltre, ha rilevato «l'assenza di idonea base giuridica in relazione alla raccolta dei dati personali e al loro trattamento per scopo di addestramento degli algoritmi sottesi al funzionamento di ChatGPT». Proseguendo nella sua verifica, il Garante ha riscontrato «che il trattamento di dati personali degli interessati risulta inesatto in quanto le informazioni fornite da ChatGPT non sempre corrispondono al dato reale» ([131]) e non sussiste una "qualsivoglia verifica dell'età degli utenti in relazione al servizio ChatGPT che, secondo i termini pubblicati da OpenAI L.L.C., è riservato a soggetti che abbiano compiuto almeno 13 anni".

L'Autorità Garante, in conclusione, ha ritenuto che «il trattamento dei dati personali degli utenti, compresi i minori, e degli interessati i cui dati sono utilizzati dal servizio si ponga in violazione degli artt. 5, 6, 8, 13 e 25 del Regolamento». Sulla base delle sue valutazioni, in data 30 marzo 2023, il Garante per la protezione dei dati personali, esercitando i suoi

---

[128] OpenAI è un'organizzazione di ricerca su Intelligenza Artificiale che gestisce ChatGPT.

[129] Comunicato Stampa del Garante per la protezione dei dati personali, 31 marzo 2023: *Intelligenza artificiale: il Garante blocca ChatGPT. Raccolta illecita di dati personali. Assenza di sistemi per la verifica dell'età dei minori.*

[130] Articolo 60 comma 11 GDPR: "Qualora, in circostanze eccezionali, un'autorità di controllo interessata abbia motivo di ritenere che urga intervenire per tutelare gli interessi degli interessati, si applica la procedura d'urgenza di cui all'articolo 66".

[131] ChatGPT viene addestrato con le informazioni pubbliche che trova su Internet e sulla base di ciò che gli utenti scrivono. Inoltre, quando l'utente scrive in italiano, non sempre gli vengono fornite risposte grammaticamente corrette. Le informazioni che vengono prelevate da Internet non sempre sono veritiere ma ChatGPT le elabora lo stesso senza prima verificarne la veridicità. Sul punto si richiama il seguente articolo: DONATO, *ChatGPT per tornare in Italia deve permettere la rettifica delle risposte errate. Per una IA è cosa quasi impossibile, DDAY.it,* 2023. https://www.dday.it/redazione/45599/chatgpt-per-tornare-in-italia-deve-permettere-la-rettifica-delle-risposte-errate-per-una-ia-e-cosa-quasi-impossibile.

poteri d'urgenza ([132]), ha limitato con effetto immediato il trattamento dei dati di utenti italiani da parte di ChatGPT.

Dalla data di ricezione del provvedimento, OpenAI ha avuto un termine di venti giorni per comunicare al Garante le misure individuate per rimediare alla violazione, pena l'irrogazione a suo carco di una sanzione amministrativa ai sensi dell'articolo 58 del GDPR. Il provvedimento ha suscitato un forte dibattito di natura giuridica e tecnica. Analizzando i motivi che hanno portato alla sospensione del trattamento dei dati personali degli utenti italiani da parte di OpenAI, diversi giuristi hanno riscontrato una forte "incisività delle motivazioni in rapporto alle violazioni contestate" ([133]); in quanto, il blocco di ChatGPT, avrebbe provocato un danneggiamento all'innovazione e alla ricerca e a coloro che lavorano con strumenti di questo tipo. Il provvedimento è stato visto come un atto di censura nei confronti delle nuove tecnologie.

Particolare è il punto di vista di Luciano Floridi, il quale, durante un'intervista ([134]) ha dichiarato che "bloccare ChatGPT è una misura draconiana. Impariamo ad usarlo e facciamo leggi", facendo inoltre riferimento alla possibilità per l'utente di utilizzare *Virtual Private Network* (*VPN*) ([135]) per aggirare il blocco imposto dal Garante. L'utilizzo di una VPN "reindirizza l'IP dell'utente attraverso un server remoto posto in un altro paese, anche europeo" ([136]).

Personalmente ritengo che il provvedimento del Garante fosse necessario, soprattutto perché ChatGPT non aveva apprestato un'informativa adeguata che permettesse agli

---

[132] Per maggiori informazioni riguardanti i poteri d'urgenza dell'Autorità Garante si richiama l'articolo 5 comma 8 del Regolamento 1/200058 e articolo 58 par. 2, lettera f) del GDPR.

[133] CALIFANO, ChatGPT e Meta EDI: spunti problematici su profili regolatori e ruolo delle autorità di controllo di protezione dati, Federalismi, 3 maggio 2023, p. VII.

[134] Leggi l'intervista rilasciata il 1° aprile 2023 al periodico *HUFFPOST*: https://www.huffingtonpost.it/economia/2023/04/01/news/luciano_floridi_chat_gpt_garante_privacy-11725205/.

[135] Nell'enciclopedia Treccani on-line si legge che questa espressione "*indica un sistema in grado di creare, tramite Internet, una rete privata che collega i siti (o servizi) utilizzati e il computer o lo smartphone dell'utente, celandone l'identità e proteggendo il traffico in entrate e in uscita*". In questo modo è come se ci fosse un tunnel, privato e sicuro, dove passano tutti i dati che vanno dal dispositivo dell'utente al sito al quale si è collegato. All'interno del tunnel i dati sono criptati e un soggetto esterno non vi può accedere. La VPN permette inoltre di accedere a servizi esteri che ad esempio non sono disponibili su server italiani. È possibile consultare la definizione dell'enciclopedia Treccani presso il seguente link: https://www.treccani.it/vocabolario/vpn_%28Neologismi%29/.

[136] DONATO, *Se ChatGPT è bloccato in Italia, gli utenti utilizzano le VPN per saltare il divieto del Garante, DDAY, 2023. https://www.dday.it/redazione/45503/se-chatgpt-e-bloccato-in-italia-gli-utenti-utilizzano-le-vpn-per-saltare-il-divieto-del-garante*.

utenti di esercitare i propri diritti e di capire le modalità di trattamento dei dati. Sia il GDPR sia il novellato Codice Privacy prevedono questi due principi, e il Garante ne verifica il rispetto. Inoltre, l'utilizzo di una *VPN* ti permette di accedere al servizio ma non tutela i tuoi dati da trattamenti illeciti. Lo scopo del Garante è tutelare il diritto alla protezione dei dati personali dei cittadini e ha bloccato ChatGPT perché violava le disposizioni del GDPR e trattava i dati in modo illecito. Se l'utente accede comunque a ChatGPT, il Garante non è più in grado di proteggerlo ma è un rischio che l'utente stesso si assume.

Dopo aver ricevuto il provvedimento, la società OpenAI ha collaborato con l'Autorità Garante per rimediare alla violazione. In data 11 aprile 2023, successivamente alle informazioni ricevute da OpenAI e alla sua disponibilità ad adottare garanzie adeguate ([137]), attraverso il provvedimento n. 9874702, il Garante ha sospeso il provvedimento di limitazione provvisoria adottato con delibera d'urgenza, assicurandosi l'impegno della società a «predisporre e pubblicare sul proprio sito internet un'informativa adeguata», «mettere a disposizione uno strumento attraverso il quale gli utenti possano esercitare il diritto di opposizione rispetto ai trattamenti». Inoltre, la società si è impegnata ad «inserire un link all'informativa nel flusso di registrazione» e a «modificare la base giuridica del trattamento dei dati personali degli utenti ai fini dell'addestramento degli algoritmi». La società ha dovuto presentare al Garante, entro il 31 maggio 2023, un programma per l'adozione di tali misure ed entro il 30 settembre 2023 implementare il sistema di *age verification*.

Se viene chiesto ora a ChatGPT di mostrare l'informativa privacy, il chatbot rimanda al sito di OpenAI nel quale è possibile visionarla. Per quanto riguarda invece il sistema di age verification, OpenAI "ha inserito nella schermata di benvenuto riservata agli utenti italiani già registrati al servizio un pulsante attraverso il quale, per riaccendere al servizio, dovranno dichiarare di essere maggiorenni o ultra tredicenni e, in questo caso, di avere il

[137] Dopo il provvedimento del Garante per la protezione dei dati personali, Open AI è implementato nuove misure di sicurezza per proteggere i dati degli utenti al fine di rendere il trattamento dei dati sicuro. Ha migliorato la sua informativa andando così a rispettare il principio di trasparenza del GDPR. Inoltre, la conoscenza di ChatGPT si basa sui dati raccolti fino al 2022 e non fornisce informazioni o dati in tempo reale. In questo modo non rischia di violare il principio di correttezza previsto nell'articolo 5 del GDPR.

consenso dei genitori" ([138]) inoltre, "ha inserito nella maschera di registrazione al servizio la richiesta della data di nascita prevedendo un blocco alla registrazione per gli utenti infratredicenni e prevedendo, nell'ipotesi di utenti ultra tredicenni ma minorenni che debbano confermare di avere il consenso dei genitori all'uso del servizio" ([139]). Le misure che sono state adottate da ChatGPT hanno soddisfatto il Garante anche se il percorso risulta essere molto lungo. OpenAI continuerà a implementare nuovi aggiornamenti di ChatGPT ma si è resa disponibile a collaborare con l'Autorità al fine di svolgere le proprie attività in conformità alla legge. Inoltre, il Garante ha dato via allo sviluppo di una task force su ChatGPT composta da tutte le diverse Autorità degli Stati membri, "al fine di promuovere cooperazione e scambio di informazioni sull'applicazione del GDPR al servizio" ([140]).

Il provvedimento contro ChatGPT è stato fondamentale perché ha permesso di capire come poter gestire le nuove tecnologie. Di fatti, grazie all'esperienza maturata e al provvedimento dell'Autorità Garante irlandese contro Google Bard, si è potuto vedere un nuovo tipo di approccio che tutela maggiormente l'individuo. Google Bard ([141]) è un chatbot sviluppato da Google che doveva essere lanciato in Europa a giugno del 2023 ma venne bloccato dal Garante privacy irlandese e di conseguenza il suo lancio venne posticipato a luglio. Il Garante irlandese bloccò il lancio ritendendo «non sufficienti né soddisfacenti quanto prodotto da Google in ordine alla conformità del software alla normativa di settore» ([142]) richiedendo così una valutazione d'impatto sula protezione dei dati. Dopo aver ricevuto il provvedimento, Google modificò la propria informativa e l'Autorità Garante ritenne questo sufficiente al fine di revocare il proprio provvedimento.

---

[138] Anastasio, *ChatGPT torna online in Italia, nuovo sistema di age verification entro il 30 settembre, Key4biz,* 2023. https://www.key4biz.it/chatgpt-torna-online-in-italia-nuovo-sistema-di-age-verification-entro-il-30-settembre/444595/.

[139] *Op.ult.cit.*

[140] Palumbo, *ChatGPT e Garante italiano: alcune riflessioni a distanza di tempo, DebertiJacchia,* 2023. https://www.dejalex.com/2023/06/chatgpt-gdpr-riflessioni-tutela-dati/?lang=it.

[141] "Bard un chatbot basato sull'AI generativa e sull'apprendimento automatico sviluppato da Google e creato sul "modello LaMDA". Si tratta di un software non direttamente integrato in Google *Search*, ma accessibile da un sito/browser indipendente. Bard può accedere a Internet e, quale prodotto di Google, usufruisce dei servizi di Google (Gmail e Docs), parlando in italiano grazie agli autoparlanti. Per accedere a Google Bard basta raggiungere il portale ufficiale e accettare le condizioni di utilizzo, leggendole con attenzione. Dopo di che Google Bard, è pronto all'uso. Lo scopo è quello, né più né meno di Chat GPT, non a caso considerato il suo concorrente". *Op.ult.cit.*

[142] PONTI, *Google Bard in Italia: rafforza la privacy, ma resta un sorvegliato speciale, Cybersecurity360,* 2023.

Tuttavia, Google Bard rimane sorvegliato dal Garante e Google dovrà impegnarsi sempre di più per rendere i propri servizi conformi al GDPR. Il nuovo approccio adottato dalle Autorità degli Stati membri si basa sul valutare preventivamente le nuove tecnologie per evitare che queste possano ledere i diritti dei cittadini europei. Nel caso in cui una tecnologia venga sviluppata in uno Stato al di fuori dell'Unione Europea, non è detto che in quel paese vi sia una normativa sulla *data protection* dettagliata e vincolante come può essere il GDPR. In questo modo, una nuova tecnologia potrà essere "lanciata" in Europa solo dopo che l'Autorità Garante avrà verificato la sua conformità al GDPR. Può sembrare un approccio che si pone in contrasto all'innovazione ma non lo è in quanto, dopo che la tecnologia sarà conforme alla normativa, il Garante darà il via libera per la sua diffusione permettendo così uno sviluppo tecnologico sicuro.

2.9 Garante contro Google Analytics: provvedimento del 9/06/2022 n.9782890

All'interno dell'Unione Europea i dati possono circolare liberamente e i cittadini vengono tutelati a pieno grazie alle disposizioni del GDPR. Risulta essere invece più problematico il trasferimento dei dati extra UE. Inizialmente, la disciplina per questa tipologia di trasferimento si basava sulla decisione di adeguatezza 2000/520 ([143]) della Commissione europea, la quale istituiva il cosiddetto *Safe Harbour*. Esercitando quanto stabilito nell'articolo 25 della Direttiva 95/46 ([144]), la Commissione aveva ritenuto il trasferimento dei dati tra l'Unione europea e le organizzazioni statunitensi aderenti al *Safe Harbour* conforme alla normativa UE e riteneva inoltre, che i "principi internazionali di riservatezza dell'approdo sicuro" ([145]) fossero in grado di tutelare l'interessato.

---

[143] 2000/520/CE Decisione della Commissione del 26 luglio 2000, notificata con il numero C (2000) 2441. È possibile consultarla presso il seguente link: eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32000D0520.

[144] Articolo 25 della Direttiva 95/46/CE comma primo e secondo: "1. Gli Stati membri dispongono che il trasferimento verso un paese terzo di dati personali oggetto di un trattamento o destinati a essere oggetto di un trattamento dopo il trasferimento può aver luogo soltanto se il paese terzo di cui trattasi garantisce un livello di protezione adeguato, fatte salve le misure nazionali di attuazione delle altre disposizioni della presente direttiva. 2. L'adeguatezza del livello di protezione garantito da un paese terzo è valutata con riguardo a tutte le circostanze relative ad un trasferimento o ad una categoria di trasferimenti di dati; in particolare sono presi in considerazione la natura dei dati, le finalità del o dei trattamenti previsti, il paese d'origine e il paese di destinazione finale, le norme di diritto, generali o settoriali, vigenti nel paese terzo di cui trattasi, nonché le regole professionali e le misure di sicurezza ivi osservate".

[145] Documento di lavoro dei servizi della commissione sull'applicazione della decisione 520/2000/CE della Commissione, del 26 luglio 2000, a norma della direttiva 95/46 del Parlamento europeo e del Consiglio sull'adeguatezza della protezione offerta dai principi di approdo sicuro e dalle relative "domande più frequenti" (FAQ) in materia di riservatezza pubblicate dal dipartimento del commercio degli Stati Uniti elaborato a Bruxelles il 13/02/2002. È possibili consultare il seguente documento presso *Privacy.it* al

Tuttavia, il 6 ottobre 2015, con la sentenza *Schrems* I ([146]), la Corte di Giustizia ha annullato tale decisione di adeguatezza perché l'ordinamento americano non garantiva una protezione adeguata dei dati personali. Schrems presentò un reclamo al Garante per la protezione dei dati irlandese denunciando Facebook Ireland. Quest'ultimo inviava i dati raccolti degli utenti europei alla sede americana e una volta che questi giungevano negli Stati Uniti le autorità di intelligence, sulla base del *Safe Harbour,* vi accedevano al fine di poter sorvegliare le comunicazioni degli utenti. In realtà, il *Safe Harbour* non poteva rappresentare una base giuridica legittima a questo tipo di attività in quanto, i giudici della Corte di Giustizia hanno ritenuto la decisione «inadeguata e poco corrispondente alle indicazioni rilevabili nella Direttiva 95/46/CE» ([147]). Questo è dovuto al fatto che, quando venne approvata la decisione di adeguatezza, la Commissione UE non effettuò un'adeguata valutazione della corrispondenza tra le disposizioni previste dalla Direttiva e quanto stabilito all'interno del Safe Harbour, svolgendo così un'attività molto superficiale. Grazie a questo caso la protezione dei dati personali si è ampliata, in quanto è stato nuovamente confermato l'approccio regolamentativo dell'Unione europea orientato maggiormente alla tutela dei diritti fondamentali rispetto alla visione utilitaristica e liberista della circolazione dei dati che è alla base del sistema statunitense.

Nel 2016, dopo l'annullamento del *Safe Harbour*, tra Stati Uniti e Unione è stato stipulato un secondo accordo che portò al cosiddetto *Privacy Shield*, volto a prevedere obblighi più stringenti per le imprese americane riguardanti la tutela dei dati personali. In particolare, le imprese dovevano essere più trasparenti e adottare meccanismi di controllo del rispetto delle regole. Inoltre, erano state garantite maggiori limitazioni sull'accesso delle autorità

---

seguente link: https://www.privacy.it/archivio/cec2002-196.html. Questi principi sono definiti nell'allegato I della decisione di adeguatezza della Commissione. In linea di principio sono classificati in questo modo: notifica, scelta, trasferimento successivo, sicurezza, integrità dei dati, accesso, garanzie d'applicazione.

[146] Sentenza della Corte (Grande Sezione) del 6 ottobre 2015, causa C-362/14. La sentenza è disponibile al seguente link: EUR-Lex - 62014CJ0362 - EN - EUR-Lex (europa.eu). Per maggiori informazioni riguardanti le sentenze Schrems, si richiama il seguente articolo: GENTILE, *La saga Schrems e la tutela dei diritti fondamentali, Federalismi.it,* 13 gennaio 2021.

[147] FREDIANI, *Safe Harbor: cosa è accaduto e come cambierà l'attuale scenario. Colin,* 2016. https://www.consulentelegaleinformatico.it/2016/01/29/safe-harbor-cosa-e-accaduto-e-come-cambiera-lattuale-scenario/#.

pubbliche ai dati degli utenti europei e furono previsti diversi strumenti di tutela per il cittadino ([148]).

Tuttavia, il 16 luglio 2020 la Corte di giustizia, con la sentenza *Schrems* II ([149]), ha caducato questo secondo accordo, in quanto gli Stati Uniti non garantivano una tutela equivalente a quella europea. In particolare, non veniva garantita la possibilità, per gli utenti, di esercitare i propri diritti presentando azioni dinanzi al Garante o giudice e le autorità di intelligence americane svolgevano controlli discriminatori e massivi violando così il principio di proporzionalità.

L'incertezza conseguente all'assenza di accordi per il trasferimento transfrontaliero dei dati personali è stata superata poi con il GDPR, che nel Capo V disciplina questa tipologia di trattamento, e fissando, all'art. 44, il principio fondamentale per cui "qualunque trasferimento di dati personali oggetto di un trattamento o destinati a essere oggetto di un trattamento dopo il trasferimento verso un paese terzo o un'organizzazione internazionale, compresi trasferimenti successivi di dati personali da un paese terzo o un'organizzazione internazionale verso un altro paese terzo o un'altra organizzazione internazionale, ha luogo soltanto se il titolare del trattamento e il responsabile del trattamento rispettano le condizioni di cui al presente capo, fatte salve le altre disposizioni del presente regolamento. Tutte le disposizioni del presente capo sono applicate al fine di assicurare che il livello di protezione delle persone fisiche garantito dal presente regolamento non sia pregiudicato".

Inoltre, l'articolo 45 ritiene lecito il trasferimento se la Commissione, mediante una decisione di adeguatezza, accerta che il paese terzo in cui verranno trasferiti i dati

---

[148] All'interno del contributo "*Privacy Shield Lo Scudo per la privacy fra Ue e USA*" del Garante per la protezione dei dati personali, vengono elencati suddetti strumenti di tutela che sono: 1. Rivolgersi direttamente all'impresa, che deve rispondere, in caso di reclamo da parte di un interessato, entro 45 giorni; 2. Utilizzare un meccanismo di ADR (Risoluzione alternativa delle controversie), gratuito; 3. Rivolgersi all'Autorità di protezione dati, che collaborerà con il Department of Commerce e la Federal Trade Commission degli U.S.A. per garantire accertamenti sui reclami ancora pendenti presentati da cittadini Ue e giungere rapidamente alla loro definizione; 4. Rivolgersi al Privacy Shield Panel (Collegio arbitrale del Privacy Shield) per ottenere, se nessun'altra soluzione si è rivelata praticabile, una decisione esecutiva attraverso un meccanismo di arbitrato. È possibile visionare il contributo al seguente link: https://www.garanteprivacy.it/documents/10160/0/Privacy+shield.+Lo+Scudo+per+la+privacy+fra+Ue+e+USA+-+Infografica#:~:text=L'accordo%20detto%20Privacy%20Shield,%2C%20ossia%20%C2%ABPorto%20sicuro%C2%BB.

[149] Sentenza della Corte di Giustizia 16 luglio 2020, nella causa C-311/18. È possibile consultare la sentenza al seguente link EUR-Lex - 62018CJ0311 - EN - EUR-Lex (europa.eu).

garantisce un'adeguata tutela dei dati personali. Dal momento che non è stata adottata una decisione di adeguatezza nei riguardi degli U.S.A., "il titolare del trattamento o il responsabile del trattamento può trasferire dati personali verso un paese terzo solo se ha previsto garanzie adeguate e a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi, potendo tali garanzie adeguate essere fornite, segnatamente, mediante clausole tipo di protezione dei dati adottate dalla Commissione" ([150]). L'autorità indipendente per la protezione dei dati personali è dunque legittimata a controllare che i trasferimenti siano leciti. Nel nostro ordinamento il Garante ha avuto modo di occuparsi della problematica in esame, in quanto è stato chiamato a verificare la legittimità del trasferimento dei dati svolto da Google *Analytics* [151].

Il 17 agosto 2020 contro la società Caffeina Media S.r.l. è stato presentato un reclamo in relazione al trasferimento a Google *LLC* ([152]) dei dati inerenti gli utenti che avevano fatto accesso al suo sito, raccolti mediante il servizio Google *Analystic*. Nel corso del procedimento Caffeina Media S.r.l ha dichiarato di essere il titolare "dei trattamenti posti in essere mediante il sito *www.caffeinamagazine.it"* ([153]), specificando che "il trattamento dei dati personali è posto in essere per il tramite dello strumento di Google *Analytics* nella sua versione gratuita" ([154]). Inoltre, allega di non avere "né la visibilità del dettaglio dei dati raccolti né può precisamente descriverne le tipologie e ha scelto di avvalersi" del servizio "perché Google afferma di trattare soltanto dati pseudonimi e su base cookie. La società è vincolata al contratto stipulato con Google ["*Google Analytics Terms of Service*"], che agisce in qualità di responsabile del trattamento dei dati raccolti tramite Google *Analytics*" ([155]). In assenza di una decisione di adeguatezza tra Unione europea e Stati Uniti, il trasferimento transnazionale deve rispettare l'articolo 46 del GDPR e il contratto stabilito tra importatore ed esportatore di dati deve essere conforme allo schema tipo emanato dalla Commissione mediante la decisione n. 2010/87/CE. In questo caso,

---

[150] Sentenza della Corte di Giustizia 16 luglio 2020, causa C-311/18, pag. 91. L'articolo 46 del GDPR stabilisce quelle che sono le garanzie adeguate necessarie.

[151] Definizione di Google Analystic presso la Guida di Google, è *una piattaforma che raccoglie i dati da siti web o app per creare report che forniscono informazioni sugli utenti che accedono al sito oppure all'app.* Per maggiori informazioni è possibile consultare il seguente link: https://support.google.com/analytics/answer/12159447?hl=it.

[152] Sede centrale di Google in California, Stati Uniti d'America.

[153] Provvedimento del 9 giugno 2022 n.9782890 p. 2. In precedenza, presso l'informativa della società, il titolare dei trattamenti risulta essere Caffeina Media Ltd e non Caffeina Meda S.r.l.

[154] *Op.ult.cit*

[155] *Op.ult.cit.*

l'accordo contrattuale tra Google *LLC* e Caffeina Media S.r.l. riprendeva le clausole contrattuali standard stabilite nella decisione n.2010/87/CE con però alcune integrazioni effettuate da Google. In particolare, la società Caffeina Media non aveva "alcuna possibilità di verificare l'implementazione a livello tecnico ovvero di impartire specifiche istruzioni sull'effettiva implementazioni delle stesse" ([156]). Suddette integrazioni sono state dichiarate invalide dalla Corte in quanto, secondo il principio di *accountability*, Caffeina Media, in qualità di titolare ed esportatore del trattamento, è tenuto a verificare "in collaborazione con l 'importatore nel paese terzo, se la legge o la prassi di quest'ultimo incidano sull'efficacia delle garanzie adeguate" ([157]) contenute nelle clausole emanate dalla Commissione.

Caffeina Media S.r.l, attraverso Google *Analystic*, era in grado di raccogliere e analizzare alcune statistiche sui propri utenti. In particolare, venivano conservati ([158]): identificatori online unici, dati di navigazione dell'utente, indirizzo IP ([159]). Quest'ultimo costituisce un dato personale nel momento in cui è in grado di "identificare un dispositivo di comunicazione elettronica, rendendo pertanto indirettamente identificabile l'interessato in qualità di utente" ([160]). Tuttavia, Google *Analytics* forniva la possibilità di rendere anonimo l'indirizzo IP dell'utente attraverso l'impostazione "IP-*Anonymization*" ([161]). Impostazione che, alla data di presentazione del reclamo, non era stata implementata da Caffeina Media S.r.l.. In realtà però, durante la fase istruttoria, il Garante ha riscontrato che l'IP-*Anonymization* non impediva "a Google *LLC* di re-identificare l'utente medesimo" ([162]), soprattutto nel caso in cui l'utente, prima di accedere al sito di Caffeina

---

[156] *Op.ult.cit.*

[157] OSTINATO, *Il Garante Privacy dice stop a Google Analytics, Ostinato,* 2022. https://blog.hostinato.it/garante-privacy-dice-stop-google-analytics.

[158] Secondo quanto riportato nel provvedimento n. 9782890 del Garante per la protezione dei dati personali, veniva raccolti anche i seguenti dati: "*nome del sito web, informazioni relative al browser, al sistema operativo, alla risoluzione dello schermo, alla lingua selezionata, data e ora della visita al sito web*".

[159] Definizione di indirizzo IP Treccani: "*Sequenza di numeri o di caratteri alfabetici che permette di individuare un elaboratore connesso in rete, indispensabile sia per ricevere sia per inviare dati; si basa sul protocollo IP (Internet Protocol), che regola l'interconnessione tra reti*". Per maggiori informazioni si richiama il seguente link https://treccani.it/enciclopedia/indirizzo-ip_%28Lessico-del-XXI-Secolo%29/.

[160] Provvedimento del 9 giugno 2022 n.9782890 p. 5.

[161] Tale impostazione andava ad oscurare l'ultimo ottetto, il meno significato, dell'indirizzo IP.

[162] SALVI, *Google Analytics "illegale" secondo il Garante Privacy: e ora?, Agenda Digitale,* 2022. https://www.agendadigitale.eu/sicurezza/privacy/google-analytics-illegale-secondo-il-garante-privacy-e-ora/.

Media S.r.l. si fosse loggato al suo account Google ([163]). Il Garante, riprendendo la sentenza *Schrems* II, ha ribadito che, in caso di assenza di una decisione di adeguatezza, il titolare del trattamento, secondo il principio di *accountability*, deve adottare le garanzie necessarie previste dall'Unione. Inoltre, ha dichiarato che il contratto tra Caffeina Media S.r.l e Google *LLC* non era lecito, in quanto permetteva alle Autorità pubbliche statunitensi di accedere ai dati degli utenti senza prevedere garanzie adeguate per i titolari dei dati. Queste ingerenze si basavano sul *Transparency report on United States national security request for user information*, normativa che, con la sentenza *Schrems* II, era stata considerata incapace di tutelare in maniera adeguata i dati personali degli utenti europei. In mancanza di una protezione adeguata, il titolare del trattamento, sempre secondo il principio di *accountability*, deve adottare delle misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al GDPR. Tuttavia, le misure ([164]) adottate in questo caso, non sono state considerate sufficienti per tutelare gli interessati. Sulla base di tutto ciò, il Garante dichiarò illecito suddetto trattamento dei dati in quanto violava: la decisione 2010/87/CE, l'articolo 46 e 13 del GDPR e il principio di *accountability* posto a carico del titolare del trattamento. Inoltre, applicando i poteri sanzionatori previsti dall'articolo 83 del GDPR, il Garante ha ordinato a Caffeina Media S.r.l di rendere il trattamento dei dati conforme al GDPR entro 90 giorni e ha sospeso il trasferimento transfrontaliero dei dati personali mediante il servizio di Google Analytics.

Bisogna sottolineare però che Stati Uniti e Unione Europea collaborano fortemente al fine di rendere sempre più sicuri i trasferimenti transfrontalieri. Di fatto, il 10 luglio 2023, la Commissione europea ha approvato una nuova decisione di adeguatezza. Tale decisione "si inserisce nell'ambito del quadro UE-USA per la protezione dei dati personali" ([165]) e

---

[163] Mediante l'accesso dell'utente al suo account, Google è in grado di associare all'indirizzo IP dell'utente diverse informazioni che permetto la sua identificazioni. Informazioni contenute nell'account Google dell'utente.

[164] Nel provvedimento del Garante per la protezione dei dati personali n. 9782890 è possibile visionare l'intero procedimento che ha portato a considerare le misure tecniche supplementari non sufficienti per proteggere l'interessato.

[165] BOSCARINO, *Privacy: la Commissione europea adotta una decisione di adeguatezza degli USA per il trasferimento dei dati personali, NT+Diritto,* 2023. https://ntplusdiritto.ilsole24ore.com/art/privacy-commissione-europea-adotta-decisione-adeguatezza-usa-il-trasferimento-dati-personali-AFGbk4C. Tra i nuovi obblighi vi rientrano: il rispetto del diritto alla cancellazione dei dati, rispetto delle limitazioni imposte all'autorità di intelligence americane, l'istituzione del Data Protecion Review Court.

le imprese americane che vi vorranno aderire, dovranno rispettare alcuni obblighi più stringenti in materia di privacy.

3.0 Come il Garante ha sanzionato l'INPS per il caso "bonus Covid"

Con i due casi precedenti si è potuto vedere come il Garante abbia esercitato solo uno dei numerosi poteri sanzionatori previsti dal GDPR, cioè la sospensione del trattamento dei dati personali. Nel caso che analizzeremo in questo paragrafo invece l'Autorità ha sanzionato con una pena pecuniaria (di 300.000 €) l'Istituto Nazionale di Previdenza Sociale (d'ora innanzi Istituto oppure INPS) per aver svolto un trattamento dei dati personali non conforme alla normativa vigente. Nel 2020, durante la pandemia COVID-19, il governo italiano ha adottato il decreto legge n.18/2020 con lo scopo di sostenere alcune categorie di lavoratori ([166]) e ha attribuito all'INPS il compito di gestire l'erogazione di un bonus da seicento euro mensili, poi aumentato a mille. Per poter ottenere il bonus è necessaria "l'assenza di titolarità di una pensione, nonché di una forma previdenziale obbligatoria, ovvero l'insussistenza di un rapporto di lavoro dipendente alla data di entrata in vigore del decreto (17 marzo 2020)" ([167]). Data la situazione di crisi, l'INPS ha deciso di erogare il bonus ha tutti i richiedenti che rispettavano i requisiti previsti dalla normativa, all'esito dei cosiddetti controlli di primo livello ([168]). L'INPS si

---

[166] Secondo il decreto legge I lavoratori che potevano richiedere il bonus erano:
"- liberi professionisti titolari di partita iva attiva alla data del 23 febbraio 2020 e ai lavoratori titolari di rapporti di collaborazione coordinata e continuativa attivi alla medesima data, iscritti alla Gestione separata di cui all'articolo 2, comma 26, della legge 8 agosto 1995, n. 335, non titolari di pensione e non iscritti ad altre forme previdenziali obbligatorie;
- lavoratori autonomi iscritti alle gestioni speciali dell'Ago, non titolari di pensione e non iscritti ad altre forme previdenziali obbligatorie, ad esclusione della Gestione separata di cui all'articolo 2, comma 26, della legge 8 agosto 1995, n. 335
- lavoratori dipendenti stagionali del settore del turismo e degli stabilimenti termali che hanno cessato involontariamente il rapporto di lavoro nel periodo compreso tra il 1° gennaio 2019 e la data di entrata in vigore della presente disposizione, non titolari di pensione e non titolari di rapporto di lavoro dipendente alla data di entrata in vigore della presente disposizione;
- operai agricoli a tempo determinato, non titolari di pensione, che nel 2019 abbiano effettuato almeno 50 giornate effettive di attività di lavoro agricolo;
- lavoratori iscritti al Fondo pensioni Lavoratori dello spettacolo, con almeno 30 contributi giornalieri versati nell'anno 2019 al medesimo Fondo, cui deriva un reddito non superiore a 50.000 euro, e non titolari di pensione".

[167] SALERNO, *Il Garante sanziona l'Inps per 300.000 Euro, il controllore dei furbetti del "bonus Covid" non tratta in modo lecito i dati personali raccolti*, *Privacy e CYBERSECURITY,* 2021, p.31.

[168] I controlli di primo livello consistevano in *"procedure informatiche fondate sul riscontro automatizzato delle informazioni dichiarate dal richiedente nella domanda presentata, con le informazioni presenti nelle banche dati detenute dall'Istituto".* Provvedimento del Garante per la protezione dei dati personali n.9556958 p 2-3.

è limita a svolgere solamente questa tipologia di controlli, di natura lieve, per evitare ritardi nella liquidazione del bonus e di conseguenza non poter aiutare i lavoratori in difficoltà. Bisogna sottolineare che il bonus venne erogato senza prima valutare alcuni aspetti importanti; come, ad esempio, capire se ricoprire una carica parlamentare e/o di amministratore regionale o locale rappresentasse una situazione ostativa alla concessione del bonus. Da questa prima analisi, si può già capire come l'Istituto sia stato superficiale e troppo affrettato nell'erogazione del bonus e una eccessiva fretta può portare a compiere errori e violazioni della normativa.

Tuttavia, dopo un'indagine giornalistica compita dal giornale Repubblica, è stato scoperto che tra i soggetti richiedenti e beneficiari del bonus vi erano ben cinque senatori e duemila amministratori locali.

Dopo la notizia, l'Istituto si è attivato svolgendo i cosiddetti controlli di secondo livello ([169]) per evitare che altri soggetti con le medesime cariche e/o simili, ricevessero il bonus. Controlli che sono stati estesi anche a coloro i quali avevano fatto richiesta del bonus ma erano stati scartati dai controlli di primo livello.

L'INPS avrebbe dovuto sapere che coloro i quali svolgono professioni di questo tipo, non sono legittimati a ricevere il bonus in quanto già titolari di una pensione. L'errore è avvenuto, secondo il Garante per la protezione dei dati, dal trattare un numero troppo elevato di dati senza le dovute autorizzazioni e precauzioni. In particolare, ciò che viene contestato all'INPS all'interno del provvedimento del Garante riguarda l'illegittimità dei due trattamenti svolti dall'Istituto stesso. Illegittimità dovuta, in primo luogo, alla violazione dell'articolo 5 del GDPR, dal momento che l'INPS ha svolto la sua attività in modo poco trasparente e poco corretto. Non sono state specificate in modo chiaro le finalità dei suddetti controlli di secondo livello e non era stata precedentemente accertata la spettanza del bonus ai soggetti dotati di cariche politiche. Inoltre, l'Istituto è stato accusato di aver violato il principio di minimizzazione dei dati in quanto, una maggiore

[169] I controlli di secondo livello consistevano nell'acquisire, dalle banche dati aperte presenti nel portale della Camera dei deputati e del Dipartimento per gli affari interni e territoriali del Ministero dell'interno, i dati anagrafici di deputati, amministratori, sindaci. Una volta acquisiti tali dati, l'INPS ha calcolato, con procedure automatizzate (decreto del Ministero delle finanze del 12 marzo 1974, n. 2227), il codice fiscale dei deputati che è stato confrontato con i codici fiscali presenti nelle domande ricevute.

attenzione durante i controlli di primo livello avrebbe reso i controlli successivi non necessari.

Ulteriore violazione che viene contestata è il mancato rispetto del principio di esattezza dei dati personali. Gli esiti dei controlli di secondo livello non sono sicuramente certi dal momento che si possono verificare casi di omonimia ma l'Istituto aveva completamente ignorato questo aspetto. Viene contestato, inoltre, la mancata valutazione d'impatto sulla protezione dei dati e il mancato coinvolgimento del *Data Protection Officer.* Mancanza ritenuta grave dal Garante dal momento che il trattamento, essendo su larga scala e basandosi su un riscontro di dati acquisiti da banche esterne all'Istituto, metteva a forte rischio i diritti e le libertà degli interessati, soprattutto nel lato mediatico.

L'ultima criticità riscontrata dal Garante è il mancato rispetto dei principi di protezione dei dati personali *by default* e *by design* in quanto "il trattamento ulteriore svolto sui parlamentari e amministratori locali non era stato predisposto in anticipo e la progettazione dei due controlli avrebbe presentato delle criticità, poiché le verifiche ulteriori sull'effettivo possesso dei requisiti sarebbero state fatte soltanto dopo l'erogazione dei benefici e non prima" ([170]).

Dopo l'accertamento delle seguenti violazioni, il Garante è stato legittimato ad applicare una sanzione amministrativa e ordinare una serie di misure correttive come "la cancellazione di tutti i dati personali fino ad ora trattati in violazione del principio di minimizzazione e effettuare la valutazione di impatto sulla protezione dei dati prima di riavviare qualsiasi operazione di trattamento" ([171]). Il Garante risulta fondamentale anche per i trattamenti dei dati personali finalizzati a raggiungere un interesse pubblico, dove sono richieste maggior attenzioni e "rende possibile un allineamento tra quadro normativo e realtà empirica" ([172]).

---

[170] SALERNO, *Il Garante sanziona l'Inps per 300.000 Euro, il controllore dei furbetti del "bonus Covid" non tratta in modo lecito i dati personali raccolti*, *Privacy e CYBERSECURITY,* 2021.
[171] Provvedimento del Garante per la protezione dei dati personali n. 9556958 p 15.
[172] Lorè, *Il caso "bonus Covid" in favore dei titolari di cariche pubbliche: i rilievi sollevati all'INPS dal Garante per la protezione dati personali,* Amministrativamente, 2022, p 278.

In seguito ad aver subito il provvedimento, l'INPS ha presentata un ricorso al Tribunale di Roma ([173]) e il giudice della sentenza ha annullato ([174]) la sanzione stabilita dal Garante. Si tratta di una sentenza di primo grado, bisognerà quindi vedere se il Garante vorrà fare appello per ottenere una riconferma della sua decisione.

[173] Sentenza n. 4735/2022 della XVIII sezione civile del Tribunale di Roma.

[174] All'interno del contributo di MANCINO, *La recente sentenza che annulla la sanzione all'Inps induce a riflessione più generali sul trattamento degli open data, Fede privacy,* 2022 è possibile visionare i motivi a fondamento della decisione del giudice. In particolare, secondo il giudice non è stato violato il principio di privacy *by design e by default* dal momento che i dati sono stati acquisiti da banche dati pubbliche e di conseguenza gli interessati potevano ragionevolmente aspettarsi un uso degli stessi al fine di svolgere un controllo in relazione al proprio status, come indicato nel considerando 47 del GDPR. Inoltre, il giudice ha ritenuto non necessaria una valutazione d'impatto sulla protezione dei dati perché nessuna delle condizioni previste nelle linee guide WP 248 del 2017 si è verificata.

CAPITOLO TERZO

IL PERCORSO DI TUTELA GIURISDIZIONALE: IL RICORSO AL GIUDICE CIVILE

3.1 Le norme che prevedono il ricorso giurisdizionale

Come si è potuto vedere, in caso di violazione della privacy, il cittadino ha a disposizione due diversi rimedi alternativi di tutela, in quanto può ricorrere alternativamente all'autorità amministrativa e a quella giurisdizionale. Il Codice Privacy, prima dell'entrata in vigore del decreto legislativo 101/2018, prevedeva la regola dell'alternatività nell'articolo 145. Successivamente con l'entrata in vigore del GDPR e la conseguente modifica del Codice, tale regola è stata ripresa nel nuovo articolo 140 bis, secondo cui il reclamo è improponibile nel caso in cui l'interessato abbia già proposto ricorso all'autorità giudiziaria; il ricorso giurisdizionale è parimenti improponibile ove sia stato già proposto un reclamo con il medesimo oggetto ([175]). L'interessato potrà comunque fare ricorso al giudice nel caso in cui non abbia ricevuto risposta al reclamo; tuttavia, dovrà aspettare il termine dei nove mesi, stabiliti dalla legge, per l'emanazione del provvedimento dell'autorità amministrativa. Se dopo la presentazione del ricorso, sopraggiunge tardivamente la risposta del Garante si possono verificare due differenti situazioni: "in caso il reclamo sia deciso prima della pronuncia del ricorso, il giudice dovrebbe dichiarare la cessazione della materia del contendere; nell'eventualità in cui, invece, sia la statuizione giudiziaria a precedere la definizione del reclamo, l'Autorità di controllo dovrebbe dichiarare il non luogo a provvedere" ([176]).

Tuttavia, i termini per l'emanazione di un provvedimento del Garante, al verificarsi di determinate circostanze previste dal GDPR, possono essere prorogati. Non è però previsto che la decisione di proroga debba essere comunicata all'interessato, e di conseguenza, nel caso in cui quest'ultimo non venga informato, non potrà conoscere la data dal quale è legittimato a presentare un ricorso al giudice. Sulla base di questo, si potrebbe quindi dedurre che presentare un ricorso in caso di inerzia del Garante, risulti essere

---

[175] ROMANO, *Le tutele dinanzi al Garante della privacy,* Pisa, 2022, p. 31.

[176] PARODO, *La tutela del diritto alla protezione dei dati personali: l'effettività dei rimedi e il ruolo nomofilattico del Comitato europeo per la protezione dei dati personali, Federalismi.it,* 2021, p.116. https://federalismi.it/nv14/articolo-documento.cfm?artid=46120.

particolarmente difficile. Inoltre, sembrerebbe che l'attività del legislatore svolta con l'emanazione del Decreto legislativo 101/2018, invece di semplificare le procedure di tutela, si è posta in contrasto con il diritto fondamentale ad un ricorso giurisdizionale effettivo ([177]). All'interno della giurisprudenza, successivamente ad un importante caso ([178]), si è sviluppata la tesi secondo cui l'alternatività tra i due strumenti di tutela, al fine di essere compatibile con l'articolo 24 della Costituzione, "deve essere inteso in senso specifico e conforme ai principi generali del diritto processuale" ([179]). Sarà sicuramente curioso, vedere come la giurisprudenza porterà avanti questa tesi affrontando i casi futuri.

Il percorso di tutela giurisdizionale trova ovviamente un suo fondamento anche a livello europeo. Di fatto, viene disciplinato dagli articoli 79 e 78 del GDPR. L'articolo 79 stabilisce che "ogni interessato ha il diritto di proporre un ricorso giurisdizionale effettivo qualora ritenga che i diritti di cui gode a norma del presente regolamento siano stati violati a seguito di un trattamento". È doveroso precisare che, così come nel Codice Privacy, anche in quest'articolo viene ripresa l'impossibilità per l'interessato di fare ricorso se è già stato avviato "altro ricorso amministrativo o extragiudiziale disponibile, compreso il diritto di proporre un reclamo a un'autorità di controllo ai sensi dell'articolo 77". Per la presentazione del ricorso, l'interessato può scegliere due diversi fori competenti che sono stati previsti all'interno dell'articolo 79. In particolare, se l'azione è "nei confronti del titolare del trattamento o del responsabile del trattamento sono promosse dinanzi alle autorità giurisdizionali dello Stato membro in cui il titolare del trattamento o il responsabile del trattamento ha uno stabilimento". In alternativa, l'interessato può presentare queste azioni presso l'autorità dello Stato membro in cui risiede abitualmente, tranne nel caso in cui il titolare o responsabile sia un'autorità pubblica di uno Stato membro. Il considerando 147 del GDPR stabilisce che nel caso in cui nel regolamento

---

[177] Diritto previsto all'articolo 24 della Costituzione italiana, dove viene stabilito che: "*tutti possono agire in giudizio per la tutela dei propri diritti e interessi legittimi. La difesa è diritto inviolabile in ogni stato e grado del procedimento. Sono assicurati ai non abbienti, con appositi istituti, i mezzi per agire e difendersi davanti ad ogni giurisdizione. La legge determina le condizioni e i modi per la riparazione degli errori giudiziari*".

[178] Corte di Cassazione, sez. Lavoro, sentenza n. 6775/2016. Per maggiori informazioni sul caso richiamo la seguente rivista: *Diritto e Giustizia. Il quotidiano di Informazione Giuridica.*

[179] LEVERONE, *Non sempre il ricorso al Garante della Privacy è alternativo all'azione giudiziaria*, 2016. Inoltre, l'avvocato prosegue ritenendo che il principio di alternatività "può applicarsi solo quando la domanda proposta in sede giurisdizionale e quella proposta in sede amministrativa siano tali che, in ipotesi di contestuale pendenza davanti a più giudici, potrebbero, in via generale, assoggettate al regime processuale della litispendenza o della continenza". È possibile visionare l'intero contributo al seguente link: https://www.dirittoegiustizia.it/#/documentDetail/9204392.

stesso vengano previste "disposizioni specifiche in materia di giurisdizione, in particolare riguardo a procedimenti che prevedono il ricorso giurisdizionale, compreso quello per risarcimento, contro un titolare del trattamento o un responsabile del trattamento, disposizioni generali in materia di giurisdizione quali quelle di cui al regolamento (UE) n. 1215/2012 del Parlamento europeo e del Consiglio non dovrebbero pregiudicare l'applicazione di dette disposizioni specifiche". Sulla base di ciò, questi criteri speciali prevalgono rispetto le disposizioni europee di natura generale in materia di giurisdizione. Questi due criteri speciali si applicano alle azioni legali avviate dall'interessato contro il titolare o il responsabile del trattamento dei dati personali, mentre quelle di accertamento negativo del titolare o del responsabile verso l'interessato sono regolate da un regolamento separato, il Regolamento (UE) 2012/1215, noto come Bruxelles I-bis. L'azione prevista dall'articolo 79 del GDPR introduce un ricorso civile ordinario, tramite il quale l'interessato può richiedere il risarcimento del danno subito e l'interruzione delle pratiche del titolare o del responsabile del trattamento che non sono conformi al Regolamento (UE) 2016/679.

L'articolo 78 invece si riferisce al ricorso giurisdizionale contro i provvedimenti del Garante. La possibilità di impugnare un provvedimento è una della garanzie previste dall'articolo 58 del GDPR e rappresenta uno strumento di difesa che può essere esercitato sia dall'interessato sia dal titolare del trattamento contro i provvedimenti prescrittivi e le ordinanze. Questa tipologia di ricorso deve essere presentata presso l'autorità giudiziaria appartenente allo Stato in cui è situato il Garante e deve avvenire entro trenta giorni dalla data di comunicazione del provvedimento stesso. Sulla base dell'articolo 10 del decreto legislativo 2011/150, il ricorso deve essere proposto entra trenta giorni dalla data di comunicazione del provvedimento e il giudice ordinario può annullare i provvedimenti del Garante. Tra il 2010 e il 2019 ([180]) questo rimedio ha subito un forte sviluppo, confermando così l'influenza del controllo giudiziario sui provvedimenti amministrativi.

[180] Per maggiori informazioni sull'incremento del numero di ricorsi presentati contro i provvedimenti del Garante per la protezione dei dati personali, si richiama la nota precedente, in particolare p. 117 e seguenti.

3.2 Il risarcimento del danno: quando è possibile ottenerlo. Analisi del percorso svolto dalla giurisprudenza

Secondo l'articolo 82 del GDPR, "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". Tuttavia, se quest'ultimi dimostrano che "l'evento dannoso non gli è in alcun modo imputabile", sono esonerati dalla responsabilità di risarcire il soggetto violato. Anche prima dell'entrata in vigore del GDPR il Codice Privacy, attraverso l'articolo 15, prevedeva che chiunque avesse cagionato un danno "ad altri per effetto del trattamento di dati", era tenuto al risarcimento ai sensi dell'articolo 2050 del Codice civile. Tuttavia, quella norma fu abrogata con il decreto 101/2018 e ora il Codice Privacy si limita a richiamare l'articolo 82 del GDPR all'interno dell'articolo 152 ([181]). Analizzando quest'ultimo articolo, è doveroso fare attenzione su un particolare aspetto. In particolare, l'articolo disciplina tutte le controversie che riguardano "l'applicazione della normativa in materia di protezione dei dati", oltre a quelle oggetto degli articoli 78 e 79 del GDPR. La scelta, del legislatore, di far riferimento alla normativa, anziché alle fonti, è ragionata e sensata in quanto, evita il verificarsi di problemi applicativi del procedimento ([182]). Sempre l'articolo 10 del Decreto legislativo 150/2011 stabilisce che "le controversie previste dall'articolo 152 del decreto legislativo 30 giugno 2003, n. 196, sono regolate dal rito del lavoro, ove non diversamente disposto dal presente articolo." Nonostante l'abrogazione dell'articolo 15,

[181] Articolo 152 Codice Privacy comma primo: "1. Tutte le controversie che riguardano le materie oggetto dei ricorsi giurisdizionali di cui agli articoli 78 e 79 del Regolamento e quelli comunque riguardanti l'applicazione della normativa in materia di protezione dei dati personali, nonché' il diritto al risarcimento del danno ai sensi dell'articolo 82 del medesimo regolamento, sono attribuite all'autorità giudiziaria ordinaria."

[182] Si richiama il seguente contributo: COSTANTINO, *La tutela giurisdizionale dei diritti al trattamento dei dati personali, Privacy.it,* 2014. In particolare, l'avv. ritiene che: "La determinazione per fonti piuttosto che per materia dell'ambito di applicazione del procedimento potrebbe suscitare qualche problema applicativo. Trattandosi di un procedimento speciale, infatti, ai sensi dell'art. 14 disp. prel., esso non può trovare applicazione al di fuori dei casi e dei tempi espressamente considerati20. Il criterio di applicazione fondato sulla fonte della disciplina sostanziale, inoltre, implica che un qualunque successivo provvedimento legislativo sulla utilizzazione dei dati personali dovrebbe considerare che il procedimento speciale regolato dall'art. 152 d.lgs. 30 giugno 2003, n. 196, potrebbe riuscire applicabile esclusivamente alle controversie dal medesimo decreto considerate". L'intero contributo è visibile al seguente link: https://www.privacy.it/archivio/costantino20031125.html.

"la responsabilità per violazione della privacy continua ad ispirarsi al nostro modello della responsabilità per esercizio di attività pericolosa di cui all'art. 250 cod.civ." ([183]).

Quando si parla di danno, viene in soccorso anche il considerando 146 del GDPR il quale afferma che questo termine "dovrebbe essere interpretato in senso lato alla luce della giurisprudenza della Corte di giustizia". Di fatto, viene risarcito sia il danno materiale sia quello immateriale, ossia, secondo la tesi maggioritaria in dottrina, sia quello patrimoniale sia quello non patrimoniale. È doveroso precisare però, che è particolarmente raro che da una violazione della disciplina riguardate la *data protection* si possa verificare un danno patrimoniale. Le violazioni di questo tipo, generalmente, per lo più comportano una "compressione della propria sfera emotiva e/o della propria reputazione", ([184]) che può causare danni psicologici o sociali. Importante è, a tal riguardo, il considerando 85 ([185]), che elenca, non in modo tassativo, i possibili danni che si possono verificare in conseguenza alla violazione delle norme sul trattamento dei dati personali.

La questione della tutela compensativa dei nocumenti derivanti da violazioni della privacy è stato oggetto di diverse pronunce giurisprudenziali, che hanno permesso di definirne i confini.

---

[183] VALERINI, *Le novità processuali in materia di privacy dopo il Reg. 679/2016 (GDPR) e il D.lgs. 101/2018, Judicium,* 2018, p. 6. https://www.judicium.it/wp-content/uploads/2018/10/Valerini.pdf.

[184] COSTA, *Risarcimento del danno per violazione della privacy: la pronuncia della Corte di Cassazione*, *Compliance Legale*, 2022. https://www.compliancelegale.it/2021/08/24/risarcimento-del-danno-per-violazione-della-privacy-la-pronuncia-della-corte-di-cassazione/.

[185] Considerando 85 del GDPR: "*Una violazione dei dati personali 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 pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica L 119/16 IT Gazzetta ufficiale dell'Unione europea 4.5.2016 interessata. Pertanto, non appena viene a conoscenza di un'avvenuta violazione dei dati personali, il titolare del trattamento dovrebbe notificare la violazione dei dati personali all'autorità di controllo competente, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che il titolare del trattamento non sia in grado di dimostrare che, conformemente al principio di responsabilizzazione, è improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Oltre il termine di 72 ore, tale notifica dovrebbe essere corredata delle ragioni del ritardo e le informazioni potrebbero essere fornite in fasi successive senza ulteriore ingiustificato ritardo*".

Già nel 2008 la Corte di Cassazione ([186]), riconosceva la circostanza che la risarcibilità del danno dovuto da un trattamento illecito può verificarsi nei soli casi di superamento della «soglia di tollerabilità della lesione minima» ([187]).

Ancora: nel 2016 la Corte ([188]), richiamando il Codice Privacy, ha precisato che, una volta dimostrata la violazione della disposizione a tutela della riservatezza, opera l'«inversione dell'onere della prova a carico dell'autore del danno, tenuto a dimostrare di aver adottato tutte le misure idonee ad evitarlo» ([189]). Inoltre, prosegue la Corte, «la presunzione *juris 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» ([190]). È doveroso sottolineare che colui che subisce il danno è tenuto a dimostrarlo secondo le regole ordinarie, in quanto un trattamento dei dati personali illecito non "giustifica l'accoglimento della pretesa risarcitoria azionata in via automatica" ([191]), concetto che è stato richiamato anche in una ulteriore sentenza ([192]) nel 2020. Il caso in questione vede protagonista un collaboratore scolastico, il quale si rivolse al Tribunale di Torino chiamando in causa il Ministero dell'Istruzione, l'Università e Ricerca (MIUR) e il direttore della scuola in cui lavorava. L'attore sosteneva che il direttore, avendo condiviso alla Polizia giudiziaria alcune sue informazioni personali ([193]), gli avesse cagionato "umiliazione, disagio e imbarazzo" ([194]) all'interno dell'Istituto Scolastico. Il Tribunale di Torino ha ritenuto infondato ([195]) il ricorso dell'attore

---

[186] Suprema Corte di Cassazione Sezione prima Civile, sentenza n. 26972, 11 febbraio 2008.
[187] *Op.ult.cit.* p. 125.
[188] Corte suprema di Cassazione Sezione prima Civile, sentenza n. 2306, 5 febbraio 2016. È possibile visionarla presso *Ex Parte Creditoris.it,* rivista di informazione giuridica al seguente link: https://www.expartecreditoris.it/wp-content/uploads/2016/03/1456934638cass.civ_.05022016.2306.pdf.
[189] *Op.ult.cit.* p. 3.
[190] *Op.ult.cit.*
[191] OSTINATO, *La tutela del diritto alla protezione dei dati personali: l'effettività dei rimedi e il ruolo nomofilattico del Comitato europeo per la protezione dei dati personali, Federalismi.it,* 2021, p.124.
[192] Suprema Corte di Cassazione Sez. I, n. 29982, 31 dicembre 2020. È possibile visionare la Sentenza al seguente link: http://dirittifondamentali.it/wp-content/uploads/2021/01/Cass.-civ.-29982-2020.pdf.
[193] In particolare, il direttore amministrativo dell'Istituto aveva informato la Polizia sul fatto che il collaboratore avesse subito in passato diverse contestazioni disciplinari.
[194] Suprema Corte di Cassazione Sezione prima Civile I, n. 29982, 31 dicembre 2020, *Dirittifondamentali.it,* p.2.
[195] Furono quattro i motivi a fondamento della decisione del Tribunale di Torino: "la necessità della comunicazione dei dati personali a fini istituzionali; l'estraneità della condotta del B. alla circolazione della notizia nel personale dell'istituto scolastico; la mancata prova dei danni-conseguenza patiti; (d) il difetto di un coefficiente minimo di gravità e serietà per dar luogo a un pregiudizio non patrimoniale risarcibile". *Op.ult.cit.*

condannandolo al pagamento delle spese in favore dei resistenti. Tuttavia, il collaboratore scolastico fece appello alla Corte di Cassazione la quale, dopo un'attenta analisi dei motivi fondativi della decisione del Tribunale di Torino e lo studio del caso, ha dichiarato inammissibile il ricorso. In particolare, nella massima, la Corte espone che il danno non patrimoniale, anche se derivato dalla violazione del diritto fondamentale alla protezione dei dati personali, «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». Con questa sentenza viene riconfermato il principio secondo cui il risarcimento del danno subito da un trattamento illecito non può essere automatico ma vi deve essere la prova da parte del soggetto violato e "dovrà, necessariamente, essere giustificato da un evento grave capace di provocare conseguenze negative all'utente" ([196]).

Facendo quindi una lettura combinata tra l'articolo 82 del GDPR e le diverse sentenze qui sopra analizzate, è possibile sostenere che per ottenere un risarcimento del danno il soggetto leso deve dimostrare l'esistenza di una violazione del regolamento 2016/679, il nesso eziologico tra la condotta illecita e le conseguenze negative patite e l'entità del danno ([197]). Tuttavia, in data 4 maggio 2023, la Corte di Giustizia ([198]) ha dato via ad un nuovo approccio per quanto riguarda il diritto al risarcimento del danno. In particolare, la CGUE è stata interpellata in sede di rinvio pregiudiziale dalla Corte suprema austriaca, chiamata a decidere su un caso dove i protagonisti erano un cittadino austriaco e la società Österreichische Post AG (d'ora innanzi Società oppure OPG). Suddetta Società, dietro corrispettivo in denaro, raccoglieva e cedeva a diverse organizzazioni informazioni sulle preferenze politiche dei cittadini austriaci. Ovviamente, suddetto trattamento, permetteva a OPG di associare, in modo più o meno certo, i diversi partiti politici ai diversi cittadini i cui dati venivano processati.

Sulla base di ciò, l'attore propose un ricorso diretto dinanzi al *Landesgericht für Zivilrechtssachen Wien* ([199]) contro OPG per chiedere al giudice di ordinare alla Società

---

[196] BELCORE, *Il risarcimento per diffusione di dati personali, Forensicnews,* 2021. https://www.forensicnews.it/il-risarcimento-per-diffusione-di-dati-personali/.
[197] CARLONE, *Il risarcimento dei danni per violazione della privacy, Studio Legale Carlone Cecchinelli Di Gregorio,* 2021. https://studiolegaleccdg.it/risarcimento-dei-danni-per-violazione-della-privacy/.
[198] Sentenza della Corte di Giustizia Terza Sezione, causa C-300/21, 4 maggio 2023.
[199] Tribunale del Land in materia civile di Vienna.

di interrompere suddetto trattamento, nonché di condannarla al risarcimento del danno immateriale subito per la somma di 1.000 euro. Si sottolinea il fatto che il cittadino austriaco non aveva dato il proprio consenso per il trattamento dei suoi dati personali. In primo appello, il giudice accolse la domanda inibitoria dell'attore, ma non quella risarcitoria. La questione giunse quindi alla Corte suprema austriaca, la quale decise di sospendere il processo per sottoporre al CGUE tre diverse questioni ([200]). Con riguardo alla prima questione, l'interpretazione dell'articolo 82 del GDPR, la Corte si è espressa dichiarando che questo articolo «deve essere interpretato nel senso che la mera violazione delle disposizioni di tale regolamento non è sufficiente per conferire un diritto al risarcimento» ([201]). Oltre alla violazione, quindi, ci deve essere «l'esistenza di un danno e il nesso di causalità tra tale danno e l'asserita violazione» ([202]). In riferimento invece alla seconda questione, come calcolare il risarcimento del danno, dal momento che nel GDPR non sono presenti disposizioni a tal riguardo, la Corte dichiara che per poter calcolare l'importo del risarcimento «i giudici nazionali devono applicare le norme interne di ciascuno Stato membro relative all'entità del risarcimento pecuniario, purché siano rispettati i principi di equivalenza e di effettività del diritto dell'Unione» ([203]). Infine, per quanto riguarda la terza e ultima questione la Corte si è espressa, ritenendo che non è necessario che il danno superi un certo grado di gravità: l'importante è che vengano rispettati i requisiti stabiliti in risposta alla prima questione.

Sulla base di quanto analizzato finora, si può notare quindi che la Corte di Giustizia ha modificato l'approccio al risarcimento del danno in materia di *data protecion*, andando

---

[200] Così è possibile leggere all'interno della sentenza dalla CGUE: "1) Se ai fini del riconoscimento di un risarcimento ai sensi dell'articolo 82 del RGPD (...) occorra, oltre a una violazione delle disposizioni del RGPD, che il ricorrente abbia patito un danno, o se sia già di per sé sufficiente la violazione di disposizioni del 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". *Op.ult.cit.* p.5.

[201] *Op.ult.cit.* p. 8.

[202] PIEMONTE e STILLO, *La Corte di Giustizia si pronuncia sul diritto al risarcimento del danno causato dal trattamento di dati personali in violazione del GDPR: siamo all'inizio di una nuova "era"?*, *Dejalex.com,* 2023, p. 2. https://www.dejalex.com/wp-content/uploads/2023/05/Articolo_La-Corte-di-Giustizia-si-pronuncia-sul-diritto-al-risarcimento-del-danno-causato-dal-trattamento-di-dati-personali-in-violazione-del-GDPR.pdf.

[203] Sentenza della Corte di Giustizia Terza Sezione, causa C-300/21, 4 maggio 2023, p. 10.

ad eliminare la cosiddetta soglia minima di tollerabilità che aveva rappresentato un linea guida per tutti questi anni.

3.3 Requisiti per far ricorso al giudice in seguito ad un provvedimento del Garante: Ordinanza 29049/2022

È stato visto come il GDPR garantisca, per l'interessato, sia la possibilità di presentare un ricorso diretto al giudice sia di impugnare il provvedimento del Garante per la protezione dei dati personali. In particolare, attraverso una sentenza, la Corte di Cassazione è riuscita a definire in maniera più chiara i possibili casi di applicazione dell'impugnazione ([204]). È doveroso riassumere la vicenda che ha occasionato la decisione della S.C. La regione Abruzzo, nel 2014, indette una procedura concorsuale riservata ai soggetti con disabilità. Durante la procedura, la regione pubblicò la graduatoria dei soggetti ammessi e non ammessi, condividendo però così dati sensibili relativi allo stato di salute dei candidati. La regione, nel pubblicare suddette informazioni, fece riferimento a quanto stabilito nel decreto legislativo n. 33/2013, con riguardo, in particolare, all'obbligo di trasparenza sancito nel decreto stesso.

Successivamente a questa pubblicazione, il Garante mediante provvedimento ([205]) censurò la condotta dell'ente territoriale, rilevando «l'illiceità del trattamento dei dati personali da parte della regione Abruzzo per illegittima diffusione di dati sensibili relativi alla condizione di salute» ([206]). Vietò così alla regione la diffusione di ulteriori dati sensibili, imponendole di implementare adeguate misure di protezione dei dati personali, oltre al pagamento di una sanzione pecuniaria (20.000 €). L'ente locale decise tuttavia di impugnare il provvedimento di fronte al Tribunale dell'Aquila ([207]). A sostegno dell'impugnazione, la regione "eccepiva la scusabilità dell'errore" ([208]) per ignoranza, ma il giudice di primo grado rigettò l'opposizione di quest'ultima in quanto, dopo la ricezione del provvedimento del Garante, La regione era consapevole della necessità di dover trattare i dati personali mediante dovute garanzie e di conseguenza il giudice riconobbe in capo all'opponente l'elemento soggettivo della colpa. La colpa sarebbe stata comunque

---

[204] Suprema Corte di Cassazione Sezione seconda Civile, ordinanza n.29049, 6 ottobre2022, Roma.
[205] Provvedimento del Garante per la protezione dei dati personali n. 313, 19 giugno 2014.
[206] Suprema Corte di Cassazione Sezione seconda Civile, ordinanza n.29049, 6 ottobre2022, Roma, p. 2. Sentenza visibile al seguente link: https://www.diritto.it/wp-content/uploads/2022/11/125761-1.pdf.
[207] Tribunale dell'Aquila, sentenza n.355, depositata il 30 aprile 2018.
[208] IADECOLA, *Confermata sanzione del Garante a Regione Abruzzo su concorso disabili*, *Diritto.it,* 2022. https://www.diritto.it/confermata-sanzione-del-garante-a-regione-abruzzo-su-concorso-disabili/.

presente, anche senza il provvedimento del Garante, visto che la pubblica amministrazione deve sempre agire nel rispetto della legge e l'ignoranza delle norme non è di conseguenza ammissibile. Inoltre, secondo il giudice, la regione avrebbe potuto pubblicare la graduatoria adottando delle tecniche di anonimizzazione o con altre modalità capaci di assicurare un corretto bilanciamento tra il diritto alla riservatezza dei candidati e le esigenze di pubblicità della procedura concorsuale.

A questo punto, la regione decise di presentare ricorso avanti alla Cassazione sulla base di diversi motivi ([209]), tra cui in particolare l'omissione da parte del Tribunale dell'"esimente della buona fede" ([210]), che rappresenta "causa di esclusione della responsabilità amministrativa in presenza di elementi positivi idonei ad ingenerare nell'autore della violazione il convincimento della liceità della sua condotta" ([211]). La Corte di Cassazione ha ritenuto infondati i motivi della ricorrente, stabilendo che la buona fede come scusabilità dell'errore non può essere accolta in quanto, "in tema di illecito amministrativo *l'error iuris* è invocabile solo a fronte della inevitabilità dell'ignoranza del precetto violato, il cui risultato è l'effetto di una valutazione complessiva circa l'obbligo di conoscenza delle leggi che grava sull'agente in relazione alla qualità professionale posseduta, oltre che al suo dovere di informazione e di interpretazione delle norme che si riferiscono direttamente all'attività svolta" ([212]). Di fatto, nel caso in questione, si trattava di interpretare delle norme per cui non è ammessa ignoranza e su cui già il giudice di primo grado si era espresso. Sulla base di ciò, la Corte di Cassazione

---

[209] Nel contributo di MANCUSI, *Protezione dati personali: il privato che impugni il provvedimento del Garante deve fornire elementi capaci di influire sulla decisione* presso la rivista *PuntodiDiritto* vengono analizzatati i motivi del ricorso alla Corte di Cassazione. In particolare, "con il primo motivo parte ricorrente ha lamentato, ex art. 360 comma 1 n.3 c.p.c, la violazione dell'art. 7 della legge n. 241/1990, per avere il Tribunale mal interpretato l'eccezione sollevata dall'amministrazione ricorrente in merito alla mancata comunicazione dell'avvio del procedimento ritenendola diretta all'ordinanza n.179/2017 - adottata a conclusione dell'iter procedimentale - piuttosto che al provvedimento iniziale n.313/2014; nonché per non aver applicato ai procedimenti sanzionatori del Garante la legge sul processo amministrativo. Con il terzo motivo la ricorrente ha denunciato, ex art.360 comma 1 n.3 c.p.c., la violazione dell'art.4 della legge n. 689/1981, nonché l'erronea motivazione del giudice "in punto di ritenuta insussistenza di causa di esclusione della responsabilità"". Questi sono alcuni motivi sollevati dalla ricorrente, per maggiori informazioni si richiama la sentenza stessa visionabile presso: http://www.consiglioregionale.piemonte.it/infolegint/dettaglioSchede.do?idScheda=12239.

[210] IADECOLA, *Confermata sanzione del Garante a Regione Abruzzo su concorso disabili*, *Diritto.it,* 2022. https://www.diritto.it/confermata-sanzione-del-garante-a-regione-abruzzo-su-concorso-disabili/.

[211] *Op.ult.cit.*

[212] BUCCA e TADDEI, *Corte di Cassazione: i limiti di impugnazione dei provvedimenti del Garante per la protezione dei dati personali,* Studio *Previti,* 2022. https://www.previti.it/corte-di-cassazione-i-limiti-di-impugnazione-dei-provvedimenti-del-garante-la-protezione-dei-dati-personali.

ha rigettato il ricorso della regione, sottolineando in particolare il fatto che «il privato che impugni il provvedimento del Garante non può limitarsi a denunciare la mancata comunicazione di avvio del procedimento e la lesione della propria pretesa partecipativa, ma deve indicare o allegare gli elementi di fatto o valutativi che, se acquisiti, avrebbero potuto influire sulla decisione finale» ([213]). Questa sentenza risulta essere particolarmente importante, poiché ha nuovamente chiarito quando sia possibile invocare l'esimente della buona fede e della scusabilità dell'errore, ma soprattutto perché ha posto dei confini chiari all'impugnazione dei provvedimenti emanati dal Garante per la protezione dei dati personali, anche al fine di evitare un eccessivo ingolfamento dei Tribunali e delle Corti.

[213] Suprema Corte di Cassazione Sezione seconda Civile, ordinanza n.29049/2022, p. 5.

CONCLUSIONI

Giunge al termine l'analisi del diritto alla riservatezza, del diritto alla protezione dei dati personali e dei rimedi giustiziali previsti in Italia per la tutela degli stessi svolto nel presente elaborato, in cui ho cercato di dimostrare il forte rapporto che sussiste tra diritto e tecnologia. La tecnologia è uno strumento fondamentale che aiuta le persone durante la loro quotidianità. Tuttavia, un uso scorretto della stessa e una mancata regolamentazione ad hoc possono provocare gravi conseguenze. Il diritto non può e non deve restare immobile rispetto al progresso tecnologico, deve essere sempre pronto per evitare vuoti di tutela.

Si è illustrato come da una vicenda verificatasi negli Stati Uniti nel 1890 si sia giunti al riconoscimento di un diritto fondamentale, a dimostrazione della dinamicità e della capacità evolutiva del diritto. La privacy è un elemento imprescindibile della nostra vita, che necessita di essere tutelata in maniera effettiva. A tali fini appare centrale l'istituzione di una Autorità amministrativa indipendente come il Garante per la protezione dei dati personali, capace di assicurare misure volte ad offrire al cittadino la massima protezione in caso di violazione dei propri diritti.

Tuttavia, il percorso non si conclude qui, con il correre del tempo, ci saranno sicuramente nuove tecnologie che incideranno sulla nostra vita e sarà curioso vedere come il diritto evolverà di conseguenza. Ovviamente, per fare ciò sarà necessaria una collaborazione attiva tra gli studiosi delle differenti discipline interessate (giuridiche, informatiche, economiche, sociologiche, etc.), le istituzioni politiche e gli operatori del settore nei diversi ordinamenti, infra ed extra UE.

BIBLIOGRAFIA

Alongi e Pompei, *Diritto della privacy e protezione dei dati personali Il GDPR alla prova della data driven economy, Roma*, 2021

Califano, *Principi E Contenuti Del Regolamento UE 2016/679 in Materia Di Protezione Dei Dati Personali*. 11 Mar. 2019.

Califano e Colapietro. *Innovazione Tecnologica E Valore Della Persona. Il Diritto Alla Protezione Dei Dati Personali Nel Regolamento UE 2016/679*. Editoriale Scientifica, 2017.

Califano, *Privacy: affermazione e pratica di un diritto fondamentale,* Napoli, 2016.

Carlone, et al. "Risarcimento Dei Danni per Violazione Della Privacy." *Studio Legale Carlone Cecchinelli Di Gregorio*, 15 Dec. 2021, studiolegaleccdg.it/risarcimento-dei-danni-per-violazione-della-privacy/.

Carrozza, et al. "AI: Profili Tecnologici. Automazione E Autonomia: Dalla Definizione Alle Possibili Applicazioni Dell'Intelligenza Artificiale." *BioLaw Journal - Rivista Di BioDiritto*, no. 3, 27 Nov. 2019, pp. 237–254, teseo.unitn.it/biolaw/article/view/1389/1393, https://doi.org/10.15168/2284-4503-450.

Colapietro, *I Principi Ispiratori Del Regolamento UE 2016/679 Sulla Protezione Dei Dati Personali E La Loro Incidenza Sul Contesto Normativo Nazionale*. 21 Nov. 2018.

Cuffaro, *I Dati Personali Nel Diritto Europeo*. G Giappichelli Editore, 29 Mar. 2019.

Floridi, La *Quarta Rivoluzione: Come l'Infosfera Sta Trasformando Il Mondo*. Milano, Raffaello Cortina, 2017.

Frediani, “Safe Harbor: Cosa è Accaduto E Come Cambierà l’Attuale Scenario.” *Colin*, 28 gennaio. 2016, www.consulentelegaleinformatico.it/2016/01/29/safe-harbor-cosa-e-accaduto-e-come-cambiera-lattuale-scenario/#.

Ghidini e Cavani, *Proprietà Intellettuale E Concorrenza. Corso Di Diritto Industriale*. Zanichelli, 2022.

Guarda e Bincoletto, *Diritto Comparato Della Privacy E Della Protezione Dei Dati Personali*. Ledizioni, 2023.

LE COSTITUZIONI DEGLI ALTRI Banca Documenti Del Consiglio Regionale Del Veneto a Cura Della Direzione Regionale Rapporti E Attività Istituzionali COSTITUZIONE DEGLI STATI UNITI.

Pagallo, *Il Diritto Nell’età Dell’informazione*. G Giappichelli Editore, 22 Dec. 2014.

Pagano, *Tutela dei dati personali: evoluzione della legislazione europea e stato del dibattito*, Torino, 1983.

Pizzetti, *Privacy E Il Diritto Europeo Alla Protezione Dei Dati Personali: Dalla Direttiva 95/46 al Nuovo Regolamento Europeo*. Torino, G. Giappichelli, 2016.

Prosser, *Privacy, in California Law Review* Vol. 48, 1960, pp. 383–423.

Resta e, *Le Persone E La Famiglia Vol. 1 Le Persone Fisiche E I Diritti Della Personalità*. 2019.

Rodotà, *Intervista su privacy e libertà,* Roma-Bari*,* 2005.

Rodotà, *Elaboratori elettronici e controllo sociale,* Bologna, 1973.

Romano, *Le Tutele Dinanzi al Garante Della Privacy. Reclami, Segnalazioni E Sanzioni*. Pacini Giuridica, 2022.

Warren e Brandeis. “The Right to Privacy.” *Harvard Law Review*, 1890, p. Vol. 5, n. 4, 193-220.

SITOGRAFIA

Alverone, *Norme Procedurali Privacy: Il Procedimento Dinanzi al Garante per l'Adozione Di Provvedimenti Correttivi E Sanzionatori | Il Portale Giuridico Online per I Professionisti - Diritto.it*. 8 June 2022, www.diritto.it/norme-procedurali-privacy-il-procedimento-dinanzi-al-garante-per-ladozione-di-provvedimenti-correttivi-e-sanzionatori/.

Belcore, "Il Risarcimento per Diffusione Di Dati Personali." *ForensicNews*, 9 Feb. 2021, www.forensicnews.it/il-risarcimento-per-diffusione-di-dati-personali/.

Bolognesi, "Le Principali Novità Introdotte Dal Decreto N. 101 Del 10 Agosto Del 2018 Rispetto Agli Obblighi Previsti Dal GDPR 2016/679 E Dlgs 196/03." *ICT Security Magazine*, 13 Dec. 2018, www.ictsecuritymagazine.com/articoli/le-principali-novita-introdotte-dal-decreto-n-101-del-10-agosto-del-2018-rispetto-agli-obblighi-previsti-dal-gdpr-2016-679-e-dlgs-196-03/.

Boscarino. "Privacy: La Commissione Europea Adotta Una Decisione Di Adeguatezza Degli USA per Il Trasferimento Dei Dati Personali." *NT+ Diritto*, 13 July 2023, ntplusdiritto.ilsole24ore.com/art/privacy-commissione-europea-adotta-decisione-adeguatezza-usa-il-trasferimento-dati-personali-AFGbk4C.

Bucca e Taddei. "Studio Previti Associazione Professionale | Corte Di Cassazione: I Limiti Di Impugnazione Dei Provvedimenti Del Garante per La Protezione Dei Dati Personali." *Studio Previti Associazione Professionale*, 19 Nov. 2022, www.previti.it/corte-di-cassazione-i-limiti-di-impugnazione-dei-provvedimenti-del-garante-la-protezione-dei-dati-personali.

Califano, "*Il Ruolo Di Vigilanza Del Garante per La Protezione Dei Dati Personali.*" *Www.federalismi.it*, 2 Dec. 2020, www.federalismi.it/ApplOpenFilePDF.cfm?artid=44514&dpath=document&dfile=02122020144607.pdf&content=Il%2Bruolo%2Bdi%2Bvigilanza%2Bdel%2B

Garante%2Bper%2Bla%2Bprotezione%2Bdei%2Bdati%2Bpersonali%2B%2D%2Bstato%2B%2D%2Bdottrina%2B%2D%2B.

"ChatGPT: Al via Una Task Force Europea." *Www.garanteprivacy.it*, 13 Apr. 2023, www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9875657.

"ChatGPT: Garante Privacy, Limitazione Provvisoria Sospesa Se OpenAI Adotterà Le Misure Richieste. L'Autorità Ha Dato Tempo Alla Società Fino al 30 aprile per Mettersi in Regola." *Www.garanteprivacy.it*, 12 Apr. 2023, www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9874751.

"ChatGPT: OpenAI Riapre La Piattaforma in Italia Garantendo Più Trasparenza E Più Diritti a Utenti E Non Utenti Europei." *Www.garanteprivacy.it*, 28 Apr. 2023, www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9881490.

Chiarello, *Il valore costituzionale della Carta di Nizza: un problema ancora aperto anche alla luce della sentenza n. 269/2017 della Corte costituzionale, Consulta online, 2018,* p. 378. https://giurcost.org/contents/giurcost/studi/chiariello.pdf.

"Cosa Fa Il Garante per La Protezione Dei Dati Personali (Garante Della Privacy)." *Openpolis*, 15 July 2020, www.openpolis.it/parole/chi-e-il-garante-per-la-protezione-dei-dati-personali-garante-della-privacy/.

Corona, "GDPR: Poteri Dell'Autorità Garante." *Legaldesk.it*, 8 July 2018, legaldesk.it/blog/gdpr-poteri-garante.

Corona, "GDPR Benvenuto, Addio Codice Privacy." *Legaldesk.it*, 8 July 2018, legaldesk.it/blog/benvenuto-gdpr-addio-codice-privacy.

Costa, “GDPR: Con Il Decreto Legislativo 101/2018 La Privacy Italiana Si Adegua.” *Spindox*, 19 Sept. 2018, www.spindox.it/it/gdpr-decreto-legislativo-101-2018-privacy/.

Costa. “Risarcimento Del Danno per Violazione Della Privacy: La Pronuncia Della Corte Di Cassazione - Compliance Legale.” *Compliance Legale*, 24 Aug. 2021, www.compliancelegale.it/2021/08/24/risarcimento-del-danno-per-violazione-della-privacy-la-pronuncia-della-corte-di-cassazione/.

Costantino, “G. Costantino: La Tutela Giurisdizionale Dei Diritti al Trattamento Dei Dati Personali.” *Www.privacy.it*, 2014, www.privacy.it/archivio/costantino20031125.html.

DEVITALAW. “Tutela Della Privacy E Data Protection: Concetti Diversi, Troppo Spesso Confusi. • DEVITALAW.” *DEVITALAW*, 4 Sept. 2020, www.devita.law/tutela-della-privacy-e-data-protection-concetti-diversi-troppo-spesso-confusi/.

Di Ciollo, *L’ambito di applicazione della normativa privacy: analisi comparata tra GDPR e direttiva 95/46/CE, Iusintinere.it,* 2019, https://www.printfriendly.com/p/g/sKdbNA.

Di Dio, “Il Diritto Ad Essere Dimenticati.” *Altalex*, 11 May 2021, www.altalex.com/documents/news/2021/05/11/diritto-ad-essere-dimenticati.

Di Francesco, “La Tutela Del Diritto Alla Protezione Dei Dati Personali: L’effettività Dei Rimedi E Il Ruolo Nomofilattico Del Comitato Europeo per La Protezione Dei Dati Personali.” *Federalismi.it*, 3 Nov. 2021, www.federalismi.it/nv14/articolo-documento.cfm?Artid=46120&content=La%2Btutela%2Bdel%2Bdiritto%2Blla%2Bprotezione%2Bdei%2Bdati%2Bpersonali%3A%2Bl%E2%80%99effettivi

t%C3%A0%2Bdei%2Brimedi%2Be%2Bil%2Bruolo%2Bnomofilattico%2Bdel%2BComitato%2Beuropeo%2Bper%2Bla%2Bprotezione%2Bdei%2Bdati%2Bpersonali&content_author=%3Cb%3EFrancesco%2BParodo%3C%2Fb%3E.

Donato, "ChatGPT per Tornare in Italia Deve Permettere La Rettifica Delle Risposte Errate. Per Una IA è Cosa Quasi Impossibile." *DDay.it*, 2023, www.dday.it/redazione/45599/chatgpt-per-tornare-in-italia-deve-permettere-la-rettifica-delle-risposte-errate-per-una-ia-e-cosa-quasi-impossibile.

Donato, "Se ChatGPT è Bloccato in Italia, Gli Utenti Utilizzano Le VPN per Saltare Il Divieto Del Garante." *DDay.it*, 2023, www.dday.it/redazione/45503/se-chatgpt-e-bloccato-in-italia-gli-utenti-utilizzano-le-vpn-per-saltare-il-divieto-del-garante.

dunp.it. "Violazione Della Privacy E Risarcimento Del Danno." *Uniriz.it*, 15 Mar. 2022, www.uniriz.it/articolo-34/violazione-della-privacy-e-risarcimento-del-danno/.

Di Tommaso Frosini, *Privacy: diritto fondamentale oppure no, Federalismi.it,* 6 agosto 2008. *https://www.federalismi.it/nv14/articolo-documento.cfm?Artid=10767&content=&content_author=*.

"EUR-Lex - Proportionality - EN - EUR-Lex." *Eur-Lex.europa.eu*, eur-lex.europa.eu/IT/legal-content/glossary/principle-of-proportionality.html.

Figini, "ChatGPT: Perché Il Blocco in Italia (Privacy Violata) E Come Aggirarlo. Il Commento Di Matteo Salvini." *IGizmo.it*, 3 Apr. 2023, www.igizmo.it/chatgpt-perche-il-blocco-in-italia-privacy-violata-e-come-aggirarlo-vpn/.

Gentile, "La Saga Schrems E La Tutela Dei Diritti Fondamentali." *Www.federalismi.it*, 13 gennaio. 2021, www.federalismi.it/ApplOpenFilePDF.cfm?artid=44743&dpath=document&dfile=13012021225756.pdf&content=La%2Bsaga%2BSchrems%2Be%2Bla%2Btut

ela%2Bdei%2Bdiritti%2Bfondamentali%2B%2D%2Bstato%2B%2D%2Bdottrina%2B%2D%2B.

Giacobbe, "Violazione Della Normativa Sulla Protezione Dei Dati." *Riskmanagement*, 11 Mar. 2021, www.riskmanagement360.it/analisti-ed-esperti/violazione-della-normativa-sulla-protezione-dei-dati-risarcibilita-del-danno-non-patrimoniale/.

Giornalettismo, "Guido Scorza Su Google Analytics: "La Soluzione Deve Essere Politica, Tra Stati Uniti E UE" - Intervista a Guido Scorza." *Www.garanteprivacy.it*, 24 June 2022, www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9783595.

"Google: Garante Privacy Stop All'uso Degli Analytics. Dati Trasferiti Negli Usa Senza Adeguate Garanzie." *Www.garanteprivacy.it*, 22 June 2022, www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9782874.

Iadecola. "Confermata Sanzione Del Garante a Regione Abruzzo Su Concorso Disabili | Il Portale Giuridico Online per I Professionisti - Diritto.it." *Diritto.it*, 17 Nov. 2022, www.diritto.it/confermata-sanzione-del-garante-a-regione-abruzzo-su-concorso-disabili/.

"Intelligenza Artificiale: Che Cos'è E Come Funziona." *Www.sas.com*, www.sas.com/it_it/insights/analytics/what-is-artificial-intelligence.html.

Intelligenza Artificiale: Il Garante Blocca ChatGPT. Raccolta Illecita Di Dati Personali. Assenza Di Sistemi per La Verifica Dell'età Dei Minori." *Www.garanteprivacy.it*, 31 Mar. 2023, www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9870847.

Leverone, "Diritto E Giustizia." *Www.dirittoegiustizia.it*, 2016, www.dirittoegiustizia.it/#/documentDetail/9204392.

Lorè, “Il Caso “Bonus Covid” in Favore Dei Titolari Di Cariche Pubbliche: I Rilievi Sollevati All’INPS Dal Garante per La Protezione Dati Personali.” *Amministrativ@Mente - Rivista Di Ateneo Dell’Università Degli Studi Di Roma “Foro Italico,”* vol. 0, no. 2, 15 July 2022, www.amministrativamente.com/index.php/formez/article/view/13295/12019.

Lubello, “Google Analytics E GDPR. Possibili Soluzioni Di Un Equilibrio Instabile.” *MediaLaws*, 30 Sept. 2022, www.medialaws.eu/rivista/google-analytics-e-gdpr-possibili-soluzioni-di-un-equilibrio-instabile/.

Mancino. *La Recente Sentenza Che Annulla La Sanzione All’Inps Induce a Riflessione Più Generali Sul Trattamento Degli Open Data*. 2022, Fede privacy.

Mancusi, “Protezione Dati Personali: Il Privato Che Impugni Il Provvedimento Del Garante Deve Fornire Elementi Capaci Di Influire Sulla Decisione.” *PuntodiDiritto*, 10 Oct. 2022, www.puntodidiritto.it/protezione-dati-personali-privato-impugni-provvedimento-garante-deve-fornire-elementi-capaci-di-influire-su-decisione/.

Michetti, “Il Prezzo Dei Dati Personali: Cosa C’è Dietro Il “Paradosso Della Privacy.”” *Agenda Digitale*, Agenda Digitale, 7 Oct. 2019, www.agendadigitale.eu/sicurezza/privacy/il-prezzo-dei-dati-personali-cosa-ce-dietro-il-paradosso-della-privacy/.

Negri, “Chat GPT, Come Funziona E Cosa Può Fare: Limiti E Opportunità.” *Blog.osservatori.net*, 17 Apr. 2023, blog.osservatori.net/it_it/chatgpt-come-funziona-cosa-puo-fare-limiti-opportunita#.

Nucara, “Ispezione Privacy: Regole Fondamentali per Affrontare Un Controllo Della GdF (E Dell’Autorità Garante).” *Cyber Security 360*, 17 Feb. 2020,

www.cybersecurity360.it/legal/privacy-dati-personali/ispezione-privacy-regole-fondamentali-per-affrontare-un-controllo-della-gdf-e-dellautorita-garante/.

Ostinato, "Il Garante Privacy Dice Stop a Google Analytics." *Blog.hostinato.it*, 2022, blog.hostinato.it/garante-privacy-dice-stop-google-analytics

Parodo, "La Tutela Del Diritto Alla Protezione Dei Dati Personali: L'effettività Dei Rimedi E Il Ruolo Nomofilattico Del Comitato Europeo per La Protezione Dei Dati Personali." *Federalismi.it*, 3 Nov. 2021, federalismi.it/nv14/articolo-documento.cfm?artid=46120.

Piemonte e Stillo, "La Corte Di Giustizia Si Pronuncia Sul Diritto al Risarcimento Del Danno Causato Dal Trattamento Di Dati Personali in Violazione Del GDPR: Siamo All'inizio Di Una Nuova Era?" *Studio Legale de Berti Jacchia Franchini Forlani*, 24 May 2023, www.dejalex.com/2023/05/corte-giustizia-pronuncia-diritto-risarcimento-danno-trattamento-dati-personali-violazione-gdpr-nuova-era/.

Pisano, "Violazioni Della Privacy: Per Ottenere Il Risarcimento Il Danno Deve Essere Rilevante." *E-Lex*, 11 Sept. 2020, www.e-lex.it/it/violazioni-della-privacy-per-ottenere-il-risarcimento-il-danno-deve-essere-rilevante/.

Pizzetti, "Codice Privacy Italiano Dopo Il Gdpr: Come Leggerlo E Applicarlo Ex Decreto 101/2018." *Agenda Digitale*, 14 Sept. 2018, www.agendadigitale.eu/sicurezza/gdpr-pizzetti-i-consigli-per-leggere-e-applicare-bene-il-decreto-101-2018-dal-19-settembre/.

Pizzetti, "La Protezione Dei Dati Personali Dalla Direttiva al Nuovo Regolamento: Una Sfida per Le Autorità Di Controllo E Una Difesa per La Libertà Dei Moderni." *MediaLaws*, 8 Feb. 2018, www.medialaws.eu/rivista/la-protezione-dei-dati-

personali-dalla-direttiva-al-nuovo-regolamento-una-sfida-per-le-autorita-di-controllo-e-una-difesa-per-la-liberta-dei-moderni/.

Pizzetti, "Pizzetti, ChatGpt: Senza Diritti Siamo Nudi Davanti All'intelligenza Artificiale." *Agenda Digitale*, Agenda Digitale, 3 Apr. 2023, www.agendadigitale.eu/sicurezza/privacy/pizzetti-chatgpt-senza-diritti-siamo-nudi-davanti-allintelligenza-artificiale/.

Pollicino, *Interpretazione o manipolazione? La Corte di giustizia definisce un nuovo diritto alla privacy digitale, Feredalismi.it, 2014.*

"Privacy Shield." *Www.garanteprivacy.it*, 26 July 2016, www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/5306161.

Quari, "Profili Storico-Comparativi Del Diritto Alla Privacy." *Diritti Comparati*, 4 Dec. 2014, www.diritticomparati.it/profili-storico-comparativi-del-diritto-alla-privacy/.

Redazione Osservatori Digital Innovation. "Chatbot, Cosa Sono E Come Possono Essere Sfruttati Dalle Aziende." *Blog.osservatori.net*, 17 Apr. 2023, blog.osservatori.net/it_it/chatbot-cosa-sono-come-utilizzarli.

Saetta, "Basi Giuridiche Del Trattamento Dei Dati Personali." *Protezione Dati Personali*, 22 July 2018, protezionedatipersonali.it/base-giuridica-del-trattamento.

Saetta, *Privacy negli Usa, Protezione dati personali,* 2016. https://protezionedatipersonali.it/privacy-negli-usa#:~:text=Negli%20Usa%20non%20esiste%20una,tutelano%20la%20protezione%20dei%20dati.

Salerno. “Il Garante Sanziona l’Inps per 300.000 Euro, Il Controllore Dei Furbetti Del “Bonus Covid” Non Tratta in Modo Lecito I Dati Personali Raccolti,.” *Privacy E CYBERSECURITY*, 2021.

Salvi, “Google Analytics “Illegale” Secondo Il Garante Privacy: E Ora?” *Agenda Digitale*, 23 June 2022, www.agendadigitale.eu/sicurezza/privacy/google-analytics-illegale-secondo-il-garante-privacy-e-ora/.

Simone, *Enrico Caruso e il diritto alla riservatezza. Una difficile costruzione giuridica, Teoria e storia del diritto privato, 2021.* *https://www.teoriaestoriadeldirittoprivato.com/wp-content/uploads/2021/12/2021_Contributi_Simone.pdf*.

Surace, “Evoluzione Storico-Giuridica Del Diritto Alla Riservatezza.” *Www.adir.unifi.it*, 2005, www.adir.unifi.it/rivista/2005/surace/cap2.htm#162.

Valerini, “Le Novità Processuali in Materia Di Privacy Dopo Il Reg. 679/2016 (GDPR) E Il D.lgs. 101/2018.” 2018.

Viggiani, *Il Penumbral Reasoning Nella Giurisprudenza Nordamericana*. 2017, dialnet.unirioja.es/servlet/articulo?codigo=6896912.

“Violazione Della Privacy: Strumenti E Garante Della Privacy.” *Www.studiolegalelbmg.com*, 22 July 2022, www.studiolegalelbmg.com/violazione-della-privacy-strumenti-garante/.

GIURISPRUDENZA RILEVANTE

Corte di Giustizia. *Edizione Provvisoria SENTENZA DELLA CORTE (Terza Sezione) 4 maggio 2023 CGUE-C300-21*. 4 May 2023.

2000/520/CE Decisione della Commissione, 26 luglio 2000, notificata con il numero C (2000) 2441.

"Provvedimento Del 9 Giugno 2022 [9782890]." *Www.garanteprivacy.it*, 9 June 2022, www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9782890.

"Provvedimento Del 30 Marzo 2023 [9870832]." *Www.garanteprivacy.it*, 30 Mar. 2023, www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9870832.

"Provvedimento Dell." *Www.garanteprivacy.it*, 11 Apr. 2023, www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9874702.

"Provvedimento Del 25 Febbraio 2021 [9556958]." *Www.garanteprivacy.it*, 25 Feb. 2021, www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9556958.

Sentenza, Cassazione Civile, Sez. Prima, Pres. Bernabai, N. 2306, 5 febbraio 2016.

Sentenza Cassazione Civile, Sez Sest, Pres. Finocchiario, N. 18812, 5 settembre 2014.

Sentenza Corte costituzionale N. 13/2019, Decisione del 05/12/2018.

Sentenza della Corte di Giustizia 16 luglio 2020, causa C-311/18.

Sentenza della Corte di Giustizia (Grande Sezione), 31 maggio, 2005, nel procedimento C- 53/03.

Olmstead v. United States 277 U.S. 438 (1928).

Griswold v. Connecticut 381 U.S. 479 (1965).

Roe v. Wade 410 U.S. 113 (1973).

Katz v. United States 389 U.S. 347 (1967).

Cass. Civ. Sentenza n. 2129 27 maggio 1975, JStor, p. 2896 https://www.jstor.org/stable/23173994.

Sentenza n. 4735/2022 della XVIII sezione civile del Tribunale di Roma.

Corte di Cassazione, sez. Lavoro, sentenza n. 6775/2016.

Suprema Corte di Cassazione Sezione prima Civile, sentenza n. 26972, 11 febbraio 2008.

Corte suprema di Cassazione Sezione prima Civile, sentenza n. 2306, 5 febbraio 2016.

Sentenza della Corte di Giustizia Terza Sezione, causa C-300/21, 4 maggio 2023.

Suprema Corte di Cassazione Sezione seconda Civile, ordinanza n.29049/2022.

Provvedimento del Garante per la protezione dei dati personali n. 313/2014.

Tribunale dell'Aquila, sentenza n.355/2018.