UNIVERSITÀ DEGLI STUDI DI PADOVA

DIPARTIMENTO DI SCIENZE POLITICHE, GIURIDICHE E STUDI INTERNAZIONALI

Corso di laurea *Magistrale* in
Scienze del governo e Politiche pubbliche – Governo delle amministrazioni

IL TRATTAMENTO DEI DATI PERSONALI E GLI STRUMENTI DI RACCOLTA DEI DATI ONLINE: COOKIES E BIG DATA

Relatore: Prof. ARIANNA FUSARO

Laureando: MARCO SGOBBI
matricola N.1243535

A.A. 2021 - 2022

Indice

Introduzione

Il presente lavoro riguarda il tema del trattamento dei dati personali e della loro commercializzazione, intesa come scambio di un bene o servizio contro la prestazione del consenso al trattamento dei dati personali dell'utente.
Negli ultimi anni l'attenzione ai temi del trattamento dei dati personali e della loro sicurezza è cresciuta vertiginosamente. La tutela dei dati personali è diventata, oggi, un settore chiave per le aziende e per le amministrazioni.
Il dato personale è ormai diventato a tutti gli effetti il metro di misura di un servizio o di un prodotto, da qui nasce inevitabilmente l'esigenza di una regolamentazione a tutela dei diritti dei cittadini, e in particolare del diritto alla protezione dei dati personali (*data protection*).
Il tema è molto attuale, in quanto in tutta l'Unione Europea si è assistito ad un processo di evoluzione del quadro normativo.
Con l'entrata in vigore del più recente Regolamento UE 2016/79 meglio noto come GDPR (*General Data Protection Regulation*), divenuto applicabile dal 25 maggio 2018, è stata abrogata la precedente Direttiva 95/46/CE, dalla quale sono nate le Leggi in materia di privacy dei principali Stati Membri, tra cui anche il nostro D.lgs 196/2003 (Codice per la protezione dei dati personali).
Nel primo capitolo del presente lavoro si andrà ad esaminare, nelle sue parti più rilevanti, il Regolamento UE relativo alla protezione dei dati personali, si passerà poi ad analizzare il tema del consenso dell'interessato esaminando anche il principio di "*Accountability*".
Nel secondo capitolo si parlerà del mercato dei dati personali, ponendo l'attenzione in particolare sui contratti di fornitura di contenuti e servizi digitali, sulla profilazione dei dati e sul loro trattamento per finalità di *marketing*.
Nel terzo capitolo si analizzeranno i principali strumenti di raccolta dei dati personali, analizzando anche i rischi per la sicurezza dei dati online.
Nel quarto e ultimo capitolo l'attenzione sarà rivolta ad alcuni casi specifici, come il famoso "Scandalo di *Facebook - Cambridge Analytica*" e il caso

della famosa applicazione Faceapp, la quale nel 2019 è divenuta una delle più scaricate dagli store dei dispositivi mobili.

CAPITOLO I

IL TRATTAMENTO DEI DATI PERSONALI: IL REGOLAMENTO UE 679/2016

1.1 – Oggetto, finalità e ambito di applicazione materiale

Sebbene negli anni Novanta fosse già chiaro come il rispetto dei diritti fondamentali, fra cui il diritto alla privacy, fosse un caposaldo dell'Unione Europea, mancavano ancora disposizioni armoniche per tutti gli Stati membri in materia di trattamento di dati personali.

L'esistenza di un articolato sistema di principi fondamentali riguardanti la protezione della privacy portò il legislatore europeo all'adozione della direttiva 95/46/CE relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, entrata in vigore il 24 ottobre 1995.

Questa direttiva era rivolta a tutti gli Stati membri, i quali avrebbero dovuto dotarsi di legislazioni conformi entro il 31 dicembre 1996.

In Italia la direttiva è stata recepita con la legge n. 675 del 31/12/1996, la prima legge italiana in materia di protezione dei dati personali, che ha introdotto il principio per cui la riservatezza delle persone fisiche e giuridiche rappresenta un diritto assoluto ed inviolabile, meritevole di tutela attraverso la comminazione di sanzioni penali, civili e amministrative.

In particolare, gli obiettivi fondamentali di questa direttiva erano due: il primo riguardava la salvaguardia del diritto alla protezione dei dati personali, mentre il secondo era quello di garantire la libera circolazione dei dati personali fra gli Stati membri dell'Unione Europea, ovvero il cosiddetto "*free flow of data"*.

Come si può notare, lo strumento legislativo adottato dall'Unione Europea per disciplinare il settore della privacy è passato da una direttiva ad un regolamento. Questo perché, per sua stessa natura, la direttiva non garantisce uniformità nell'applicazione dei principi dettati dal legislatore europeo, mentre il regolamento sì.

Infatti, «*la direttiva vincola lo stato membro cui è rivolta per quanto riguarda il risultato da raggiungere, salva restando la competenza degli organi nazionali in merito alla forma e ai mezzi*»[1]. Ciò significa che, salva l'ipotesi di una direttiva dettagliata (o *self-executing*), si tratta di una fonte del diritto che si limita ad enunciare principi e criteri generali che vincolano lo Stato in relazione al solo risultato da perseguire; dunque, è un atto di mera "armonizzazione" delle normative nazionali.

In particolare, la direttiva 95/46/CE è stata decisiva per l'introduzione negli Stati membri di una disciplina a tutela della privacy, delineando un quadro normativo completo recepito negli ordinamenti nazionali, ma allo stesso tempo «*Non ha impedito la frammentazione dell'applicazione della protezione dei dati personali nel territorio dell'Unione, né ha eliminato l'incertezza giuridica o la percezione, largamente diffusa nel pubblico, che in particolare le operazioni online comportino rischi per la protezione delle persone fisiche*»[2].

Il regolamento invece, è definito nell'art 288 TFUE come un atto a portata generale, obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri. Ciò che distingue un regolamento da una direttiva è dunque l'immediata applicabilità negli ordinamenti nazionali, che non lascia alcun margine di discrezionalità agli stessi in ordine alla sua applicazione: le sue disposizioni sono vincolanti e precettive, applicabili anche in presenza di norme nazionali contrastanti, prevalendo su queste ultime. Il regolamento, quindi, è in grado di produrre effetti diretti all'interno degli ordinamenti statali, mentre nel caso della direttiva sono i provvedimenti di recepimento a produrre un effetto nell'ordinamento.

Il 4 maggio 2016 è stato pubblicato sulla Gazzetta Ufficiale dell'Unione Europea il Regolamento UE 2016/679, noto anche con l'acronimo inglese "GDPR" (General Data Protection Regulation).

Il GDPR è la nuova normativa relativa alla protezione dei dati personali che abroga la precedente direttiva 95/46/CE con l'obiettivo di uniformare

[1] Art 288 del Trattato sul funzionamento dell'Unione Europea del 13 dicembre 2007

[2] Considerando n.9 GDPR

definitivamente la regolamentazione in materia di protezione dei dati personali all'interno dell'Unione Europea.

Il Regolamento UE 2016/679 è entrato pienamente in vigore a decorrere dal 25 maggio 2018 e si può affermare che, da un lato, mette un freno alla confusione normativa generata per effetto della precedente direttiva 95/46/CE e, dall'altro lato, adegua la disciplina sul trattamento dei dati personali alle moderne tecnologie, rispondendo ad un'esigenza particolarmente avvertita soprattutto nell'era della globalizzazione che stiamo vivendo[3].

Negli ultimi anni, infatti, l'innovazione tecnologica e la globalizzazione hanno fatto sì che la raccolta e la successiva condivisione dei dati personali siano aumentate drasticamente, rendendo gli individui sempre più facilmente tracciabili.

A tal proposito, il Regolamento 2016/679 dichiara che: «*la tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività. Sempre più spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che le riguardano*»[4].

Successivamente, il Regolamento afferma anche che la tecnologia ha ormai trasformato l'economia e le relazioni sociali e dovrebbe essere in grado di favorire la libera circolazione dei dati personali all'interno dell'Unione, nonché il loro trasferimento verso paesi terzi e organizzazioni internazionali, garantendo in ogni caso un elevato livello di protezione dei dati personali.

Analizzando nello specifico il testo normativo, l'articolo 1, denominato "Oggetto e finalità" al comma 1 specifica che il Regolamento "stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati". Si può quindi osservare il duplice oggetto del Regolamento: protezione dei dati personali da un lato e libera circolazione degli stessi dall'altro. Questa protezione è espressamente qualificata come un diritto

[3] B. Locoratolo, "*Il Trattamento Dei Dati Personali e la Privacy*", (Napoli, Simone, 2021)

[4] Considerando n.6 GDPR

fondamentale, ai sensi dell'art. 8, par. 1 della Carta dei diritti fondamentali dell'UE e dell'art. 16, par. 1 del TFUE[5].

Tuttavia, il diritto alla protezione dei dati personali è un diritto distinto ed autonomo rispetto al diritto alla riservatezza (privacy) in quanto estende la tutela dell'individuo oltre la sfera privata e in particolar modo nelle relazioni sociali, garantendo così il controllo sulla circolazione dei propri dati e la possibilità per l'interessato di richiedere la loro cancellazione o rettifica[6].

Secondo buona parte della dottrina è possibile far risalire le origini del diritto alla privacy al 15 dicembre 1890, quando l'avvocato Samuel Warren e il Giudice Louis Brandeis pubblicarono un celebre articolo sulla famosa rivista accademica "*Harvard Law Review*", intitolato "*The Right to Privacy*"[7].

Nell'articolo in questione, il diritto alla privacy veniva definito come: *"Il diritto dell'individuo a decidere quali informazioni su sé stesso dovrebbero essere comunicate agli altri e in quali circostanze".*

Su questo filone si inserisce la definizione di un celebre giurista italiano, nonché primo garante della privacy nel nostro paese: Stefano Rodotà, il quale definisce il diritto alla privacy come: "*il diritto a mantenere il controllo delle proprie informazioni e di determinare le modalità della costruzione della propria sfera privata*"[8].

Il diritto fondamentale alla protezione dei dati di carattere personale non può essere, però, una prerogativa assoluta dell'individuo, ma deve essere considerato alla luce della sua funzione sociale e, soprattutto, deve essere contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità[9].

L'obiettivo primario del Regolamento è, dunque, quello di fornire un livello coerente ed elevato di protezione alle persone fisiche e di rimuovere gli ostacoli alla circolazione dei dati personali all'interno dell'UE.

---

[5] Considerando n.1 GDPR

[6] B. Saetta, "*Diritto alla protezione dei dati personali*", in *Protezionedatipersonali.it*, 2018

[7] F. Corona, "*Diritto alla riservatezza: riconoscimento ed evoluzione normativa*", in *Legaldesk.it*, 2018

[8] Data Protection Manager, "*Nascita del diritto alla Privacy e sua evoluzione come diritto alla riservatezza e alla protezione dei dati*", in *Privacymanager.eu*, 2021

[9] Considerando n.4 GDPR

Al fine di assicurare certezza del diritto e trasparenza agli operatori economici è necessario però che il livello di protezione sia equivalente in tutti gli Stati membri. In tale prospettiva, il Regolamento si propone di offrire alle persone fisiche, in tutti gli Stati membri, lo stesso livello di diritti azionabili nonché di obblighi e responsabilità per i titolari e i responsabili del trattamento.

Con riguardo alla portata applicativa delle norme regolamentari, gli articoli 2 e 3 del GDPR distinguono tra un ambito di applicazione materiale ed uno territoriale.

Innanzitutto, il Regolamento si applica solamente con riferimento alle persone fisiche viventi, in relazione al trattamento dei propri dati personali, a prescindere dalla loro nazionalità o dal luogo di residenza[10].

Inoltre, si applica sia al trattamento interamente o parzialmente automatizzato che al trattamento manuale dei dati personali[11], se questi ultimi sono contenuti o destinati ad essere contenuti in un archivio[12].

La protezione prevista dal Regolamento esclude dal suo campo di applicazione le persone fisiche decedute e le persone giuridiche. I dati personali di quest'ultime, infatti, sono disciplinate da altre normative che non saranno oggetto di analisi in questo elaborato.

Come dispone il par. 2 dell'art. 2, inoltre, le disposizioni del regolamento non si applicano: a questioni di tutela dei diritti e delle libertà fondamentali o di libera circolazione dei dati personali riferite ad attività che non rientrano nell'ambito di applicazione del diritto europeo (ad esempio le attività riguardanti la sicurezza nazionale); al trattamento dei dati personali effettuato dagli Stati membri nell'esercizio di attività relative alla politica estera e di sicurezza comune dell'Unione[13]; al trattamento di dati personali effettuato da una persona fisica nell'ambito di attività a carattere esclusivamente personale o domestico, e quindi senza una connessione

[10] Considerando n.14 GDPR

[11] Art. 2 GDPR, comma 1

[12] Un "archivio" è definito dal legislatore europeo come «qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico» (Art. 3 GDPR)

[13] Considerando n. 16 GDPR

con un'attività commerciale o professionale[14]; al trattamento effettuato dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse[15]. Infine, al trattamento dei dati personali da parte di Istituzioni, organi, uffici e agenzie dell'Unione si applica il Regolamento UE/2018/1725 che ha abrogato il precedente Regolamento (CE) n. 45/2001.

Dal punto di vista dell'applicazione territoriale, l'art. 3 del Regolamento richiama innanzitutto il principio di stabilimento: secondo tale criterio non ha rilevanza il luogo geografico in cui viene effettuato il trattamento ma bisogna verificare se nel territorio europeo sia presente, per mezzo di uno stabilimento, un titolare o un responsabile del trattamento e se il trattamento avvenga nell'ambito delle attività di quello stabilimento.

La nozione di stabilimento è contenuta nel considerando n.22 del GDPR, il quale afferma che «*lo stabilimento implica l'effettivo e reale svolgimento di attività nel quadro di un'organizzazione stabile. A tale riguardo, non è determinante la forma giuridica assunta, sia essa una succursale o una filiale dotata di personalità giuridica*»[16].

I dati, quindi, possono anche essere detenuti all'estero, purché il soggetto che li tratta sia stabilito nel territorio nazionale (si tratta del medesimo principio applicato dall'Agenzia delle Entrate italiana)[17].

L'art. 3 stabilisce, dunque, al par.1, che il Regolamento in questione si applica al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione.

[14] Considerando n. 18 GDPR
[15] Considerando n. 19 GDPR
[16] Considerando n. 22 GDPR
[17] B. Saetta, "*Competenza territoriale e principio di stabilimento*", in *Protezionedatipersonali.it*, 2022

Il successivo paragrafo 2 della norma, invece, completa la disciplina richiamando il principio della collocazione geografica dei soggetti interessati al trattamento.

In attuazione di tale principio, il regolamento si applica «*al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano:*

a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato;

b) *il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione*»[18].

Infine, la disposizione si chiude con l'ulteriore previsione che «*il Regolamento si applica al trattamento dei dati personali effettuato da un titolare del trattamento che non è stabilito nell'Unione, ma in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico*»[19].

1.2 - Il Dato Personale

La normativa sulla privacy si applica al trattamento dei dati personali delle persone fisiche. La prima questione da risolvere per la comprensione della disciplina vigente riguarda l'esatta individuazione del concetto di dato personale.

Riuscire a definire con esattezza cosa s'intenda con questo termine è un presupposto essenziale per comprendere quale sia l'ambito effettivo di estensione della tutela ad essi riconosciuta[20].

---

[18] Art. 3 GDPR par. 2

[19] Art. 3 GDPR par.3

[20] La nozione di dato personale è stata approfonditamente indagata in un corposo studio – "What are personal data?" – che la UK Information Commission ha nel 2004 commissionato all'Università di Sheffield al fine di favorire la comprensione della locuzione "dati personali" e contribuire a darne una definizione coerente e attendibile. La ricerca è stata condotta utilizzando più chiavi di lettura – giuridica, sociologica e psicologica – nonché attraverso un'indagine empirica su come il termine "dati personali" sia stato interpretato e applicato dalle autorità

Nel GDPR, il dato personale è definito come «*qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale*»[21].

Partendo dalla definizione giuridica, si può certamente affermare che i "dati personali" sono "informazioni"; una locuzione che, tuttavia, si presta a plurime interpretazioni, un termine dal significato ambiguo, multiforme, comunemente utilizzato, per esempio, tanto per far riferimento all'informazione come "contenuto", quanto al supporto materiale che immagazzina quel contenuto[22].

Per meglio comprendere quale sia il significato del termine '"informazione" richiamato dalla disciplina normativa in materia di privacy, può tornare utile la classificazione elaborata dall'autore Herbert Zech[23], il quale propone di distinguere tra informazioni semantiche, ovvero informazioni con un certo significato, informazioni sintattiche, ossia informazioni rappresentate da una certa quantità di segni, e informazioni strutturali, rappresentate dalla struttura di un oggetto fisico. "Ognuno dei tre tipi di informazioni" aggiunge l'autore "può essere trovato nella vita quotidiana: quando parliamo di una notizia, di una storia o del "contenuto" di un libro ci riferiamo al livello semantico, mentre con la composizione di un testo o di un file ci si riferisce al livello sintattico. Infine, quando abbiamo a che fare con un CD, o un libro stampato, ecc. ci riferiamo al livello strutturale. Naturalmente i tre livelli sono

preposte alla protezione dei dati nelle diverse giurisdizioni europee. Lo studio è reperibile sul sito https://www.frareg.com/cms/wp-content/ uploads/personal_data.pdf.

[21] Art. 4 GDPR, comma 1

[22] C. Irti, "*Dato personale, dato anonimo e crisi del modello normativo dell'identità*", in *Juscivile.it*, 2020

[23] H ZECH, Information us a property, 6 JIPITEC 192, par 1, 2015; ID., A legal framework for a data economy in the European Digital Single Market: rights to use data, Journal of Intellectual Property Law & Practice, vol. 11, n. 6, 2016, p. 460 ss.; ID. Data as a Tradeable Commodity, in AA. VV., European Contract Law and the Digital Single Market, edited by A. DE FRANCESCHI, Cambridge, Intersentia, 2016, p. 51 ss

collegati, in quanto il significato può essere contenuto all'interno di un testo e un testo può essere stampato. Così, lo strato fisico porta lo strato sintattico e lo strato sintattico lo strato semantico.

Una prima definizione di dati personali può essere, dunque, data da un punto di vista semantico, considerando come tali quelle informazioni che hanno un certo significato, le quali descrivono qualcosa (riferibile ad una persona fisica) a cui sia possibile dare un senso[24], a prescindere dallo strumento sintattico e dal supporto materiale utilizzato per esprimere e contenere l'informazione.

L'espressione "qualsiasi informazione" rappresenta la volontà del legislatore europeo di definire un concetto molto ampio di dati personali allo scopo di ottenerne un'interpretazione altrettanto estesa. È importante precisare che non è necessario che l'informazione sia di natura riservata o intima: anche alcune informazioni generalmente disponibili, come i dati pubblici, sono dati personali. Inoltre, perché l'informazione diventi un "dato personale" non è necessario che sia vera o dimostrata[25].

La dottrina qualifica il dato personale come un "bene giuridico di secondo grado", inquadrandolo come lo strumento tecnico-giuridico attraverso il quale i legislatori nazionali e comunitari tutelano l'insieme dei diritti collegati all'identità personale[26].

Analizzando la definizione all'articolo 4, è possibile distinguere i "dati personali" dai "dati identificativi" basandosi sulla possibilità e capacità di identificare il soggetto da cui provengono tali dati: i dati personali sono tutti quei dati che consentono di identificare la persona fisica sia in maniera diretta che in maniera indiretta, mentre i dati identificativi sono tutti quei dati che consentono di identificare la persona fisica solamente in maniera

[24] " Data is a description of something that allows it to be recorded, analyzed, and reorganized", così L. FLORIDI, 'Philosophical Conceptions of Information', in G. SOMMARUGa (edited by), Formal Theories of Information: From Shannon to Semantic Information Theory and General Concepts of Information, Springer, 2009, p. 13 ss

[25] M. Ravarotto, "*IL MERCATO DEI DATI PERSONALI. IN PARTICOLARE: IL CASO MEDIAWORLD*", 2019/2020, Dipartimento di Diritto Privato e Critica del diritto, Università Degli Studi di Padova

[26] B. Locoratolo, "*Il Trattamento Dei Dati Personali e la Privacy*" (Napoli, Simone, 2021), pag 46

diretta[27]. Si può quindi affermare che il dato identificativo non è che una "species" all'interno del "genus" principale[28].

Ad esempio, sono dati identificativi che permettono l'identificazione del soggetto cui si riferiscono, oltre al nome e al cognome (i quali sono identificatori immediati), l'indirizzo di casa o l'indirizzo e-mail, il numero di telefono o il numero di un documento (carta di identità, passaporto o patente di guida), oppure ancora la targa del proprio veicolo.

La questione dell'identificabilità di una persona, al fine di circoscrivere l'applicabilità delle norme, è affrontata anche nei considerando del GDPR. Innanzitutto, viene affermato che «Per stabilire l'identificabilità di una persona è opportuno considerare tutti i mezzi, come l'individuazione, di cui il titolare del trattamento o un terzo può ragionevolmente avvalersi per identificare detta persona fisica direttamente o indirettamente»[29].

In secondo luogo, si afferma che «*le persone fisiche possono essere associate a identificativi online prodotti dai dispositivi, dalle applicazioni, dagli strumenti e dai protocolli utilizzati, quali gli indirizzi IP, a marcatori temporanei (cookies) o a identificativi di altro tipo, come i tag di identificazione a radiofrequenza. Tali identificativi possono lasciare tracce che, in particolare se combinate con identificativi univoci e altre informazioni ricevute dai server, possono essere utilizzate per creare profili delle persone fisiche e identificarle*»[30].

A questo proposito, è interessante menzionare una famosa sentenza della Corte di Giustizia Europea: "Patrick Breyer contro la Repubblica Federale Tedesca" del 19 ottobre 2016[31], la quale esprime una precisazione importante in materia di protezione dei dati personali.

Nella fattispecie, la Repubblica Federale tedesca raccoglieva gli indirizzi IP degli utenti che navigavano i suoi siti governativi, e Breyer ha avviato una

---

[27] A. Amato, "*Dati "personali" e dati "identificativi": come distinguerli?*", in *Studioscicchitano.it*, 2019

[28] A. Careni, "*Dati personali e dati identificativi: differenze ed effetti derivanti dall'art. 13 Codice Privacy*", in *Mondodiritto.it*, 2021

[29] Considerando n. 26 GDPR

[30] Considerando n. 30 GDPR

[31] InfoCuria – Giurisprudenza, https://curia.europa.eu/juris/document/document.jsf?docid=184668&doclang=IT

causa contro la Germania chiedendo che fosse inibita tale raccolta, in considerazione del fatto che l'indirizzo IP (*Internet Protocol Address*) doveva ritenersi un dato personale. Di conseguenza, secondo Breyer, occorreva il consenso dell'utente per raccogliere e conservare l'IP.
La Germania si è difesa sostenendo che la raccolta dei dati (cioè nome del dominio, termini di ricerca, data e ora della sessione, volume di dati trasferiti e indirizzo IP del computer da cui l'utente navigava) avveniva con l'obiettivo di prevenire attacchi informatici e perseguire eventuali aggressori[32].
Un indirizzo IP è un indirizzo univoco che identifica un dispositivo su *Internet* o in una rete locale. IP è l'acronimo di "*Internet Protocol*", ovvero protocollo Internet, e costituisce l'insieme delle regole che disciplinano il formato dei dati scambiati su Internet o sulla rete locale.
In pratica un indirizzo IP è un identificatore che consente ai dispositivi di scambiarsi informazioni su una rete: può contenere informazioni sulla posizione e consentire l'accesso ai dispositivi per la comunicazione.
Gli indirizzi IP sono costituiti da serie di quattro numeri, ad esempio 192.158.1.38, ciascuno dei quali può variare da 0 a 255. Questi indirizzi non vengono assegnati in maniera casuale, bensì vengono generati matematicamente e allocati tramite la *Internet Assigned Numbers Authority* (IANA), una divisione di *Internet Corporation for Assigned Names and Numbers* (ICANN), la quale è un'organizzazione no-profit fondata negli Stati Uniti nel 1998, con lo scopo di garantire la sicurezza su Internet e renderla utilizzabile a tutti[33].
La Corte, nella fattispecie, si era soffermata sui cd. indirizzi IP "dinamici", individuati in quegli indirizzi temporanei per i dispositivi collegati a una rete che cambiano continuamente nel tempo[34] (la Corte puntualizzava la distinzione tra indirizzi IP dinamici e statici, i quali invece sono indirizzi che rimangono invariati e consentono l'identificazione permanente del dispositivo connesso alla rete).

[32] B. Saetta, "*L'indirizzo IP dinamico è dato personale*", in *Brunosaetta.it*, 2022
[33] Kaspersky, "*Che cos'è un indirizzo IP - Definizione e spiegazione*", in *Kaspersky.it*, 2022
[34] Kaila, "*Indirizzo IP dinamico*", in *Tecnologico.wiki*, 2022

Nella decisione della Corte veniva affermato che tale tipologia di indirizzo, pur non costituendo un'informazione riferita ad una persona fisica identificata (perché non consente di rivelare direttamente l'identità della persona fisica che utilizza il computer con il quale si accede al sito), rappresenta uno strumento per poter identificare indirettamente una persona (quindi ha rilevanza ai fini dell'identificabilità della persona), laddove l'indirizzo IP sia incrociato con informazioni aggiuntive di dati raccolti dal *provider*, cioè dal fornitore di accesso a Internet.

Sotto questo profilo, conclude la Corte, l'indirizzo IP dinamico deve ritenersi comunque un dato personale in quanto permette l'identificabilità dell'utente (intestatario del contratto di accesso) attraverso l'incrocio con i dati raccolti dal provider.

Dalla indicata nozione di dato personale appare evidente, dunque, l'intenzione del legislatore di assicurare una portata ampia alla normativa, facendo rientrare nella definizione di dato qualunque informazione il cui utilizzo può portare all'identificazione, anche indiretta, di un soggetto.

Entrando nel dettaglio della definizione di dato personale, nel GDPR non è considerato come tale il "dato anonimo", ossia quel dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile[35]. Il legislatore europeo, non considerandolo come dato personale, sottrae il dato anonimo dall'ambito di applicazione materiale della normativa sulla protezione dei dati personali. A questo proposito, il considerando n. 26 del GDPR prevede che «*I principi di protezione dei dati non dovrebbero pertanto applicarsi a informazioni anonime, vale a dire informazioni che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato. Il*

[35] Legge 675/96, art. 2 e Codice Privacy (D.lgs 196/2003) art. 4, abrogato dal D.lgs 101/2018. Ad oggi si ritengono valide per il diritto interno le definizioni fornite dall'art. 4 del GDPR. Tali definizioni non contemplano i "dati anonimi" né la "anonimizzazione", così oggi ci ritroviamo senza una nozione formale di questi concetti.

presente regolamento non si applica pertanto al trattamento di tali informazioni anonime, anche per finalità statistiche o di ricerca»[36].

Diversamente dal dato anonimo, che non è considerato dato personale, viene considerato come tale il dato pseudonimo, il quale viene dunque sottoposto alla normativa sul trattamento dei dati personali.

Il Regolamento 2016/679 reca un glossario all'art. 4 ove è puntualmente definita la "pseudonimizzazione" come «*il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile*»[37][38].

Ciò significa che l'uso di "informazioni aggiuntive" può portare all'identificazione degli individui, motivo per cui i dati pseudonimi sono classificati come dati personali.

Dalla lettera dell'art. 4 citato si ricavano, dunque, importanti principi per un corretto ricorso alla pseudonimizzazione dei dati personali. Innanzitutto, è necessario che non sia possibile l'identificabilità diretta del soggetto interessato.

È importante sottolineare che «*l'applicazione della pseudonimizzazione ai dati personali può ridurre i rischi per gli interessati e aiutare i titolari del trattamento e i responsabili del trattamento a rispettare i loro obblighi di protezione dei dati*»[39]. La pseudonimizzazione però, pur essendo di per sé una misura di protezione dei dati personali, necessita della predisposizione di ulteriori misure di sicurezza, tecniche ed organizzative per far sì che le informazioni aggiuntive siano conservate separatamente e che i dati personali non siano attribuiti ad una persona fisica identificata o identificabile.

---

[36] Considerando n. 26 GDPR

[37] M. Massimini, "*Anonimizzazione dei dati personali: significato, benefici e dubbi in ottica GDPR*", in *Privacy.it*, 11/05/2021

[38] Art. 4, par. 1, n. 5, GDPR

[39] Considerando n. 28 GDPR

Tale impostazione è confermata anche da altre disposizioni del Regolamento stesso: da un lato è previsto che l'introduzione esplicita della pseudonimizzazione non è intesa a precludere altre misure di protezione dei dati[40]; dall'altro lato, la pseudonimizzazione è inclusa tra le misure tecniche ed organizzative necessarie per garantire un livello di sicurezza del trattamento adeguato al rischio, di cui all'art. 32 GDPR, lett. a).

1.3– Il Trattamento dei dati e i principi applicabili

Il Regolamento disciplina all'art. 4 comma 2 la nozione di trattamento: si parla di trattamento dei dati personali riferendosi a «*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*»[41].

Facendo un'analisi più approfondita della definizione di cui all'art. 4, è necessario chiarire che la raccolta dei dati consiste nell'attività di acquisizione del dato ed è la prima operazione che generalmente rappresenta l'inizio del trattamento; la registrazione consiste nella memorizzazione dei dati su un qualsiasi supporto; l'organizzazione consiste nella classificazione dei dati secondo un metodo prescelto; la conservazione consiste nel mantenere memorizzate le informazioni su un qualsiasi supporto; la consultazione è la lettura dei dati personali. Fondamentale poi è la differenza tra comunicazione e diffusione: la comunicazione consiste nella cessione di dati personali ad uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati. In caso di comunicazione il dato viene trasferito a terzi.

[40] Considerando n. 28 GDPR
[41] Art. 4 GDPR comma 2

Per diffusione, invece, si intende l'azione di fornire i propri dati a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione. Si ha, quindi, diffusione anche quando si pubblica online, ad esempio una fotografia in un qualsiasi social network. In assenza di consenso, l'attività di diffusione deve ritenersi illecita[42].

La precedente impostazione del nostro Codice della privacy era improntata su una diversa disciplina a seconda del soggetto che effettuava il trattamento. In particolare, si distinguevano "regole generali", applicabili a tutti i tipi di trattamento, le quali dovevano essere rispettate da qualsiasi titolare, pubblico o privato che fosse[43]; regole ulteriori e specifiche per i soggetti pubblici[44], nonché per i soggetti privati e gli enti pubblici economici[45].

Le modifiche apportate col il D. lgs 101/2018 rispondono ad una diversa impostazione della disciplina, che non si basa più sulla natura pubblica o privata del soggetto che opera il trattamento, ma è incentrata unicamente sulla finalità perseguita con il trattamento, vale a dire la sua attinenza o meno con un interesse pubblico. Quindi, se il Codice della privacy "ante riforma" del 2018 legiferava anche sulla P.A., dettando una disciplina specifica, il decreto del 2018 ha letteralmente eliminato tutte le norme di riferimento (artt. da 18 a 22) ed ha introdotto una disciplina sul trattamento dei dati personali per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri attraverso il nuovo art. 2 ter del D. lgs 196/2003[4647].

---

[42] B. Saetta, "*Trattamento dei dati personali*", in *Protezionedatipersonali.it – Brunosaetta.it*, 2021

[43] D. lgs 196/2003, Capo I, Titolo III, artt. Da 11 a 17; https://web.camera.it/parlam/leggi/deleghe/Testi/03196dl.htm#1

[44] D. lgs 196/2003, Capo II, artt. Da 18 a 22

[45] D. lgs 196/2003, Capo III, artt. Da 23 a 27

[46] B. Locoratolo, "*Il Trattamento Dei Dati Personali e la Privacy*" (Napoli, Simone, 2021), pag. 52-53

[47] Art. 2-ter Nuovo Codice Privacy – D.lgs 196/2003 aggiornato al D.lgs 101/2018, in *Cyberlaws.it*, 2022, https://www.cyberlaws.it/2018/articolo-2-ter-nuovo-codice-privacy-d-lgs-196-2003-base-giuridica/

Il Regolamento stabilisce le condizioni di liceità all'art.6 par. 1 e dispone che il trattamento è lecito solo se e nella misura in cui ricorra almeno una delle condizioni indicate:

a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità.

La prestazione del consenso è la più ovvia delle condizioni, considerato che è proprio l'interessato che autorizza il trattamento dei propri dati personali per le finalità indicate. Il consenso, oggetto dei prossimi paragrafi, deve essere libero, specifico, informato e inequivocabile[48]; per i minori il consenso è valido a partire dai 16 anni, anche se l'Ue dà la possibilità agli Stati membri di modificare questo limite al ribasso, purché non lo si collochi al di sotto dei 13 anni[49].

b) Il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso.

Ad esempio, si può pensare ai casi in cui per l'avvio di trattative finalizzate alla stipula di un contratto sia necessario inviare un preventivo, oppure in sede di esecuzione di un contratto già stipulato sia necessario compilare schede di intervento tecnico per assistenza contenente dati specifici (come i dati catastali) o trasmettere fatture e note di accredito. In questi casi, il conferimento dei dati è obbligatorio, in quanto in mancanza di essi non sarebbe possibile per il contraente smaltire le istanze precontrattuali e contrattuali, come la fornitura di un servizio, ovvero eseguire il contratto stipulato con l'interessato[50].

Inoltre, vale la pena richiamare le "*Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects – version for public consultation*" che, benché riferite ad uno specifico ambito di utilizzo, forniscono chiare e precise indicazioni generale sulla liceità del trattamento a norma dell'art. 6 comma b) del GDPR. All'interno delle stesse, si evince come, affinché il

[48] F. Corona, "*Consenso privacy: le nuove regole del GDPR*", in *Legaldesk.it*, 2022.
[49] G.C. Arija, "*Consenso Privacy Minorenni: chi lo dà?*", in *Laleggepertutti.it*, 2019
[50] B. Locoratolo, "*Il trattamento dei dati personali e la privacy*", (Napoli, Simone, 2021), pag. 54

Data Controller basi correttamente il trattamento sull'esecuzione di un contratto o di misure precontrattuale dovrà dimostrare: l'esistenza e la validità di tale contratto e/o delle misure precontrattuali sulla base della normativa applicabile, e che il trattamento dei dati forniti dall'interessato sia oggettivamente necessario per l'esecuzione di quel contratto o di quelle misure precontrattuali[51].

c) Il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;

Si pensi, ad esempio, all'obbligo per le banche di adempiere agli obblighi di legge in ambito fiscale, contabile e alle norme antiriciclaggio e antifrode, mediante la trasmissione dei dati.

È opportuno puntualizzare che il trattamento effettuato in conformità a un obbligo legale al quale il titolare del trattamento è soggetto, è lecito anche senza il consenso dell'interessato.

d) Il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;

Il considerando n. 46 del GDPR chiarisce che il ricorso a tale base giuridica può essere invocata solo se nessuna delle altre condizioni di liceità può trovare applicazione: «Il trattamento di dati personali dovrebbe essere altresì considerato lecito quando è necessario per proteggere un interesse essenziale per la vita dell'interessato o di un'altra persona fisica. Il trattamento di dati personali fondato sull'interesse vitale di un'altra persona fisica dovrebbe avere luogo in principio unicamente quando il trattamento non può essere manifestamente fondato su un'altra base giuridica. Alcuni tipi di trattamento dei dati personali possono rispondere sia a rilevanti motivi di interesse pubblico sia agli interessi vitali dell'interessato, per esempio se il trattamento è necessario a fini umanitari, tra l'altro per tenere sotto controllo l'evoluzione di epidemie e la loro diffusione o in casi di emergenze umanitarie, in particolare in casi di catastrofi di origine naturale e umana»[52].

---

[51] M. Cassaro, "*Basi di liceità del trattamento, come scegliere ed essere compliant al GDPR*", in *Cybersecurity360.it*, 2022

[52] Considerando n. 46 GDPR

e) Il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.

Tale previsione conferma la circostanza della diversa impostazione della normativa sul trattamento dei dati personali rispetto al passato: il legislatore europeo, con il regolamento, ha abbandonato la vecchia distinzione basata sulla natura pubblica o privata dei soggetti che trattano i dati ed ha optato per una disciplina fondata esclusivamente sulla finalità perseguita con il trattamento, a seconda che riguardi un interesse pubblico o privato. In merito rilevano l'art. 2 ter del nostro Codice, che contiene previsioni in merito alla base giuridica per il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri[53], e il successivo art. 2 sexies relativo al trattamento di categorie particolari di dati necessario per motivi di interesse pubblico rilevante[54].

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

Innanzitutto, la lettera f) non si applica al trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti.

Il legittimo interesse rappresenta quella relazione equilibrata, pertinente ed appropriata esistente tra l'interessato ed il titolare del trattamento[55].

Questa condizione di liceità è quella che maggiormente esprime il cd. principio di responsabilizzazione (accountability) di chi effettua il trattamento.

Infine, il legittimo interesse può essere validamente utilizzato per giustificare l'introduzione di misure di sicurezza che il titolare deve implementare ex art. 32 del GDPR che determinano un trattamento dei dati personali non

[53] D.lgs. 30 giugno 2003, n. 196, PARTE I, Titolo I, Capo II, art 2 ter
[54] D.lgs. 30 giugno 2003, n. 196, PARTE I, Titolo I, Capo II, art 2 sexies
[55] Considerando n. 47 GDPR

fondabile su diversa condizione di liceità. Come, ad esempio, così come precisato dal Considerando 49, «il trattamento di dati personali relativi al traffico, in misura strettamente necessaria e proporzionata per garantire la sicurezza delle reti e dell'informazione, vale a dire la capacità di una rete o di un sistema d'informazione di resistere, a un dato livello di sicurezza, a eventi imprevisti o atti illeciti o dolosi che compromettano la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati personali conservati o trasmessi e la sicurezza dei relativi servizi offerti o resi accessibili tramite tali reti e sistemi da autorità pubbliche ecc»[56].

Il successivo par. 3 dell'art. 6 del GDPR stabilisce che la base giuridica su cui si fonda il trattamento dei dati di cui alle precedenti lettere c) ed e) del paragrafo 1 – ossia quando il trattamento è necessario per adempiere un obbligo legale del titolare e quando è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri – deve essere stabilita dal diritto dell'Unione o dal diritto dello Stato membro cui è soggetto il titolare del trattamento. La base giuridica è ciò che autorizza legalmente il trattamento, così soddisfacendo il principio di liceità. In assenza di una base legale il trattamento è illecito[57]. La finalità del trattamento è determinata in relazione a tale base giuridica oppure, relativamente all'ipotesi di cui alla lettera e), deve essere necessaria per l'esecuzione di un compito svolto nel pubblico interesse o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento. La base giuridica deve essere indicata nell'informativa rivolta agli utenti. Inoltre, è utile documentare la scelta della base giuridica, e menzionarla nel registro dei trattamenti.

Il Regolamento europeo contiene poi una precisa indicazione dei principi che devono essere applicati al trattamento dei dati personali. I dati personali, ai sensi dell'art. 5 del GDPR sono:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);

[56] Considerando n. 49 GDPR

[57] B. Saetta, "*Base giuridica del trattamento dei dati*", in *Protezionedatipersonali.it*, 2022

b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità iniziali («limitazione della finalità»);
c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»); la minimizzazione comporta che vengano raccolti solo dati pertinenti, quindi limitando il trattamento a ciò che è realmente necessario e indispensabile rispetto alla finalità alla quale sono destinati[58]. Nel caso in cui sia possibile utilizzare dati anonimizzati o pseudonimizzati per il raggiungimento dell'obiettivo, si dovrebbe evitare del tutto l'utilizzo dei dati personali[59]. La minimizzazione dei dati deve inoltre essere prevista fin dalla progettazione del trattamento[60].
d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);
e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati («limitazione della conservazione»);
f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

Analizzando l'art.5, innanzitutto si può affermare che il trattamento del dato personale deve essere lecito. Da qui si introduce il principio di liceità del trattamento, il quale stabilisce che i dati personali devono essere trattati nel rispetto delle leggi. Il trattamento deve basarsi su una disposizione del diritto

[58] I. Todaro, "*Dati anonimi, pseudonimi, e minimizzazione*", in *Sinergetica.it*, 2018
[59] B. Saetta, "*Qualità dei Dati*", in *Protezionedatipersonali.it*, 2022
[60] Art. 25 GDPR – B. Saetta "*Privacy By Design e By Default*", in *Protezionedatipersonali.it*, 2022

nazionale, quindi non solo con riferimento alla normativa di settore (protezione dei dati personali) ma a tutte le norme vigenti (es. Codice civile, Statuto dei lavoratori, ecc.).

La legge deve essere accessibile alle persone interessate e prevedibile quanto ai suoi effetti. Una norma è "prevedibile" se è formulata in maniera da consentire all'interessato di regolare il proprio comportamento[61].

Procedendo con l'analisi dei principi applicabili al trattamento dei dati, il principio di correttezza stabilisce che le modalità di raccolta e di utilizzo dei dati devono essere corrette, così come lo stesso trattamento dei dati in tutti i suoi aspetti. In particolare, questo principio richiede che i dati personali non siano trattati in modo pregiudizievole, discriminatorio, imprevisto o fuorviante per l'interessato[62]. Il principio di correttezza va a sostituire il principio di lealtà contenuto nella vecchia normativa, nella quale si dava rilevanza al rapporto tra il titolare e l'interessato. Oggi l'impegno non è più soltanto con l'interessato, ma con l'intera società nella quale tutti noi viviamo, per cui il trattamento deve essere corretto, in modo da garantire all'intera collettività che il trattamento non ponga a rischio i dati personali.

Infine, la trasparenza è il terzo elemento che completa i requisiti indispensabili del trattamento. Quello della trasparenza non è solo un principio fondamentale del trattamento, ma anche un vero e proprio diritto dell'interessato. Il suo scopo è di alimentare la fiducia dei cittadini nell'economia digitale, e deve essere inteso quale «obbligo di rendere conoscibili le modalità con cui i dati sono raccolti, utilizzati e consultati grazie ad informazioni e comunicazioni facilmente accessibili e comprensibili, utilizzando un linguaggio semplice e chiaro. Tale principio riguarda, in particolare, l'informazione degli interessati sull'identità del titolare del trattamento e sulle finalità del trattamento e ulteriori informazioni per assicurare un trattamento corretto e trasparente con riguardo alle persone fisiche interessate e ai loro diritti di ottenere conferma e comunicazione di un trattamento di dati personali che li riguardano»[63].

---

[61] B. Saetta, "*Liceità del trattamento*", in *Protezionedatipersonali.it*, 2022

[62] B. Saetta, "*Correttezza e trasparenza del trattamento*", in *Protezionedatipersonali.it*, 2022

[63] Considerando n. 39 GDPR

Per capire bene l'innovazione data dal principio di trasparenza nel trattamento dati con il GDPR, occorre partire dall'art.5, paragrafo 1, lettera a) che, indicando i principi applicabili al trattamento, specifica che i dati personali devono essere trattati in modo lecito, corretto e trasparente. L'art. 6 della Direttiva 95/46 si limitava invece a dire, al paragrafo 1 lettera a), che i dati personali devono essere trattati "lealmente e lecitamente". È evidente la discontinuità tra il nuovo Regolamento e il sistema precedente, soprattutto perché ora la trasparenza diventa un aspetto generale ed essenziale di ogni trattamento di dati personali. Una condizione, dunque, che si applica ai trattamenti in quanto tali e durante tutto il loro corso, indipendentemente dal rapporto che possa sussistere tra il titolare e la tutela dei diritti degli interessati i cui dati sono oggetto di trattamento.
Un primo punto assolutamente essenziale nel quadro del GDPR è dunque che tanto i titolari (*controllers*) quanto i responsabili (*processors*) devono assicurare che i trattamenti o le parti di trattamento da ciascuno attuati risponda al principio di trasparenza[64].
Sempre nel considerando n. 39 del GDPR, si può notare come sia riconducibile a tale principio l'esigenza di sensibilizzare e proteggere le persone con riferimento «ai rischi, alle norme, alle garanzie e ai diritti relativi al trattamento dei dati personali, nonché alle modalità di esercizio dei loro diritti relativi a tale trattamento»[65].

1.4 - Il Principio di Accountability

Nel GDPR il legislatore europeo ha adottato un approccio normativo alla figura del titolare del trattamento, discostandosi dalle impostazioni tradizionali: nel Regolamento, infatti, non vi è un'elencazione delle attività che deve porre in essere il titolare, rimettendo queste alla sua discrezionalità, ma la disciplina si incentra sulla responsabilità del titolare: l'accountability (o responsabilizzazione)[66].

---

[64] F. Pizzetti, "*Trasparenza nel trattamento dati, che cambia col GDPR: l'alba di un nuovo valore sociale*", in *Agendadigitale.eu*, 2022
[65] Considerando n. 39 GDPR
[66] B. Locoratolo, "*Il Trattamento Dei Dati Personali e la Privacy*" (Napoli, Simone, 2021), pag. 104

Si deve tenere presente che il termine “accountability” ha origini anglosassoni e la sua traduzione con il termine “responsabilizzazione” non è del tutto corretta. La sua traduzione lessicale significa “essere in grado di dar conto” e nel contesto del GDPR riguarda il saper rispondere e dare conto dei risultati ottenuti o di quanto sia stato fatto in merito al trattamento dei dati personali[67].

Tuttavia, il termine “responsabilizzazione” è sembrato quello che potesse rispecchiare al meglio l’essenza di questo principio, con il quale, da un lato, si richiede al titolare del trattamento di introdurre misure tecnico e organizzative conformi alla normativa privacy, e dall’altro vi è anche l’onere di dimostrare quanto messo in atto.

Infatti, con la responsabilizzazione del titolare del trattamento, si richiede non solo il rispetto degli obblighi iniziali previsti nel Regolamento, ma anche una continua attività di controllo e verifica delle proprie attività di trattamento[68].

L’accountability include aspetti quali l’affidabilità e la competenza aziendale nella gestione dei dati personali ed è stata oggetto di particolari attenzioni fin dalla trentaduesima Conferenza Internazionale sulla Protezione dei Dati Personali che si tenne a Gerusalemme nell’ottobre 2010[69]; in quell’occasione furono trattati temi particolarmente innovativi tra cui i Social Networks, la Privacy by Design, il diritto all’oblio digitale e, appunto, l’accountability che rappresentò la vera novità. Essa fu originariamente elaborata per favorire il flusso di dati personali a livello internazionale ma può senza dubbi avere un’applicazione più ampia, rappresentando un più generale paradigma nel trattamento dei dati personali.

Noi oggi viviamo in un sistema articolato e complesso, nel quale è necessario adeguare le esigenze di una moltitudine di soggetti che operano quotidianamente nel tessuto socioeconomico. A questo proposito, è stata avvertita fin dal primo momento l’esigenza di poter contare su un impianto

[67] Impresoft, “*Principio di accountability e GDPR: facciamo chiarezza*”, in *blog.impresoftgroup.com*, 2020

[68] F. Corona, “*Principio di accountability: pilastro del nuovo GDPR*”, in *Legaldesk.it*, 2018

[69] M. Iaselli, “*Il principio di accountability: uno dei pilastri del GDPR*”, in *Altalex.it*, 2018

normativo che consentisse l'utilizzo di dati di varia natura al fine di generare flussi utili allo sviluppo di un'economia sovranazionale. Questa necessità, tuttavia, si è scontrata con un dato di fatto che in qualche modo ne limitava notevolmente le capacità espansive, ossia la presenza di legislazioni nazionali diversificate che ponevano notevoli problemi di bilanciamento, anche dal punto di vista dell'Unione Europea.

L'accountability in particolare affianca ad un profilo meramente giuridico una dimensione amministrativa ed etica che promuove un decisionismo responsabile che sia in grado di promuovere un dialogo rispettoso della legalità e della capacità di rispettare il principio di trasparenza, inteso in questo caso come la capacità di accedere ai propri dati e verificare quale sia la sorte designata dal titolare del trattamento. L'accountability, quindi, si impone come strumento per l'attuazione di meccanismi pratici in un contesto in cui l'adempimento degli obblighi legali e la garanzia di un'assistenza adeguata diventano indici virtuosi della tutela dei dati.

In particolare, il concetto di accountability è espresso chiaramente nell'art. 5 del GDPR. La norma, dopo aver elencato, al par. 1 i principi applicabili al trattamento dei dati affinché lo stesso sia legittimo, al successivo par. 2 aggiunge: «Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»)»[70].

Tale previsione generale viene specificata all'art. 24 del GDPR, dove il concetto di accountability viene esplicitato nell'obbligo del titolare di mettere in atto misure tecniche ed organizzative adeguate, per garantire ed essere in grado di dimostrare che il trattamento è effettuato conformemente alla normativa europea.

A tali previsioni corrisponde il considerando n. 74, nel quale viene precisata la responsabilità generale del titolare del trattamento «per qualsiasi trattamento di dati personali che quest'ultimo abbia effettuato direttamente o che altri abbiano effettuato per suo conto»[71].

[70] Art. 5 GDPR, par. 2

[71] Considerando n. 74 GDPR

Le misure tecniche ed organizzative che il titolare ritiene adeguate per la propria organizzazione, le quali possono essere riesaminate e aggiornate, sono adottate in virtù «della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche»[72]. La loro adozione, dunque, è rimessa ad una decisione discrezionale del titolare ed è basata su un'autovalutazione che lo stesso titolare deve compiere nei confronti della validità del proprio sistema di privacy, al fine di renderlo idoneo a garantire la sicurezza dell'interessato e, allo stesso tempo, ad esonerarlo da future responsabilità.

Tale impostazione normativa è la risultante di un approccio positivo e proattivo alla responsabilizzazione del titolare, nel senso che diviene fondamentale programmare a priori quante più misure possibili per evitare un danno futuro, anche attraverso l'elaborazione di modelli organizzativi molto soggettivi[73]. Il legislatore si pone, dunque, in un'ottica di prevenzione e non di reazione, nel senso che una buona programmazione effettuata ex ante riduce di molto i rischi di insorgenza di danni futuri e dunque influisce sull'eventuale responsabilità dello stesso. Tutto ciò significa che il titolare del trattamento dovrà sempre essere in grado di dimostrare di aver fatto tutto il possibile per realizzare un sistema di privacy sicuro per la tutela dell'interessato[74].

La necessità di dar conto a terzi dell'attività svolta, delle risorse impiegate e degli obiettivi perseguiti rappresenta oggi una prerogativa tipica delle Pubbliche Amministrazioni, il cui operato appare sempre più come se fosse messo alla prova da parte dei cosiddetti "stakeholder". Proprio con riguardo alle attività tipiche delle P.A., oggi, si ritiene necessario garantire alla cittadinanza che accede quotidianamente alle procedure amministrative e all'erogazione dei servizi locali una maggiore trasparenza. Proprio la trasparenza costituisce un indicatore fondamentale per valutare i servizi di

[72] Art. 24 GDPR, comma 1

[73] Datalog, "*GDPR PRIVACY: IL PRINCIPIO DI ACCOUNTABILITY O RESPONSABILIZZAZIONE*", in *Datalog.it*, 2018

[74] B. Locoratolo, "*Il Trattamento Dei Dati Personali e la Privacy*" (Napoli, Simone, 2021), pag. 105

pubblica utilità e il grado di efficienza degli organismi impegnati nel fornirli. L'efficacia di un servizio e la valutazione dello stesso passa necessariamente attraverso la trasparenza delle informazioni fornite ai cittadini che usufruiscono di quel servizio, della trasparenza delle procedure per accedervi e delle informazioni fornite in tutte le fasi del procedimento.
Secondo i maggiori organismi internazionali, l'accountability si comporrebbe di almeno tre elementi, i cosiddetti "pilastri":

- Trasparenza: questo principio si traduce in una completa accessibilità alle informazioni, in primo luogo per i cittadini, anche in qualità di utenti del servizio. La trasparenza include la predisposizione di strumenti volti a rendere più visibili decisioni, azioni, performance e risultati delle amministrazioni e l'allargamento della governance degli enti e dei servizi pubblici locali alla partecipazione delle organizzazioni dei cittadini e dei consumatori;
- Responsività: consiste nella capacità di rendere conto di scelte, comportamenti e azioni e di rispondere alle questioni poste dagli stakeholders. Ciò significa che le istituzioni devono rispondere in modo pubblico, coerente e dimostrabile alle richieste dei cittadini-consumatori, verificare la tracciabilità dell'azione amministrativa, valutarla a partire dal punto di vista civico e garantire una capacità di influenza della popolazione sulle modalità di gestione dei servizi pubblici;
- Compliance: ossia sviluppare la capacità di far rispettare le norme sia nel senso di mantenere l'azione pubblica nell'alveo tracciato dalle leggi, sia nel senso di far osservare le regole di comportamento agli operatori della Pubblica Amministrazione. Compliance, quindi, si riferisce al rispetto delle norme ed è intesa sia come garanzia della legittimità dell'azione che come adeguamento dell'azione stessa agli standard qualitativi e di appropriatezza definiti dalle leggi e dai regolamenti o dagli impegni assunti volontariamente per mezzo di linee guida etiche o codici di condotta. Pertanto, sotto questo profilo,

l'accountability potrebbe essere definita come "l'obbligo di spiegare e giustificare il proprio comportamento"[75].

È possibile rinvenire una particolare applicazione del concetto di accountability nel settore della sicurezza informatica. In questo settore, infatti, l'accountability può essere intesa come la capacità di un sistema di identificare ogni singolo utente e determinarne le azioni e il comportamento all'interno del sistema stesso grazie al supporto dell'audit delle tracce e di un sistema di autenticazione (*login*).

In generale si deve però ritenere che l'accountability rappresenti un aspetto del controllo di accesso che si basa sulla concezione che gli individui siano responsabili per le proprie azioni all'interno del sistema e che debbano, appunto, renderne conto ai terzi che ne facciano richiesta.

In quest'ottica, spicca la figura dell'*Accountability Project*, che mira a sviluppare strumenti che possano essere utilizzati dalle organizzazioni per valutare lo stato della propria *accountability* e dimostrarlo alle Autorità Garanti per la protezione dei dati personali qualora dovessero essere chiamate in causa.

1.5 - Il Consenso dell'interessato

In un'ottica di maggiore attenzione per l'individuo, il GDPR individua e disciplina i diritti che spettano all'interessato negli artt. che vanno da 15 a 22, ossia alla persona fisica identificata o identificabile la quale è titolare dei dati.

In quanto titolare dei dati da trattare, il primo e più importante diritto della persona fisica è quello di conoscere il trattamento che verrà effettuato sui propri dati personali e decidere se prestare il proprio consenso al trattamento di tali dati[76].

Il consenso è una delle basi giuridiche previste dal legislatore affinché il trattamento dei dati sia lecito e, provenendo direttamente dal soggetto

[75] M. Iaselli, "*Accountability*", in *Altalex.com*, 2018

[76] B. Locoratolo, "*Il Trattamento Dei Dati Personali e la Privacy*" (Napoli, Simone, 2021), pag. 77

titolare dei dati da trattare, rappresenta sotto alcuni aspetti la base che maggiormente fornisce garanzie di certezza al titolare del trattamento.

Il consenso viene definito dal GDPR come qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento[77].

A questo proposito, è interessante menzionare il considerando n. 32 del GDPR, in quanto esamina le modalità in cui può essere prestato il consenso. Esso specifica che «*Il consenso dovrebbe essere espresso mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano, ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale […] Se il consenso dell'interessato è richiesto attraverso mezzi elettronici, la richiesta deve essere chiara, concisa e non interferire immotivatamente con il servizio per il quale il consenso è espresso*»[78].

Se, dunque, è necessario che il consenso dell'interessato sia sempre espresso attraverso un atto inequivocabile, nel senso che non deve suscitare alcun dubbio relativamente alla volontà del soggetto di acconsentire al trattamento, esso non deve essere necessariamente prestato con una dichiarazione scritta. Tale affermazione non ha valore nel caso in cui vi sia il trattamento di particolari categorie di dati personali, per i quali l'art. 9 del GDPR richiede il cd. consenso esplicito dell'interessato[79], e in caso di sottoposizione a processi decisionali automatizzati (come la profilazione), i quali sono possibili proprio qualora la decisione si basi sul consenso esplicito dell'interessato[80].

Il GDPR prevede che qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato

[77] Art. 4, comma 1, n. 11, GDPR
[78] Considerando n. 32 GDPR
[79] Art. 9, par. 1 GDPR
[80] Art. 22 GDPR, par. 2, lettera c

ha espresso il proprio consenso al trattamento dei propri dati personali; l'onere della prova, dunque, ricade sul titolare del trattamento[81].

Procedendo nell'analisi dell'art. 7 del GDPR, si possono elencare le altre caratteristiche del consenso: innanzitutto, il consenso deve essere libero, nel senso che l'interessato deve poter acconsentire liberamente al trattamento dei dati, compiendo una scelta reale e non condizionata o limitata[82], senza che il negato consenso comporti conseguenze negative. Nello specifico «nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto»[83].

Poi, il consenso deve essere specifico: le richieste di consenso devono essere differenziate per ogni obiettivo del trattamento dei dati[84]. Per esempio, se fornisco il mio indirizzo e-mail per ricevere la conferma sull'ordine che ho effettuato con un acquisto online e l'azienda vuole utilizzare la mia e-mail per inviarmi offerte promozionali, sarà necessario che l'azienda in questione distingua i due consensi.

Il consenso deve inoltre essere informato, ciò significa che il titolare del trattamento ha l'obbligo di fornire all'interessato, ancor prima che avvenga la raccolta dei suoi dati, la cd. informativa, la quale deve contenere tutte le informazioni che permettono all'interessato di effettuare una scelta consapevole e di comprendere perché, in che modo, dove e per quanto tempo verranno utilizzati i suoi dati.

Si tratta dunque di una comunicazione relativa alle modalità e finalità del trattamento che il titolare dello stesso, cioè colui che andrà ad effettuare il trattamento dei dati, ha l'obbligo di fornire al soggetto titolare dei dati, per soddisfare il principio di accountability che, come abbiamo già visto, gli

---

[81] Art. 7 GDPR, par. 1

[82] Privacyos, "*Consenso GDPR: caratteristiche e modalità di raccolta*", in *Privacyos.com*

[83] Art. 7 GDPR par. 4

[84] Privacydati, "*Quali sono gli attributi del consenso al trattamento dati obbligatorio secondo il nuovo Regolamento GDPR?*", in *Privacydati.it* 2022

impone di progettare i trattamenti fin dall'inizio in modo da evitare l'insorgenza di rischi e danni futuri.

L'informativa, dettagliatamente disciplinata negli articoli 12, 13 e 14 del Regolamento Europeo, deve essere «concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori. Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici»[85].

Tra le numerose informazioni da fornire, ai sensi dell'art. 13 del GDPR, rilevano:

- L'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;
- I dati di contatto del Responsabile della protezione dei dati, quando previsto;
- le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
- Qualora il trattamento sia necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, i legittimi interessi perseguiti dal titolare del trattamento o da terzi;
- Gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
- Ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione

Oltre a queste informazioni, nel momento in cui sono stati ottenuti i dati dall'interessato, il titolare del trattamento deve fornire le seguenti ulteriori indicazioni[86]:

- Il periodo di conservazione dei dati personali, ovvero il criterio per determinarlo;

[85] Art. 12 GDPR, par. 1

[86] Datalog, "*GDPR PRIVACY: COSA SONO L'INFORMATIVA E IL CONSENSO*", in *Datalog.it*, 2022

- L’intenzione del titolare del trattamento di trasferire dati personali a un Paese terzo o a un’organizzazione internazionale;
- Il diritto dell’interessato di proporre reclamo ad un’autorità di controllo;
- L’esistenza di un processo automatizzato, compresa la profilazione, e l’indicazione delle logiche utilizzate, dell’importanza e delle conseguenze del trattamento;
- Il diritto di accesso ai dati da parte dell’interessato;
- Il diritto di rettifica e di cancellazione;
- La limitazione del trattamento o l’opposizione allo stesso
- Il diritto alla portabilità (disciplinato dall’articolo 20 del GDPR, che consente all’interessato di trasferire i propri dati personali forniti da un titolare del trattamento ad un altro, ad esempio da un’azienda all’altra);
- Il diritto di revocare il consenso in qualsiasi momento, senza pregiudicare la liceità del trattamento basata sul consenso prestato precedentemente alla revoca.

Quanto alla tempistica per effettuare la comunicazione, è stabilito che, qualora si tratti di dati raccolti direttamente presso l’interessato (e quindi comunicati immediatamente dallo stesso), l’informativa deve essere fornita nel momento in cui i dati personali sono ottenuti[87].

Invece, nel caso in cui i dati personali non siano stati raccolti direttamente presso l’interessato ma siano stati ricevuti da terzi, l’informativa dovrà essere resa entro un termine ragionevole dall’ottenimento degli stessi (comunque entro un mese), oppure al momento della prima comunicazione all’interessato o al terzo, a seconda che i dati personali siano destinati alla comunicazione con l’interessato oppure sia prevista la comunicazione ad altro destinatario[88].

Non occorre informare l'interessato quando[89]:

- l'interessato dispone già delle informazioni;

[87] Art. 13 GDPR
[88] Art. 14 GDPR par. 3, lettera a)
[89] Art. 14 GDPR par. 5

- comunicare tali informazioni risulta impossibile o implicherebbe uno sforzo sproporzionato;
- l'ottenimento o la comunicazione sono espressamente previsti dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare;
- i dati personali debbano rimanere riservati per obbligo di segreto professionale disciplinato dal diritto dell'Unione o degli Stati membri.

Procedendo nell'analisi delle caratteristiche del consenso, esso deve essere verificabile, e questo comporta che spetta all'azienda l'onere della prova (come abbiamo già visto in precedenza) e di conseguenza l'obbligo di dimostrare la genuinità del consenso in caso di contestazione o all'autorità che ne faccia richiesta. Non necessariamente questa prova deve essere in forma scritta, può essere raccolta digitalmente purché offra all'azienda la tutela necessaria.

L'ultima caratteristica del consenso riguarda la sua revocabilità. «L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di esprimere il proprio consenso, l'interessato viene informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato»[90].

Nelle situazioni, poi, in cui emergono "gravi rischi per la protezione dei dati", è richiesto un consenso esplicito, il quale rappresenta un diverso livello di consenso rispetto a quello ordinario. Ci si riferisce in particolare ai dati relativi all'articolo 9 del GDPR, ai trasferimenti verso Paesi terzi o verso organizzazioni internazionali[91].

Il Gruppo Articolo 29 (WP29) suggerisce per esempio che il consenso dato attraverso una espressa e formale dichiarazione scritta (firmata dall'interessato) è da considerarsi esplicito[92].

[90] Art. 7 GDPR, par. 3

[91] Art. 49 GDPR, par. 1 lettera a)

[92] M. Iaselli, "*Consenso al trattamento*", in *Altalex.com*, 2018

Tra i tratti più innovativi del Regolamento in tema di consenso, vi è la previsione relativa alla capacità del minore di prestare il consenso al trattamento dei dati[93].

Per poter validamente prestare il consenso al trattamento dei propri dati personali, l'interessato deve essere maggiorenne, in quanto nel nostro ordinamento, è al compimento dei 18 anni che si acquisisce la capacità di agire, ossia quella capacità che ci permette di esercitare liberamente diritti ed assumere obblighi.

Cosa succede se l'interessato è un minore?

La questione si pone in tutta la sua problematicità nell'attuale società, dove i Social Networks e il mondo digitale rappresentano ormai la quotidianità, soprattutto per gli adolescenti. La delicatezza della tematica ha imposto al legislatore, sia europeo che nazionale, di disciplinare la fattispecie dettando specifiche previsioni volte a tutelare il minore.

L'art. 8 del GDPR fissa il limite a 16 anni per esprimere validamente il consenso al trattamento dei dati personali; per un'età inferiore ai 16 anni, il trattamento è lecito solo se e nella misura in cui tale consenso sia prestato o autorizzato dal titolare della responsabilità genitoriale.

Il Regolamento europeo, poi, rimette alla discrezionalità dei legislatori nazionali la possibilità di stabilire, per la medesima finalità, un'età inferiore purché non sia al di sotto dei 13 anni.

Trattandosi di una previsione espressa in un ordinamento sovranazionale, il legislatore europeo ha precisato che la norma contenuta nel par.1 dell'art. 8 «non pregiudica le disposizioni generali del diritto dei contratti degli Stati membri, quali le norme sulla validità, la formazione o l'efficacia di un contratto rispetto a un minore»[94].

Sul piano nazionale, invece, in attuazione dell'art. 8 del GDPR, l'art. 2 quinquies del Codice della privacy, disciplina il consenso del minore in relazione ai servizi della società dell'informazione e, con tale disposizione,

---

[93] I.A. Caggiano, "*Il consenso al trattamento dei dati personali nel nuovo Regolamento europeo. Analisi giuridica e studi comportamentali*", Il Mulino, 2018

[94] Art. 8 GDPR, par. 3

il legislatore ha attuato la possibilità di deroga al limite dell'età rispetto ai 16 anni fissati nel GDPR.

A questo proposito, nel nostro ordinamento viene fissato a 14 anni il limite di età per la valida espressione del consenso, mentre per i soggetti di età inferiore a 14 anni il consenso è espresso da chi ne esercita la responsabilità genitoriale[95].

Inoltre, in relazione all'offerta diretta ai minori dei servizi in questione, il legislatore italiano prescrive determinate regole che devono essere rispettate dal titolare del trattamento: questi, infatti, è tenuto a «redigere con linguaggio particolarmente chiaro e semplice, conciso ed esaustivo, facilmente accessibile e comprensibile dal minore, al fine di rendere significativo il consenso prestato da quest'ultimo, le informazioni e le comunicazioni relative al trattamento che lo riguardi»[96].

1.6 – Il trattamento dei dati particolari (ex dati sensibili)

Il D. lgs 196/2003 utilizzava il termine "dati sensibili" in riferimento a specifici tipi di informazioni riferibili ad una persona, prevedendo il consenso esplicito per poterli trattare e una tutela rafforzata per la gestione di tali dati (le cd. misure di sicurezza idonee)[97].

Il D. lgs 196/2003 considerava come sensibili i dati personali in grado di rivelare:

- l'origine razziale ed etnica di un individuo;
- le sue convinzioni e adesioni religiose, politiche e filosofiche;
- lo stato di salute e la vita sessuale[98].

L'art. 9 del GDPR stabilisce, come regola generale, il divieto di trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una

[95] Art. 2 quinquies Codice della Privacy, par. 1
[96] Art. 2 quinquies Codice della Privacy, par. 2
[97] Redazione Insic, "*La normativa per il trattamento dei dati sensibili*", in *insic.it*, 2021
[98] Privacylab, "*I dati sensibili nel GDPR: cosa sono e come vanno trattati*", in *Privacylab.it*, 2020

persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

Il successivo par. 2 dell'art. 9 prevede delle eccezioni a tale divieto e stabilisce che il trattamento di tali categorie di dati è consentito qualora:

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

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

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

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

j) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato[99].

Per quanto riguarda la disciplina nazionale, l'art. 2 sexies del nostro Codice della privacy, parallelamente a quanto stabilito dalla disposizione europea, stabilisce che «*I trattamenti delle categorie particolari di dati personali di cui*

[99] Art. 9 GDPR, par. 2

all'articolo 9, par. 1, del Regolamento, necessari per motivi di interesse pubblico rilevante ai sensi del par. 2, lettera g), del medesimo articolo, sono ammessi qualora siano previsti dal diritto dell'Unione europea ovvero, nell'ordinamento interno, da disposizioni di legge o di regolamento o da atti amministrativi generali che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato»[100].

Con riferimento ai dati genetici, biometrici e relativi alla salute, proprio per la loro peculiarità, l'art. 9 del GDPR rimette agli Stati membri la possibilità di mantenere o introdurre ulteriori condizioni, comprese limitazioni, rispetto a quelle individuate nella norma stessa[101].

Le definizioni giuridiche di queste tipologie di dati sono contenute rispettivamente nei paragrafi 13, 14 e 15 dell'art. 4: i dati genetici sono «*i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione*»[102]. I dati biometrici sono «*i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici*»[103]. I dati relativi alla salute sono «*i dati personali attinenti alla salute fisica o mentale di una persona*

[100] Art. 2 sexies Codice della Privacy, par. 1
Il D.L. 8 ottobre 2021, n. 139, convertito con modificazioni dalla L. 3 dicembre 2021, n. 205, ha disposto (con l'art. 9, comma 5) che "Gli articoli 2-ter, comma 1, 2-sexies, comma 1, e 58, commi 1 e 2, del codice di cui al decreto legislativo n. 196 del 2003 [...], come modificati dal presente articolo, si applicano anche ai casi in cui disposizioni di legge già in vigore stabiliscono che i tipi di dati che possono essere trattati, le operazioni eseguibili, il motivo di interesse pubblico rilevante, la finalità del trattamento nonché le misure appropriate e specifiche per tutelare i diritti fondamentali dell'interessato e i suoi interessi sono previsti da uno o più regolamenti".
[101] Art. 9 GDPR, par. 4
[102] Art. 4 GDPR, par. 13
[103] Art. 4 GDPR, par. 14

fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute»[104].

Nel nostro ordinamento, il legislatore del D. lgs 101/2018 ha inserito nel Codice della Privacy un nuovo art. 2-septies, dedicato alla previsione di misure di garanzia per il trattamento di questi dati.

Secondo la disposizione del Codice, tali dati possono essere trattati in presenza di una delle condizioni previste dall'art. 9 par. 2 del GDPR ed in conformità alle misure di garanzia disposte dal Garante[105].

Dal punto di vista procedurale, il provvedimento del Garante che stabilisce le misure di garanzia viene adottato con cadenza almeno biennale a seguito di una consultazione pubblica della durata di un periodo non inferiore a sessanta giorni[106].

Il provvedimento del Garante, secondo la relazione di accompagnamento al d.lgs. 101/2018[107] e il secondo comma dell'art. 2-septies, deve tenere conto delle linee guida, delle raccomandazioni e delle migliori prassi pubblicate dal Comitato europeo per la protezione dei dati, dell'evoluzione scientifica e tecnologica del settore oggetto delle misure e dell'interesse alla libera circolazione dei dati personali nel territorio dell'Unione Europea.

Le misure di garanzia sono adottate in relazione a ciascuna categoria di dati personali, avendo riguardo alle specifiche finalità del trattamento e tali misure possono individuare ulteriori condizioni sulla base delle quali il trattamento dei dati è consentito. In particolare, le misure di garanzia individuano le misure di sicurezza, comprese quelle tecniche di cifratura e di pseudonimizzazione, le misure di minimizzazione, le modalità specifiche di accesso selettivo ai dati e per rendere le informazioni agli interessati, nonché le eventuali misure necessarie a garantire i diritti degli interessati[108].

---

[104] Art. 4 GDPR, par. 15

[105] B. Locoratolo Beatrice, "*Il Trattamento Dei Dati Personali e la Privacy*" (Napoli, Simone, 2021), pag. 64

[106] S. Gazzella, "*Trattamento dei dati genetici, biometrici e sanitari: ecco le misure di garanzie*", in *cybersecurity360.it*, 2020

[107] Disponibile sul sito della Camera: http://documenti.camera.it/apps/nuovosito/attigoverno/Schedalavori/getTesto.ashx?file=0022_F001.pdf&leg=XVIII

[108] Art. 2-septies Codice della Privacy, comma 5

Dal momento che le misure di garanzia hanno il ruolo di fondare la liceità delle attività di trattamento di dati genetici, biometrici e relativi alla salute, l'eventuale violazione delle relative prescrizioni comporterà un trattamento illecito di dati personali.

CAPITOLO II
IL MERCATO E LA CONTRATTUALIZZAZIONE DEI DATI PERSONALI

2.1 – Il valore patrimoniale dei dati personali

L'evoluzione del diritto alla protezione dei dati personali ha subìto una trasformazione soprattutto a fronte dell'utilizzo di sempre più sofisticati e innovativi strumenti elettronici e della continua mole di dati oggetto di transito[109].

Quando si parla del concetto di mercato dei dati personali si fa riferimento alla prassi sempre più diffusa di offrire beni e servizi in cambio del consenso al trattamento dei dati personali degli utenti, senza quindi richiedere un corrispettivo in denaro. Questa apparente gratuità del contratto viene, tuttavia, smentita dal valore economico dei dati personali raccolti.

La realtà economica odierna è ormai costellata di una pluralità di casi in cui alcuni operatori del mercato sono disposti a prestare un servizio, o più genericamente ad eseguire una prestazione di carattere patrimoniale, senza ricevere in cambio un corrispettivo monetario, ponendo la sola condizione di poter trattare i dati personali del consumatore. Gli esempi provengono principalmente dal mercato digitale: basti pensare ai servizi di social network, messaggistica istantanea, archiviazione cloud, motori di ricerca, portali di informazione, applicazioni per smartphone e tablet, piattaforme di streaming, programmi informatici e altre pubblicazioni elettroniche[110].

Il fenomeno in questione non è del tutto nuovo, né può considerarsi circoscritto all'universo digitale. Già in passato, non era del tutto inusuale la

[109] M.C. Mazzei, "*Utilizzo dei dati personali: la linea sottile tra uso lecito e non*", in Altalex.com, 2021

[110] G. Versaci, "*La contrattualizzazione dei dati personali dei consumatori*", Edizioni Scientifiche Italiane, 2020.

fornitura di beni materiali giustificata dalla possibilità di ottenere e trattare informazioni personali del soggetto destinatario del bene: Rodotà riportava l'esempio della fornitura di prodotti in omaggio a tutti i clienti disposti a compilare questionari diretti a raccogliere informazioni personali su di essi[111].

Andrew Keen, imprenditore e scrittore angloamericano noto per le sue posizioni critiche nei confronti della rete, ha affermato che «*L'enorme massa di dati personali che ogni giorno gli utenti riversano in rete è il nuovo petrolio, il motore della nuova economia*»[112].

Keen afferma inoltre che sin dalle sue origini, Internet ha posto tre questioni fondamentali: la diseguaglianza economica, il lavoro e la privacy. Il modello economico che prevede una fruizione gratuita dei servizi non può essere compatibile con la tutela della privacy.

Le grandi Aziende come Google, Apple o Facebook hanno, sempre secondo Keen, un unico e specifico interesse, cioè quello di raccogliere una crescente quantità di informazioni a scopo pubblicitario. Questo costituisce il prezzo da pagare per vivere nella società dell'informazione e per usufruire di una fruizione gratuita del web.

Keen accusa Google di aver diffuso la bugia che Internet è una piattaforma libera e gratuita, ma in realtà i dati degli utenti che vengono raccolti diventano una moneta di scambio assai preziosa che sostituisce un modello economico a pagamento[113].

Apparentemente, infatti, gran parte delle nuove tecnologie e applicazioni è gratuita per gli utenti che ne usufruiscono, ma, a fronte della gratuità dei servizi, il prezzo è costituito dalla concessione dei propri dati.

I dati, infatti, consentono alle imprese e, in generale agli operatori economici, di creare una sorta di identikit dell'utenza e di targettizzare i propri prodotti sulla base delle singole preferenze dei consumatori e degli

---

[111] S. Rodotà, Conclusioni, cit. p. 308. Cfr. G. Resta e V. Zeno-Zencovich, "*Volontà e consenso nella fruizione dei servizi in rete*".

[112] A. Jacona, "*Dati personali, il petrolio dell'economia digitale*", in *Apogeonline.com*, 2011.

[113] L. Frachilich, "*Andrew Keen: "Privacy e gratuità su Internet sono solo un sogno""*, in *Wired.it*, 2014

utenti. È proprio per questo motivo che ci si chiede se i dati possano essere paragonati alle merci e costituire un vero e proprio oggetto di scambio.
La patrimonializzazione del dato risulta essere un aspetto non pienamente cristallizzato, ed è tipico delle nuove tecnologie dei mercati digitali: è dunque necessario che gli operatori informino il consumatore sull'utilizzo dei propri dati nelle transazioni commerciali.
Lo scambio "dati vs servizi" effettuato attraverso un social network, un sito web o una qualsiasi altra applicazione tecnologica deve indicare, infatti, con chiarezza, completezza e non ingannevolezza, le informazioni inerenti all'utilizzo dei dati stessi a tutela del consumatore.
È rilevante evidenziare che l'Autorità garante della concorrenza e del mercato (AGCM) ha riconosciuto il valore economico dei dati personali[114].
L'Autorità aveva sancito nel 2018 la violazione del Codice del consumo da parte di *Facebook Ireland Ltd*. e *Facebook Inc* i quali non avevano ottemperato alla diffida di rimuovere la pratica scorretta sull'utilizzo dei dati degli utenti[115].
In particolare, con tale decisione, l'Autorità aveva accertato che Facebook induceva ingannevolmente gli utenti a registrarsi sulla sua piattaforma non informandoli subito e in modo adeguato, durante la procedura di attivazione dell'account, dell'attività di raccolta, con intento commerciale, dei dati da loro forniti e, più in generale, delle finalità remunerative sottese al servizio, enfatizzandone viceversa la gratuità.
Per l'Antitrust, inoltre, le informazioni fornite da Facebook risultavano generiche e incomplete e non fornivano un'adeguata distinzione tra l'utilizzo dei dati necessario per la personalizzazione del servizio (con l'obiettivo di facilitare la socializzazione con altri utenti) e l'utilizzo dei dati per realizzare campagne pubblicitarie mirate.
Oltre a sanzionare Facebook con una multa pari a cinque milioni di euro, l'Autorità aveva vietato l'ulteriore diffusione della pratica ingannevole e disposto la pubblicazione di una dichiarazione di rettifica sulla homepage

[114] AGCM, Decisione CV154, 11 maggio 2017.
[115] AGCM, Decisione IP330, 17 febbraio 2021.

del sito internet aziendale per l'Italia, sull'app Facebook e sulla pagina personale di ciascun utente italiano registrato.

L'istruttoria ha permesso di accertare che le due società non avevano pubblicato la dichiarazione rettificativa, non cessando neppure la pratica scorretta accertata. Secondo l'Autorità, Facebook non forniva ancora un'immediata e chiara informazione sulla raccolta e sull'utilizzo a fini commerciali dei dati degli utenti. Queste informazioni sono infatti necessarie al consumatore per decidere se aderire al servizio, alla luce del valore economico assunto per Facebook dai dati ceduti dall'utente, che costituivano il corrispettivo stesso per l'utilizzo del servizio.

A livello dottrinale, non ci sono stati dubbi sull'esistenza di un vero e proprio contratto tra il gestore della piattaforma social e gli utenti, mentre si è acceso un dibattito con riguardo al tipo di contratto stipulato. Una parte della dottrina si è focalizzata sull'assenza di un corrispettivo dell'utente, corroborata dall'assenza di obblighi in capo al gestore del social network (stando alle condizioni generali più frequenti), giungendo alla conclusione di trovarsi dinanzi ad un contratto gratuito[116].

Sul versante opposto, si è deciso di valorizzare la clausola, ricorrente nei contratti di social network, in base alla quale l'utente concede al gestore del sito una licenza libera da *royalty* sui contenuti coperti da proprietà intellettuale, così come si è puntata l'attenzione sul consenso dello stesso utente al trattamento dei propri dati personali, letto in chiave di "disposizione della privacy"[117].

La combinazione di tali elementi è ritenuta sufficiente per configurare uno scambio, in senso giuridico, di godimento di beni immateriali, che vede l'utente usufruire dell'accesso alla piattaforma social, reso possibile dalla licenza di utilizzo del software concessa dal gestore, e quest'ultimo contemporaneamente trarre profitto dai contenuti di proprietà intellettuale e dai dati personali rilasciati dall'utente.

---

[116] Astone F., "*Il rapporto tra gestore e singolo utente: questioni generali*", in Ann. It. Dir. Aut., 2011, p. 108;

[117] C. Perlingieri, "*Profili civilistici dei social networks*", Napoli, 2014

C'è da segnalare che anche chi preferisce qualificare il contratto come "gratuito" non esita a precisare che si tratterebbe di una gratuità pur sempre interessata, posto che «i fornitori di servizi di social network perseguono un interesse economico, attraverso la vendita di spazi pubblicitari e la commercializzazione di attività di profilazione dell'utenza»[118].

2.2 – La profilazione dei dati personali

Ai sensi dell'art. 4 del GDPR si intende per profilazione «*qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica*»[119].

Secondo quanto si legge nel GDPR, la profilazione richiede tre requisiti specifici:

1) il trattamento deve essere automatizzato: un processo decisionale automatizzato si ha quando vengono prese decisioni impiegando mezzi tecnologici senza che vi sia un coinvolgimento umano;
2) i dati personali costituiscono l'oggetto del trattamento;
3) l'obiettivo finale della raccolta dei dati deve essere lo studio del comportamento delle persone fisiche.

Il Considerando n. 24 del GDPR specifica ulteriormente che, per stabilire se si è in presenza di profilazione «*è opportuno verificare se le persone fisiche sono tracciate su internet, compreso l'eventuale ricorso successivo a tecniche di trattamento dei dati personali che consistono nella profilazione della persona fisica, in particolare per adottare decisioni che la riguardano o analizzarne o prevederne le preferenze, i comportamenti e le posizioni personali*»[120].

---

[118] Caterina R., "*Cyberspazio, social networks e teoria generale del contratto*", in ann. It. Aut., 2011 p. 96

[119] Art. 4 GDPR

[120] Considerando n. 24 GDPR

Inoltre, vi è anche il considerando n. 71 del GDPR, il quale specifica che «*al fine di garantire un trattamento corretto e trasparente nel rispetto dell'interessato, è opportuno che il titolare del trattamento utilizzi procedure matematiche o statistiche appropriate per la profilazione, metta in atto misure tecniche e organizzative adeguate al fine di garantire, in particolare, che siano rettificati i fattori che comportano inesattezze dei dati e sia minimizzato il rischio di errori e al fine di garantire la sicurezza dei dati personali secondo una modalità che tenga conto dei potenziali rischi esistenti per gli interessi e i diritti dell'interessato e che impedisca tra l'altro effetti discriminatori*»[121].

Il Gruppo di Lavoro ex articolo 29 (WP29), il 3 ottobre del 2017, ha pubblicato un documento contenente le Linee Guida in tema di processo decisionale automatizzato e profilazione rispetto alle regole enunciate dal Regolamento europeo 2016/679.

Queste Linee Guida hanno lo scopo di chiarire meglio le disposizioni del GDPR su specifici argomenti, riportando anche esempi e casi pratici offerti dall'esperienza acquisita negli Stati membri[122]. Sono esclusi dall'intervento delle Linee guida i cookies, la cui disciplina specifica è contenuta nel Provvedimento dell'8 maggio 2014 n. 229[123].

La profilazione degli utenti viene effettuata attraverso alcuni sistemi che operano in *background*, quindi all'insaputa dell'interessato stesso.

Per questo motivo il titolare del trattamento è obbligato a fornire all'interessato un'informativa chiara, completa ed esaustiva, in modo tale che ci sia un consenso esplicito per effettuare l'attività di profilazione.

Non sarà quindi possibile utilizzare dati raccolti precedentemente per altre finalità, a meno che non ci sia stato il consenso dell'interessato per la specifica finalità di profilazione. In caso contrario spetta al titolare del trattamento l'obbligo di mettere in atto misure di sicurezza adeguate al fine di proteggere l'interessato. Ovviamente la profilazione deve essere svolta

[121] Considerando n. 71 GDPR

[122] M. Iaselli, "*Profilazione*", in *Altalex.com*, 2018

[123] G. Serafini "*Profilazione e trattamento dei dati personali: cosa c'è da sapere*", in *Soiel.it*, 2018

utilizzando i soli dati strettamente necessari per la finalità indicata, in ossequio al principio di pertinenza e di proporzionalità[124].

Nell'informativa devono, quindi, essere esplicitate le modalità e le finalità della profilazione. Inoltre, deve essere chiarita la logica alla base del trattamento e le conseguenze previste per l'interessato a seguito di tale tipo di trattamento, intendendo in tal senso i criteri utilizzati per giungere alla decisione.

L'attività di profilazione è generalmente considerata molto invasiva e può portare a danni ed abusi a carico degli utenti.

L'utilizzo delle tecniche e delle tecnologie di profilazione, che si sono via via evolute, permette l'effettuazione, allorché si disponga del giusto quantitativo di dati, di un'attività di marketing mirata, detta anche "*Behavioural Advertising*". Questa è una tecnica basata sul tracciamento (*tracking*) delle attività online degli utenti, al fine di costruire dei profili degli utenti di Internet con lo scopo di offrire loro pubblicità più rilevante (mirata, *tailored*) per gli utenti stessi, e quindi più efficace[125].

D'altra parte, la profilazione può anche portare a differenti offerte commerciali (*price discrimination*) a seconda della persona o della categoria nella quale essa viene inclusa, con la conseguenza di creare possibili forme di diseguaglianza sociale o discriminazioni verso le minoranze. Alcune categorie di persone, infatti, potrebbero non essere mai raggiunte da alcune offerte, portando a discriminazioni del tutto ingiustificate[126].

Il GDPR prevede possibili rischi significativi per i diritti e le libertà degli individui riconnessi sia alla tendenziale opacità dei processi e meccanismi automatizzati che porta spesso l'individuo, oggetto di profilazione, a non esserne a conoscenza, sia alla creazione, da parte del titolare, di dati nuovi e aggiuntivi rispetto agli originali che potrebbero inquadrare l'interessato in

[124] Datalog, "*GDPR PRIVACY: CHE COS'È LA PROFILAZIONE*", in *Datalog.it*

[125] B. Saetta, "*Pubblicità comportamentale e real-time bidding*", in *Protezionedatipersonali.it*, 2022

[126] B. Saetta, "*Profilazione e processi decisionali automatizzati*", in *Protezionedatipersonali.it*, 2022

una categoria a cui non si riconosce, condizionando così le sue scelte e, in alcuni casi, portando anche a forme di discriminazione.

Pertanto, il GDPR, per correggere questa asimmetria informativa e di potere negoziale tra titolare e interessato ed evitare pregiudizi alla sfera giuridica di quest'ultimo, individua una serie di requisiti su cui concentrarsi per rendere questi trattamenti automatizzati conformi alla normativa:

- Specifiche prescrizioni in tema di trasparenza e correttezza;
- Maggiori obblighi di accountability;
- Basi giuridiche specifiche per la legittimazione del trattamento;
- Garanzie per gli individui in tema di diritto di opposizione alla profilazione e, in particolare, alla profilazione per finalità di marketing;
- Esecuzione di una valutazione d'impatto sulla protezione dei dati laddove non siano soddisfatte certe condizioni.

Il Regolamento europeo sancisce un generale divieto di sottoporre un individuo a processi decisionali automatizzati compresa la profilazione. Tuttavia, l'articolo 22 del GDPR, paragrafo 1, stabilisce che: «*l'interessato ha diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona*»[127]. È necessario precisare che per "decisione basata unicamente sul trattamento automatizzato" si intende una decisione presa senza che vi sia il coinvolgimento di un essere umano che possa influenzare ed eventualmente cambiare il risultato attraverso la sua autorità o competenza.

Quindi, l'ambito di applicazione è limitato alle sole ipotesi in cui il processo decisionale automatizzato:

- Produce effetti giuridici;
- Incide in modo significativo sulla persona dell'utente e la decisione è basata interamente sul trattamento automatizzato dei dati.

Il Considerando 71 del GDPR cita, come esempi di decisioni automatizzate che possono incidere sui diritti e le libertà degli individui in maniera rilevante,

[127] Art. 22 GDPR, par. 1

il rifiuto automatico di una domanda di credito online o pratiche di assunzione elettronica senza interventi umani[128].

L'art. 22 del GDPR al paragrafo 2 prevede tre eccezioni al divieto generale di un processo decisionale completamente automatizzato che comporti effetti nella sfera giuridica dell'individuo[129]:

a) Quando la decisione è necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento;
b) Quando la decisione è autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento;
c) quando la decisione si basa sul consenso esplicito dell'interessato.

Riguardo al punto a), i Garanti europei chiariscono che la necessità di utilizzare decisioni automatizzate per l'esecuzione o la conclusione di un contratto deve essere interpretata in modo restrittivo, ciò significa che il titolare del trattamento deve essere in grado di dimostrare che la profilazione è necessaria e non è possibile utilizzare mezzi alternativi meno invasivi in grado di raggiungere lo stesso risultato.

In riferimento invece al punto b), la legislazione degli Stati membri può, in casi specifici, autorizzare il ricorso ad un processo decisionale automatizzato per il monitoraggio e la prevenzione delle frodi e dell'evasione fiscale o per garantire la sicurezza e l'affidabilità di un servizio fornito dal titolare.

Infine, riguardo al punto c), il Regolamento richiede il consenso esplicito dell'interessato, ossia confermato da una dichiarazione espressa e non desunto da comportamento concludente.

Il GDPR prevede che gli individui soggetti alla profilazione abbiano una pluralità di diritti, quali l'opposizione alla stessa (articolo 21), la richiesta di cancellazione o la rettifica del loro profilo (articolo 17) e la contestazione alle decisioni automatizzate (articolo 22, paragrafo 3).

Per quanto riguarda il diritto di opposizione all'attività di profilazione, l'interessato ha il diritto di opporsi qualora non volesse essere oggetto di

[128] Considerando n.71 GDPR
[129] Art. 22 GDPR par. 2

una decisione basata esclusivamente su un trattamento automatizzato, tra cui la profilazione, che produce effetti giuridici che lo riguardano.
In tal caso il titolare è obbligato ad interrompere immediatamente il trattamento finché non dimostra all'interessato che il trattamento automatizzato e la profilazione non violano i suoi diritti e le sue libertà. Inoltre, l'interessato può espressamente chiedere che ogni decisione automatizzata che lo riguardi sia condizionata da un intervento umano, di poter esprimere il proprio punto di vista e di contestare la decisione, con adeguate motivazioni. Il WP29 sottolinea che la supervisione umana della conclusione raggiunta dalla macchina deve essere significativa, altrimenti sarebbe solo un modo per aggirare il divieto.
Il problema sta, però, nel fatto che i sistemi automatizzati oggi non sono solamente estremamente complessi, ma i loro codici sono anche soggetti ad elevati livelli di segretezza poiché, in base alla direttiva *Trade Secrets* dell'Unione europea, gli algoritmi di profilazione sono protetti e considerati segreti commerciali[130].
Infine, il trattamento basato su sistemi automatizzati deve essere preceduto dalla cosiddetta "valutazione di impatto", proprio perché dalle elaborazioni possono derivare dettagli informativi ritenuti di natura particolarmente invasiva, ma anche perché possono essere impiegati una quantità significativa di dati ai quali devono essere assicurati gli opportuni livelli di protezione e garanzia contro i possibili rischi per i diritti e le libertà degli interessati.

2.2.1 – La Valutazione di impatto

La valutazione d'impatto sulla protezione dei dati (D.P.I.A., cioè *Data Protection Impact Assessment*) è contenuta nell'art. 35 del GDPR, il quale afferma che tale valutazione deve essere effettuata dal titolare del trattamento «quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le

[130] B. Saetta, "*Profilazione e processi decisionali automatizzati*", in *Protezionedatipersonali.it*, 2022

finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche»[131].

In sostanza la DPIA è un processo volto a descrivere il trattamento, valutarne la necessità e la proporzionalità e a gestire gli eventuali rischi per i diritti e le libertà delle persone derivanti dal trattamento.

Con tale strumento l'onere dell'analisi dei rischi passa dai Garanti ai titolari del trattamento. Se prima era necessario richiedere all'Autorità di controllo un'autorizzazione preventiva, adesso il GDPR pone questo onere direttamente a carico del titolare del trattamento, in applicazione del principio di *accountability*.

Il titolare, quindi, è tenuto a sviluppare una valutazione ex ante (prima di iniziare il trattamento) delle eventuali conseguenze del trattamento dei dati personali sulle libertà e i diritti degli interessati. Il responsabile del trattamento deve inoltre assistere il titolare fornendogli ogni informazione necessaria[132].

La valutazione di impatto deve contenere almeno:

- la descrizione sistematica dei trattamenti previsti, la finalità del trattamento, compreso l'eventuale interesse legittimo perseguito dal titolare;
- la valutazione della necessità e proporzionalità del trattamento in relazione alla finalità;
- la valutazione dei rischi per i diritti e le libertà degli interessati;
- le misure previste per affrontare i rischi, incluse le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati e dimostrare la conformità al regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione[133].

Infine, l'art. 35 del GDPR, al paragrafo n. 3, indica i casi in cui è richiesta la valutazione d'impatto:

---

[131] Art. 35 GDPR par. 1

[132] B. Saetta, "*Valutazione di impatto (DPIA) e rischio del trattamento*", in *Protezionedatipersonali.it*, 2022

[133] M. Iaselli, "*Valutazione di impatto sulla protezione dei dati (DPIA)*", in *Altalex.com*, 2018

a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata sul trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono allo stesso modo significativamente su dette persone fisiche;
b) il trattamento, su larga scala, di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10;
c) la sorveglianza sistematica di una zona accessibile al pubblico su larga scala

Con riferimento all'ultimo punto, il considerando 91 ci aiuta a definire il concetto di "larga scala", fondamentale per l'interpretazione della disposizione, dove recita: «i trattamenti su larga scala, che mirano al trattamento di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato»[134].

Il titolare del trattamento deve consultarsi col DPO (*Data Protection Offer*), detto anche "Responsabile per la Protezione dei Dati" (RPD) quando svolge la valutazione di impatto. Questa figura ha il compito di fornire, se richiesto, un parere in merito alla valutazione di impatto e sorvegliarne lo svolgimento. Nel caso in cui il titolare non concordi con le indicazioni del DPO dovrà motivare e documentare il suo dissenso.

L'art. 36 del GDPR stabilisce che «*il titolare del trattamento, prima di procedere al trattamento, deve consultare l'autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio*»[135].

[134] Considerando n. 91 GDPR
[135] Art. 36 GDPR

2.3 – I Contratti di fornitura di contenuti e servizi digitali

Il 26 novembre 2021 è stato pubblicato in Gazzetta Ufficiale il decreto legislativo 4 novembre 2021, n. 173, di attuazione della direttiva UE 2019/770 del Parlamento Europeo e del Consiglio del 20 maggio 2019 relativa a determinati aspetti dei contratti di fornitura di contenuti e di servizi digitali (c.d. DCD).

Il decreto apporta alcune modifiche al Codice del Consumo (D.lgs. 206/2005) nel quale viene inserito il nuovo "Capo I-bis – Dei Contratti di fornitura di contenuto digitale e di servizi digitali", che contiene gli articoli da art. 135 octies a 135-vicies ter.

Le novità introdotte dal decreto hanno assunto efficacia a partire dal 1° gennaio 2022 e si applicano alle forniture di contenuti o servizi digitali avvenute a partire da quella data, con l'eccezione del diritto di regresso e delle regole sulla modifica del contenuto o del servizio digitale (nuovi articoli 135-quindecies e 135-vicies semel), che si applicano invece, solo ai contratti conclusi a decorrere dal 1° gennaio 2022[136].

Queste novità riguardano la conformità del contenuto o servizio digitale al contratto, il cosiddetto "pagamento" mediante dati personali da parte del consumatore, i rimedi in caso di difetto di conformità al contratto o di mancata fornitura, con le relative modalità di esercizio, nonché la modifica del contenuto o del servizio digitale[137].

In contemporanea, in Italia è stata recepita anche la direttiva 2019/771 con il D. lgs 170/2021, il quale ha modificato gli articoli da 128 a 135 del Codice del consumo ed ha aggiunto gli articoli da 135 bis a 135 septies.

In particolare, sono state ampliate le definizioni di:

- Bene, includendo «*qualsiasi bene mobile materiale che incorpora, o è interconnesso con, un contenuto digitale o un servizio digitale in modo tale che la mancanza di detto contenuto digitale o servizio*

[136] M. Martorana, R. Savella, "*Fornitura di contenuti o servizi digitali: le modifiche al Codice del consumo*", in *Altalex.com*, 2021

[137] S. Corongiu, "*Contratti di fornitura di contenuto e di servizi digitali: le novità del d.lgs. n. 173/2021*", in *Altalex.com*, 2021

digitale impedirebbe lo svolgimento delle funzioni proprie del bene ("beni con elementi digitali")»[138];

- Venditore, comprendendo «*il fornitore di piattaforme se agisce per finalità che rientrano nel quadro della sua attività e quale controparte contrattuale del consumatore per la fornitura di contenuto digitale o di servizi digitali*»[139].
- Contenuto digitale: «*i dati prodotti e forniti in formato digitale*»[140];
- Servizio digitale: «*un servizio che consente al consumatore di creare, trasformare, memorizzare i dati o di accedervi in formato digitale; oppure un servizio che consente la condivisione di dati in formato digitale caricati o creati dal consumatore o da altri utenti di tale servizio o qualsiasi altra interazione con tali dati*»[141].

Unitamente alla direttiva (UE) 2019/771, la DCD si inserisce nella strategia del legislatore europeo volta alla creazione di un mercato unico digitale nell'Unione Europea, contribuendo al corretto funzionamento del mercato interno e garantendo un'adeguata tutela ai consumatori.

Ai sensi dei commi 3 e 4 dell'articolo 135 octies le disposizioni del Capo I-bis si applicano a due diverse ipotesi:

1) A qualsiasi contratto in cui il professionista fornisce, o si obbliga a fornire, un contenuto digitale o un servizio digitale al consumatore e il consumatore corrisponde, o si obbliga a corrispondere, un prezzo;
2) Al caso in cui il professionista fornisce, o si obbliga a fornire, un contenuto digitale o un servizio digitale al consumatore e il consumatore fornisce, o si obbliga a fornire, dati personali al professionista, quando tali dati non sono trattati dal professionista esclusivamente per l'esecuzione del contratto.

Per la prima volta, quindi, un atto legislativo riconosce la possibilità di utilizzare i dati personali come mezzo di pagamento per l'acquisto di contenuti o servizi digitali.

[138] Art. 128 Codice del Consumo, par. 2, lettera e)
[139] Art. 128 Codice del Consumo, par. 2, lettera c)
[140] Art. 128 Codice del Consumo, par. 2 lettera f)
[141] Art. 128 Codice del Consumo, par. 2 lettera g)

L'ipotesi in cui il consumatore fornisce (o si impegna a fornire) dati personali all'operatore economico è a sua volta scomponibile in due modelli: il primo caratterizzato dalla cd. gratuità interessata, in quanto l'erogazione del servizio costituisce uno strumento per la raccolta e il trattamento dei dati[142]; il secondo invece qualificabile come del tutto gratuito[143].

Soltanto nel primo caso, infatti, il professionista richiede i dati per finalità remunerative o comunque per trarne un vantaggio di natura economica, mentre nel secondo caso la richiesta del consenso al trattamento risulta "necessitata", ossia connessa a ragioni meramente funzionali all'esecuzione della prestazione o all'assolvimento di obblighi di legge[144].

Sul tema del pagamento tramite dati personali, è utile citare il considerando n. 24 della direttiva UE 2019/770, il quale recita: «*La presente direttiva dovrebbe altresì applicarsi nel caso in cui il consumatore acconsenta a che il materiale che caricherà e che contiene dati personali, come fotografie o post, sia trattato a fini commerciali dall'operatore economico. Gli Stati membri dovrebbero tuttavia mantenere la facoltà di decidere in merito al soddisfacimento dei requisiti in materia di formazione, esistenza e validità di un contratto a norma del diritto nazionale*»[145].

Si può affermare, quindi, che sia stato lasciato un margine di discrezionalità agli Stati membri: non essendo chiaro se questo tipo di accordo possa soddisfare i requisiti di formazione del contratto delle varie legislazioni nazionali, stando al considerando n. 24 della direttiva ogni Paese deve essere in grado di decidere autonomamente sulla questione.

---

[142] Tale affermazione è riscontrabile nella maggior parte delle ipotesi di erogazione di servizi e spicca in modo particolare nell'accesso a social networks ove l'attività del gestore trova giustificazione nello scambio che, in ragione all'attività degli utenti, si realizza con l'inserzionista. Allo stesso modo, la gratuità del servizio fornito agli utenti è funzione di quel medesimo scambio ed è una gratuità interessata, giustificata dal collegamento causale che si realizza tra prestazioni del gestore, prestazioni dell'inserzionista e attività degli utenti, cfr. F. Astone, "*Il rapporto tra gestore e utente: questioni generali*" in *Aida*, 2011, p. 114

[143] C. Camardi, "*Prime osservazioni sulla Direttiva (UE) 2019/770 sui contratti per la fornitura di contenuti e servizi digitali*" p. 499 e ss.

[144] A. Addante, "*La circolazione negoziale dei dati personali nei contratti di fornitura di contenuti e servizi digitali*", in Giustizia Civile, fasc. 4, p. 889, 2020

[145] Direttiva UE 2019/770, Considerando n. 24

Da qui emerge la volontà del legislatore europeo di garantire anche a queste situazioni le stesse tutele giuridiche che vengono assicurate ai contratti di fornitura di contenuti o servizi digitali[146].

Tuttavia, in Italia i problemi interpretativi sulla natura giuridica di questa tipologia di accordo non sono stati affrontati dal legislatore nazionale in fase di recepimento, vi è stata solamente una semplice trasposizione della lettera della Direttiva nella legge interna.

A parte il quarto comma dell'articolo 135-octies e il comma 6 dell'articolo 135-novies, il quale recita che «*In caso di conflitto tra le disposizioni del nuovo Capo I bis e quelle adottate dall'Unione europea in materia di protezione dei dati personali, prevalgono queste ultime*» il caso di "pagamento" tramite i dati personali del consumatore non è oggetto di ulteriore considerazione da parte del legislatore italiano.

L'art. 135 novies del Codice del consumo, inoltre, esclude dall'ambito di applicazione della nuova disciplina introdotta con il d.lgs. n. 173 del 2021 i contenuti digitali o i servizi digitali incorporati o interconnessi con beni di cui all'art. 135-octies, comma 2, lett. c): si tratta dei c.d. "beni con elementi digitali", che trovano espressa disciplina nella direttiva UE 2019/771.

I "beni con elementi digitali", come abbiamo già visto, sono i beni mobili materiali che incorporano o sono interconnessi con un contenuto digitale o un servizio digitale, in modo tale che la mancanza di detto contenuto o servizio digitale impedirebbe lo svolgimento delle funzioni del bene. Tale esclusione viene applicata a prescindere dalla circostanza che detti contenuti o servizi digitali siano forniti dal venditore o da un terzo.

Quando è dubbio se la fornitura del contenuto o del servizio digitale incorporato o interconnesso faccia parte del contratto di vendita, si presume che il contenuto o il servizio digitale incorporato o interconnesso rientri nel contratto di vendita[147].

Inoltre, le disposizioni introdotte con il d.lgs. 173/2021 non si applicano ai contratti concernenti:

---

[146] M. Martorana, R. Savella, "*Fornitura di contenuti o servizi digitali: le modifiche al Codice del consumo*", in *Altalex.com*, 2021

[147] Art. 128, comma 3, Codice del consumo e Art. 135 novies, comma 1, Codice del consumo

a) la fornitura di servizi diversi dai servizi digitali, ad esempio contratti di fornitura di servizi professionali quali servizi di traduzione, di architettura, legali o altri servizi di consulenza professionale;
b) i servizi di comunicazioni elettroniche ai sensi dell'articolo 2, punto 4), della direttiva (UE) 2018/1972 (i messaggi di testo SMS), con l'eccezione dei servizi di comunicazioni interpersonale senza numero (i servizi di *e-mail* e di messaggistica *online*);
c) i servizi di assistenza sanitaria;
d) i servizi di gioco d'azzardo forniti mediante strumenti elettronici o qualsiasi altra tecnologia che facilita le comunicazioni e su richiesta individuale di un destinatario di tali servizi;
e) i servizi finanziari, vale a dire qualsiasi servizio di natura bancaria, creditizia, assicurativa, servizi pensionistici individuali, di investimento o di pagamento;
f) il software offerto sulla base di una licenza libera e aperta in cui non viene pagato alcun prezzo e i dati personali forniti dal consumatore sono utilizzati esclusivamente al fine di migliorare il software specifico;
g) il contenuto digitale quale parte di uno spettacolo o di un evento, come le proiezioni cinematografiche digitali;
h) il contenuto digitale fornito da enti pubblici, a norma della direttiva 2019/1024 del Parlamento europeo e del Consiglio relativa al riutilizzo dell'informazione del settore pubblico[148].

Lo scopo primario della normativa in analisi è quello di garantire che anche la fornitura di contenuti o di servizi digitali rispetti determinati requisiti e sia oggetto di specifici obblighi e responsabilità delle parti.

L'articolo 135-decies indica i requisiti soggettivi e quelli oggettivi che il contenuto o servizio deve possedere per essere considerato conforme al contratto. In particolare, per rispettare i requisiti soggettivi di conformità il contenuto o il servizio deve:

[148] Art. 135 novies, Codice del consumo, comma 2

a) corrispondere alla descrizione, alla quantità e alla qualità previste dal contratto e presentare funzionalità, compatibilità, interoperabilità e le altre caratteristiche previste dal contratto;
b) essere idoneo ad ogni uso particolare voluto dal consumatore e che è stato da questi portato a conoscenza del professionista al più tardi al momento della conclusione del contratto e che il professionista ha accettato;
c) essere fornito con tutti gli accessori, le istruzioni anche in merito all'installazione e all'assistenza ai clienti, come previsto dal contratto;
d) essere aggiornato come previsto dal contratto[149].

Successivamente, al comma 5 del medesimo articolo, sono elencati i requisiti oggettivi di conformità, i quali, in sintesi, comprendono:

a) L'adeguatezza agli scopi per cui un contenuto o servizio digitale del medesimo tipo sarebbe utilizzato;
b) La presenza delle qualità, quantità e caratteristiche di prestazione che normalmente si trovano per quel tipo di contenuto o servizio e che il consumatore può ragionevolmente aspettarsi;
c) La presenza degli accessori e istruzioni che il consumatore può ragionevolmente aspettarsi di ricevere;
d) La conformità all'eventuale versione di prova o anteprima messa a disposizione prima della conclusione del contratto[150].

2.4 – I rimedi in caso di non conformità dei contenuti o servizi digitali

Il professionista è obbligato ad assicurare che il consumatore venga informato e riceva gli aggiornamenti, anche di sicurezza, necessari a mantenere la conformità del contenuto o del servizio digitale[151].

Il professionista deve in ogni caso assicurare la conformità del contenuto o del servizio per tutta la durata della fornitura, quando questa avviene in modo continuativo per un determinato periodo di tempo.

[149] Art. 135 decies, Codice del consumo, comma 4
[150] Art. 135 decies, Codice del consumo, comma 5
[151] Art. 135 undecies Codice del consumo, e "*Contratti di fornitura di contenuto digitale e di servizi digitali*", in *eur-lex.europa.eu*

Il contenuto o servizio, salvo diverso accordo, deve essere fornito nella versione più recente disponibile sul mercato al momento della conclusione del contratto.

A tutela del consumatore, vi è la circostanza in cui l'onere della prova riguardo al fatto se il contenuto digitale o il servizio digitale sia stato fornito correttamente e nei termini contrattuali è a carico del professionista.

In caso di difetto di conformità che risulti evidente entro il termine di un anno dal momento in cui il contenuto digitale o il servizio digitale è stato fornito, è onere del professionista provare che il contenuto digitale o il servizio digitale era conforme al momento della fornitura; lo stesso dicasi per gli aggiornamenti[152].

La norma risulta di particolare protezione per il consumatore e tende a prevenire comportamenti del professionista non conformi a correttezza, basati sulla convinzione che il consumatore acquirente potrebbe non avere competenze sufficienti per provare i difetti del contenuto o servizio acquistato.

Tuttavia, nel caso in cui il consumatore sia stato informato dal professionista sulla disponibilità dell'aggiornamento, sulle conseguenze della sua mancata installazione e su come effettuarla, quest'ultimo non è tenuto a rispondere per i difetti di conformità che derivano unicamente dalla mancata installazione entro un congruo termine dell'aggiornamento[153].

Resta fermo l'onere del consumatore di collaborare con il professionista «*per quanto ragionevolmente possibile e necessario al fine di accertare se la causa del difetto di conformità del contenuto o del servizio digitale risieda nel suo ambiente digitale*»[154]. Tale norma è fondamentale poiché, in mancanza di detta collaborazione, e se dovesse risultare che il professionista aveva precedentemente informato il consumatore dei requisiti relativi all'ambiente digitale necessario, l'onere della prova si

[152] "*Contratti di fornitura di contenuto digitale e di servizi digitali entra in vigore la normativa europea recepita*", in "*letsnetwork.it"*, 2022

[153] M. Martorana, R. Savella, "*Fornitura di contenuti o servizi digitali: le modifiche al Codice del consumo*", in "*Altalex.com*", 2021

[154] Art. 135 sexiesdecies, par. 5, Codice del consumo

inverte e sarà poi il consumatore a dover provare l'esistenza del difetto di conformità[155].

L'articolo 135 quaterdecies del Codice del consumo sancisce la responsabilità del professionista, oltre che per la mancata fornitura di contenuti o servizi digitali, anche per i difetti di conformità dei medesimi che si manifestano entro due anni a decorrere dal momento della fornitura.

Il termine di prescrizione per il diritto di azione del consumatore è di 26 mesi a partire da quella data[156].

Il professionista ha comunque la facoltà di esercitare il diritto di regresso nei confronti dei soggetti facenti parte della catena distributiva eventualmente responsabili per il difetto di conformità[157].

Inoltre, «*il professionista che abbia ottemperato ai rimedi esperiti dal consumatore può agire, entro un anno dall'esecuzione della prestazione, in regresso nei confronti del soggetto o dei soggetti responsabili per ottenere la reintegrazione di quanto prestato*»[158].

Gli articoli 135-septiesdecies e 135-octiesdecies disciplinano i rimedi per la mancata fornitura e per i difetti di conformità.

Nel caso di mancata fornitura, il consumatore può inviare al professionista una richiesta di adempiere; se quest'ultimo non adempie entro un termine congruo o un termine fissato dalle parti, il consumatore ha diritto alla risoluzione del contratto.

Il consumatore, inoltre, ha il diritto di risolvere immediatamente il contratto senza una preventiva richiesta di adempimento quando:

- Il professionista ha dichiarato che non fornirà il contenuto digitale o il servizio digitale;
- Il consumatore e il professionista hanno concordato un termine essenziale per la fornitura stessa[159].

---

[155] S. Corongiu, "*Contratti di fornitura di contenuto e di servizi digitali: le novità del d.lgs. n. 173/2021*", in "*Altalex.com*", 2021

[156] Art. 135-quaterdecies Codice del consumo, comma 4

[157] Art. 135 quinquiesdecies Codice del consumo, comma 1

[158] Art. 135 quinquiesdecies Codice del consumo, comma 2

[159] Art. 135 septiesdecies Codice del consumo, comma 2

In presenza di difetti di conformità, invece, il consumatore ha diritto al ripristino della conformità o ad una congrua riduzione del prezzo o alla risoluzione del contratto[160].

Se il servizio o il contenuto digitale è stato fornito in cambio del pagamento di un prezzo, l'art. 135 octiesdecies attribuisce al consumatore il diritto di chiedere la riduzione proporzionale del prezzo, oppure la risoluzione del contratto in uno dei seguenti casi:

a) il rimedio del ripristino della conformità del contenuto digitale o del servizio digitale è impossibile o sproporzionato ai sensi del comma 2 dell'art. 135 octies;
b) il professionista non ha ripristinato la conformità del contenuto digitale o del servizio digitale;
c) si manifesta un difetto di conformità, nonostante il tentativo del professionista di ripristinare la conformità del contenuto digitale o servizio digitale;
d) il difetto di conformità è talmente grave da giustificare un'immediata riduzione del prezzo o risoluzione del contratto;
e) il professionista ha dichiarato che non procederà al ripristino della conformità del contenuto digitale o del servizio digitale entro un congruo termine o senza notevoli inconvenienti per il consumatore[161].

In ogni caso, l'art. 135-octiesdecies prevede che, «*se il contenuto digitale o il servizio digitale è stato fornito in cambio del pagamento di un prezzo, il consumatore non ha diritto di risolvere il contratto se il difetto di conformità è di lieve entità. L'onere della prova riguardo al fatto che il difetto di conformità è di lieve entità è a carico del professionista*»[162].

L'articolo 135-noviesdecies disciplina la risoluzione del contratto, precisando che il consumatore può esercitare il diritto di risoluzione del

[160] Art. 135 octiesdecies Codice del consumo, comma 1
[161] Art. 135 octiesdecies Codice del consumo, comma 4
[162] Art. 135 octiesdecies Codice del consumo, comma 6

contratto mediante una dichiarazione in cui manifesta la propria volontà in tal senso[163].

Nel caso di risoluzione del contratto il professionista è tenuto a rimborsare al consumatore tutti gli importi versati in esecuzione del contratto al netto del periodo di tempo antecedente la risoluzione in cui il consumatore ha potuto fruire del contenuto digitale o del servizio digitale acquistato[164].

Si precisa, infine, che il consumatore non è tenuto a pagare per l'utilizzo del contenuto digitale o del servizio digitale nel periodo che precede la risoluzione del contratto qualora il contenuto o il servizio non siano risultati conformi al contratto[165].

L'articolo 135-viciessemel disciplina le modifiche del contratto: qualora il contratto preveda che il contenuto digitale sia fornito o reso accessibile al consumatore per un certo periodo di tempo, il professionista può modificare il contenuto digitale o il servizio digitale se vengono soddisfatte alcune condizioni:

a) il contratto consente tale modifica e ne fornisce una motivazione valida;
b) la modifica viene realizzata senza costi aggiuntivi per il consumatore;
c) il consumatore è informato in modo chiaro e comprensibile riguardo alla modifica[166].

Il consumatore ha il diritto di recedere gratuitamente dal contratto entro trenta giorni dalla data di ricevimento dell'informazione o, se successivo, dal momento in cui il contenuto digitale o il servizio digitale è stato modificato dal professionista, qualora la modifica del contratto incida negativamente sull'utilizzo o sull'accesso del contenuto o servizio digitale da parte del consumatore, a meno che tali conseguenze negative siano trascurabili[167].

Infine, è fondamentale citare l'articolo 135 vicies bis che riguarda il carattere imperativo delle norme introdotte nel Capo I-bis dal d. lgs 173/2021 e che

[163] Art. 135 noviesdecies Codice del consumo, comma 1
[164] S. Corongiu, "*Contratti di fornitura di contenuto e di servizi digitali: le novità del d.lgs. n. 173/2021*", in "*Altalex.com*", 2021
[165] Art. 135 noviesdecies Codice del consumo, comma 2
[166] Art. 135 viciessemel Codice del consumo, comma 1
[167] Art. 135 viciessemel Codice del consumo, comma 2

contiene ulteriori misure di tutela nei confronti del consumatore. Nello specifico, viene sancita la nullità di qualsiasi patto «*anteriore alla comunicazione al professionista del difetto di conformità o dell'informazione da parte del professionista circa la modifica del contenuto digitale o del servizio digitale, volto ad escludere o limitare i diritti riconosciuti dal nuovo Capo*»[168]. Tale nullità può essere fatta valere solamente dal consumatore e può essere rilevata d'ufficio dal giudice.

Analogamente, il comma 3 del medesimo articolo sancisce la nullità di ogni eventuale clausola contrattuale che, prevedendo l'applicabilità al contratto di una legislazione di uno Stato terzo, privi di fatto il consumatore della protezione assicurata dal Capo I bis[169].

Vi è infine un aspetto che rende di particolare evidenza la complementarità della protezione dei dati personali rispetto alla tutela contrattuale derivante dall'accesso a contenuti o servizi digitali, cioè la possibilità di inquadrare le violazioni in materia di sicurezza nel trattamento dei dati fra i difetti di conformità, ai sensi della Direttiva 770/2019.

Questo aspetto è di notevole interesse perché apre alla possibilità di una concreta incorporazione della *data protection* nelle maglie dei rimedi contrattuali, non soltanto per singole e specifiche ipotesi, bensì anche con riguardo ai principi fondamentali contenuti nel GDPR, i quali impongono anche l'obbligo di adottare misure tecniche ed organizzative adeguate a tutelare i diritti degli interessati, strutturandole secondo i parametri della *privacy by design e by default*[170]. Questa evenienza, seppur non ribadita espressamente nella Direttiva n. 770/2019, viene esplicitata nell'ambito del considerando n. 48 della medesima direttiva ed è confermata da ulteriori indizi normativi che impongono al professionista di rispettare gli obblighi previsti dal GDPR e che, in termini generali, sanciscono l'applicabilità del

[168] Art. 135 viciesbis Codice del consumo, comma 1

[169] Art. 135 viciesbis Codice del consumo, comma 3

[170] F. Bravo, "*L'architettura del trattamento e la sicurezza dei dati e dei sistemi", in "I dati personali nel diritto europeo*", cit., p. 775

diritto dell'UE in materia di dati personali a qualsiasi dato personale trattato nei contratti di fornitura[171].

Vi sono poi numerosi esempi di possibili violazioni della sicurezza dei dati conseguenti all'accesso ad un contenuto o servizio digitale mal progettato e di conseguenza esposto a potenziali rischi di intrusione altrui. Uno fra tanti è il caso di software di cifratura inadeguati che comportano la divulgazione non autorizzata a terzi, oppure l'ipotesi in cui le informazioni personali di un utente/consumatore siano esposte ad attacchi da parte di *spyware* (un tipo di virus che si nasconde nei dispositivi, il quale monitora le attività dell'utente e sottrae informazioni sensibili come dati bancari e password), con il rischio di un utilizzo abusivo da parte di terzi[172].

In conclusione, si può affermare che con il D.lgs 173/2021 è stata fatta una trasposizione quasi del tutto letterale della Direttiva (UE) 2019/770, estendendo ai contratti di fornitura di contenuti e servizi digitali le tutele previste dalla disciplina consumeristica per i difetti di conformità e la mancata fornitura, senza però affrontare la questione della qualificazione giuridica dell'accordo sulla base del quale il consumatore fornisce i propri dati personali come controprestazione. Ogni tentativo di considerare le modifiche così introdotte nel Codice del consumo come un riconoscimento giuridico di questo tipo di scambio deve fare i conti con le problematiche ancora irrisolte e derivanti dal coordinamento di queste previsioni con quelle del GDPR e della disciplina generale dei contratti[173].

---

[171] C. Camardi, "*Prime osservazioni sulla Direttiva (UE) 770/2019 sui contratti per la fornitura di contenuti e servizi digitali*" in A. Addante, "*La circolazione negoziale dei dati personali nei contratti di fornitura di contenuti e servizi digitali*", 2020

[172] Lo stesso Considerando n. 48 della Direttiva 770/2019 offre una casistica esemplificativa a tal riguardo

[173] M. Martorana, R. Savella, "*Fornitura di contenuti o servizi digitali: le modifiche al Codice del consumo*", in "*Altalex.com"*, 2021

2.5 – Il trattamento dei dati per finalità di marketing e il consenso al trattamento dei dati da parte di terzi

Il marketing è da sempre uno dei principali strumenti per lo sviluppo di un'azienda, la quale può diffondere il proprio *brand* e promuovere i propri prodotti portandoli alla conoscenza del pubblico.

Il termine "marketing" si riferisce a quel ramo dell'economia che riguarda lo studio descrittivo e l'analisi del mercato e indica l'azione sul mercato da parte delle imprese destinata al piazzamento di prodotti o servizi, considerando come obiettivo finale il maggiore profitto e come causalità la possibilità di avere prodotti capaci di realizzare tale operazione finanziaria[174].

Tuttavia, se in passato le aziende acquistavano semplicemente uno spazio pubblico o una pagina di un quotidiano per affiggere cartelloni pubblicitari o riportare le novità del momento ai potenziali lettori, oggi la principale sfida che sono chiamate ad affrontare riguarda l'utilizzo delle nuove tecnologie.

In un mondo sempre più tecnologicamente avanzato, il marketing riveste un ruolo fondamentale, ma il problema sorge in relazione al trattamento dei dati personali per finalità di marketing, soprattutto laddove tali dati vengono utilizzati per indirizzare massicce campagne pubblicitarie all'utente, talvolta anche piuttosto frequenti e di conseguenza molto spesso indesiderate[175].

Si tratta quindi di capire non solo come si sia evoluto il marketing con le nuove tecnologie, ma anche come e quando questo possa rientrare nel legittimo interesse dell'attore commerciale.

Prima della c.d. rivoluzione digitale, il marketing era già alla base dei processi di sviluppo del business. Tuttavia, si cercava di reperire informazioni tramite strumenti prettamente empirici, come, per esempio, le indagini statistiche e le analisi di mercato.

Ottenere dei *feedback* da parte dei clienti risultava particolarmente difficile poiché non esistevano canali adeguati attraverso cui i clienti potessero esprimersi in maniera efficace e così andavano perdute enormi quantità di

[174] F. Corona, "*Tutto quello che devi sapere sul marketing e GDPR*", in "*Legaldesk.it*", 2019
[175] M. Martorana, Z. Sichi, "*Dati utilizzati a fini di marketing*", in "*Altalex.com*", 2021

informazioni utili per migliorare le aziende, le loro strategie di mercato e, di conseguenza, i loro prodotti.

L'obiettivo di ogni efficace strategia di marketing, infatti, è quello di individuare i bisogni dei clienti attuali e potenziali, definendo azioni opportune per generare soddisfazione con reciproco vantaggio[176].

Oggi, nell'era della digitalizzazione, è radicalmente cambiato il modo di ricorrere alle strategie di marketing e di applicarle; gli strumenti odierni e l'introduzione di nuove figure professionali (come, ad esempio, il "*Data Analyst*") permettono di trattare una grande mole di dati e informazioni che in passato andavano persi, i quali sono utili a migliorare i risultati delle campagne pubblicitarie, ma anche a comprendere meglio l'andamento del mercato.

Il raggiungimento di questi obiettivi è sempre più semplice, grazie alle possibilità offerte dalle tecnologie legate all'intelligenza artificiale e alla personalizzazione dei contenuti. Infatti, una gran parte del marketing digitale avviene attraverso una fitta profilazione degli utenti, ossia, come abbiamo già visto, ai sensi dell'art 4 del GDPR, «*qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica*», che, applicato al marketing, significa elaborare i dati relativi a uno o più clienti o utenti allo scopo di suddividerli in gruppi omogenei in base a gusti, interessi e comportamenti[177].

Tuttavia, sappiamo già che l'art. 22 del GDPR prevede che l'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato. Solitamente, chi svolge attività di marketing ha bisogno di raccogliere più dati possibili, ma in ogni caso il trattamento dei dati personali deve essere minimizzato (in base al principio generale dell'art. 5 del GDPR) e, se la profilazione si basa unicamente su trattamenti automatizzati, è necessario il consenso specifico per ogni finalità.

[176] A. Gualtieri, "*Marketing, trattamento dati e GDPR: istruzioni per l'uso*" in "*Pmi.it*"
[177] M. Martorana, Z. Sichi, "*Dati utilizzati a fini di marketing*", in "*Altalex.com*", 2021

Di norma, quindi, l'invio di comunicazioni a fini promozionali attraverso strumenti elettronici automatizzati richiede la preventiva manifestazione del consenso da parte dell'interessato.

Tuttavia, l'art. 130 comma 4 del Codice Privacy introduce un'importante eccezione: si tratta del c.d. *soft spam.*, Con questo termine ci si riferisce a quella pratica di invio di comunicazioni promozionali mediante e-mail o posta tradizionale ai clienti per pubblicizzare prodotti e/o servizi correlati a quelli già in precedenza acquistati dal destinatario[178]. In simili ipotesi il Codice Privacy dispone che non è necessario ottenere il previo consenso da parte dell'interessato a patto che ricorrano le seguenti condizioni:

1) il destinatario della comunicazione sia già cliente o sia un ex cliente della società titolare del trattamento;
2) la comunicazione commerciale riguardi "servizi analoghi a quelli oggetto della vendita";
3) nell'informativa privacy l'interessato sia stato informato che i suoi dati potranno essere utilizzati anche per finalità di soft spam;
4) l'interessato sia stato informato del diritto di *opt-out*, cioè del diritto di rifiutare in maniera agevole e gratuita l'invio di simili comunicazioni[179].

Nelle ipotesi descritte, la base giuridica che legittima l'invio delle comunicazioni promozionali si rinviene nel legittimo interesse imputabile al titolare del trattamento che può essere anche di carattere commerciale, proprio come nel caso del marketing.

Questa deroga al principio del cd. *opt-in*[180] è fondata sulla considerazione che, nella relazione col cliente, sia ragionevole consentire alla società titolare del trattamento che ha legittimamente ottenuto l'indirizzo e-mail di tale cliente, di continuare ad utilizzarla per finalità commerciali.

---

[178] F. Pozzato, "*E-mail marketing senza consenso: il c.d. soft spam*", in "*Dirittoprivacy.com*", 2019

[179] Art. 130 Codice Privacy, comma 4

[180] Con l'opt-out è possibile trasmettere comunicazioni a tutti, tranne per chi ha disdetto la propria sottoscrizione. Con il sistema dell'opt-in, invece, si coinvolge solo chi desidera partecipare dietro consenso preventivo. M. Mandico "*Opt-in e opt-out: come funzionano le newsletter*" in "*Glistatigenerali.com*"

Inoltre, il considerando n. 47 del GDPR, che fa riferimento al marketing diretto[181] come possibile legittimo interesse, afferma che se il trattamento è basato sui legittimi interessi non occorre che vi sia il consenso dell'interessato, «*a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato, tenuto conto delle ragionevoli aspettative nutrite dall'interessato in base alla sua relazione con il titolare del trattamento*»[182].

Si tratta, in buona sostanza, del bilanciamento tra l'interesse legittimo della società titolare del trattamento e i diritti dell'interessato nell'ambito delle comunicazioni per finalità di marketing.

Spesso, inoltre, accade che i titolari del trattamento, attraverso dei moduli contrattuali cartacei o appositi *form on-line*, richiedano ai propri clienti di manifestare il consenso al trattamento dei dati personali per finalità promozionali non solo proprie ma anche di soggetti terzi, ai quali successivamente li comunicano e/o li cedono.

Il problema nasce dal fatto che spesso ciò viene svolto senza una chiara e precisa identificazione di tali soggetti terzi, né nell'informativa né nella formula di acquisizione del consenso e, talvolta, senza nemmeno l'indicazione della categoria economica o merceologica di appartenenza dei cessionari, in aperta violazione di quanto previsto dalla normativa privacy[183].

Di tali problematiche il Garante privacy si era già occupato nelle "Linee Guida in materia di attività promozionale e contrasto allo spam del 4 luglio 2013" (c.d. provv. "Antispam"), fino ad arrivare ai recenti provvedimenti

[181] Il *direct marketing* (marketing diretto) è una forma di pubblicità attraverso la quale le aziende, ma anche gli enti comunicano direttamente con clienti specifici, anche con un rapporto uno a uno, allo scopo di acquisire nuovi clienti, fidelizzarli ed eventualmente recuperarli in caso di abbandono. Tutto ciò attraverso l'utilizzo di strumenti e tecniche di comunicazione che permettano di raggiungere un target definito ed ottenere risposte oggettive misurabili, quantificabili e qualificabili, per meglio approcciarsi ai consumatori. F. Corona, "*Tutto quello che devi sapere sul marketing e GDPR*" in "*Legaldesk.it*", 2020

[182] Considerando n. 47 GDPR

[183] F. Pozzato, "*Cessione di dati personali per finalità di marketing*", in "*Dirittoprivacy.com*", 2019

emanati nei confronti di Fastweb S.p.A (25 marzo 2021) e di Iren Mercato S.p.A (13 maggio 2021)[184].

La comunicazione o cessione di dati personali a terzi per finalità di marketing presuppone che l'informativa privacy fornita dal Titolare ai sensi dell'art. 13 GDPR individui, almeno per categorie di appartenenza economiche o merceologiche, i terzi che riceveranno e utilizzeranno i dati per proprie finalità di marketing. Lo svolgimento dell'attività promozionale da parte dei cessionari dei dati richiede, inoltre, uno specifico consenso da parte dell'interessato[185], il quale va distinto da quello eventualmente già richiesto dal titolare per svolgere le sue attività promozionali. Solamente qualora l'interessato abbia rilasciato il consenso per la cessione dei propri dati a soggetti terzi per finalità di marketing, questi ultimi potranno effettuare nei suoi confronti l'attività promozionale, senza dover acquisire nuovamente il suo consenso. Il cessionario deve tuttavia fornire all'interessato l'informativa privacy c.d. successiva di cui all'art. 14 GDPR, in cui è tenuto a precisare da chi ha ricevuto i dati personali.

Queste regole devono applicarsi anche quando i soggetti terzi, ai quali si intenda comunicare e/o cedere i dati raccolti per finalità di *marketing*, siano società controllate, controllanti o comunque a vario titolo collegate con il soggetto che ha raccolto i dati personali degli interessati[186].

Per quanto riguarda i provvedimenti dell'Autorità Garante, vi è un caso molto recente, e si tratta del provvedimento con il quale l'Autorità ha ordinato a Fastweb il pagamento di una sanzione di oltre 4 milioni e 500

---

[184] A. M. Lorito, M. Defidio, "*La comunicazione dei dati personali a terzi per finalità promozionali: gli ultimi provvedimenti del Garante tra conferme e novità*", in "Dgrs.it", 2022

[185] Quando si effettuano delle attività di marketing, sia che i dati siano stati acquisiti direttamente presso l'interessato, sia che siano stati acquisiti da soggetti terzi che hanno raccolto i dati dall'interessato, è necessario che il consenso dell'interessato sia acquisito lecitamente, oltre che libero, manifesto e inequivocabile e che siano rispettati i principi previsti dal Regolamento UE 679/2016, tra cui il principio di liceità, correttezza e trasparenza del trattamento. Inoltre, il principio di accountability deve essere considerato come un caposaldo, in un'ottica di responsabilizzazione del Titolare stesso e di una corretta gestione del sistema privacy. in A. Rimoldi, "*MARKETING E TRATTAMENTO DI DATI PERSONALI: ATTENZIONE QUANDO I DATI PROVENGONO DA SOGGETTI TERZI!*" in "*Mondoprivacy.it*"

[186] F. Pozzato, "*Cessione di dati personali per finalità di marketing*", in "*Dirittoprivacy.com*", 2019

mila euro per aver trattato in modo illecito i dati personali di milioni di utenti a fini di telemarketing.

Nello specifico, centinaia di utenti avevano presentato segnalazioni e reclami lamentando continue telefonate promozionali riguardanti servizi di telefonia e internet offerti da Fastweb effettuate senza il loro consenso, facendo emergere che vari call-center abusivi stavano effettuando attività di telemarketing violando sia le disposizioni in materia di protezione dei dati personali sia le misure di sicurezza dei sistemi di gestione della clientela[187].

L'Autorità ha quindi ordinato a Fastweb di adeguare i trattamenti in materia di telemarketing e aumentare le misure di sicurezza per impedire accessi abusivi ai propri database, con il successivo divieto di utilizzare i dati contenuti nelle liste anagrafiche fornite da partner terzi, senza che questi ultimi abbiano acquisito un consenso specifico, libero e informato dagli interessati alla comunicazione a terzi dei propri dati[188].

Merita una particolare considerazione anche il provvedimento dell'11 marzo 2021, adottato nei confronti della società Mediacom S.r.l., nel quale sono contenute delle indicazioni che possono creare, per come formulate, alcuni equivoci in materia di validità del consenso per la cessione a terzi con finalità di comunicazione promozionale[189].

Con tale pronuncia, l'Autorità ha contestato la validità del consenso sul quale la società Mediacom S.r.l. fondava la legittimità del trattamento finalizzato alla cessione a terzi, per assenza di "specificità".

Come abbiamo già visto nel precedente capitolo, per essere specifico, il consenso deve essere riferito ad una precisa finalità che, nel caso in esame, è quella della comunicazione dei dati a soggetti terzi (affinché ne possano fare un "uso" promozionale): tali soggetti dovrebbero essere indicati, almeno per categorie merceologiche di appartenenza, all'interno dell'informativa privacy del titolare, al fine di garantire che il consenso risulti

[187] https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9570980
[188] M. Martorana, Z. Sichi, "*Dati utilizzati a fini di marketing*", in "*Altalex.com*", 2021
[189] Registro dei provvedimenti n. 99 dell'11 marzo 2021 - https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9577065

altresì “informato”. La specificità richiamata in questo provvedimento non riguarda tanto i destinatari quanto, invece, la specificità della finalità.
Tuttavia, risulta importante chiarire che non è sufficiente che il titolare del trattamento raccolga un consenso separato, ma è necessario anche che il metodo utilizzato per ottenere il consenso sia formulato in maniera chiara e precisa, in modo da non indurre in errore il soggetto interessato in merito alle finalità di trattamento verso le quali sta prestando il proprio consenso per il trattamento dei propri dati.
In conclusione, si può affermare che le aziende hanno il legittimo interesse a far progredire il loro business diffondendo e pubblicizzando i loro beni o servizi, ma l’utente detiene sempre e comunque il diritto di sapere come vengono usati i propri dati, perché, dove e a quali soggetti verranno eventualmente trasferiti, potendo sempre decidere se acconsentire o meno.

CAPITOLO III
GLI STRUMENTI DI RACCOLTA DEI DATI PERSONALI
3.1 - I Cookies: Definizione, funzioni e classificazione

Sia che siamo semplici utenti che navigano quotidianamente su Internet, sia che siamo proprietari di un sito web, la maggior parte di noi sa che quando visita un sito internet quest'ultimo rilascia sul nostro computer una serie di cookie che possono essere considerati delle vere e proprie tracce.
Il nome cookie deriva dalla tecnica usata in ambienti UNIX[190] sin dagli anni Ottanta e chiamata “*magic cookie*”, termine attestato la prima volta nell’ambito informatico nel 1979. A sua volta, da che cosa “*magic cookie*” prenda il nome non è chiaro: non è escluso il riferimento a una fiaba[191].
In informatica quando si parla di cookie (“biscotto” in inglese), ci si riferisce generalmente ad una tipologia specifica di cookie: i “*cookie http*”, i quali sono anche chiamati “*web cookies”* o “*browser cookies”*.

[190] “*UNIX è un sistema operativo “open source” (con licenza libera), sviluppato nel 1969 presso i laboratori Bell*”. In “*vitolavecchia.altervista.org*”
[191] A. Polimeni, “*Cookie: cosa sono, come funzionano e come proteggerti”, in “agendadigitale.eu*”, 2022.

I siti hanno iniziato ad usare questo tipo di cookie nella seconda metà degli anni ’90, e da allora i cookie hanno avuto una massiccia diffusione.
I cookie vengono creati dal server e costituiscono dei mezzi per raccogliere informazioni generate da un sito web e salvate da un browser di un utente internet sul disco rigido locale del computer o del dispositivo mobile[192]. Più precisamente, i cookie sono dei file di testo in formato *.txt* o *.xml* di piccole dimensioni (arrivano a pesare al massimo fino a 4 Kilobytes)[193]. Essi svolgono la funzione di semplificare e velocizzare gli accessi ai siti web da parte degli utenti, vengono inviati direttamente al browser dell’utente e salvati direttamente nel computer dal quale si accede alla sessione.
Questo scambio di informazioni consente ai siti di riconoscere il computer e l’utente che accede al sito e di inviargli informazioni personalizzate in base alle varie ricerche e sessioni di navigazione.
Infatti, ad ogni visita dello stesso sito web, i cookie vengono aperti ed eventualmente modificati. Questo implica una forma di violazione della riservatezza, visto che il compito di molti cookies è tenere traccia delle abitudini degli utenti del web. Per questo motivo la legislazione di molti Paesi, compresa l’Italia, obbliga i siti a richiedere agli utenti un esplicito consenso riguardante l’utilizzo dei cookies nei loro confronti.
Molti siti precisano che i cookies sono utilizzati per personalizzare l’esperienza di navigazione, ma questa può avvenire anche in modo anonimo, senza salvare informazioni sulla visita[194].
Secondo il nuovo GDPR le informazioni sugli utenti contenute nei cookies devono essere trattate e gestite come dati personali[195].
I dati salvati nei cookie non sono pericolosi di per sé, non contengono alcun tipo di virus. Il problema sta nel modo in cui un determinato sito web può utilizzare quei dati, potenzialmente violando la privacy dell’utente.

---

[192] S. Chiarloni, C. Besso, M. Bove, A. Carratta, E. D’Alessandro, A. Saletti, “*Cookie e consenso dell’utente” in “Diritto Processuale Civile*”, Giurisprudenza Italiana, 2020.
[193] M. Mancosu, “*Cosa Sono I Cookie*”, in “*ottimizzazione-pc.it*”, 2018.
[194] La maggior parte dei browser per navigare in internet offrono la possibilità della cd. “navigazione in incognito”, la quale permette di navigare normalmente nei siti web senza però salvare la cronologia di navigazione e i cookie provenienti dai vari siti.
[195] Net informatica, “*A cosa servono i cookies*”, in “*net-informatica.it*”

Senza un'adeguata sicurezza o protezione, infatti, gli hacker e i cybercriminali possono facilmente utilizzare le informazioni contenute nei cookie per estrapolare la cronologia della navigazione[196].

Esistono tanti tipi di cookie, diversi per aspetti tecnici, durata, provenienza e funzione.

La prima grande distinzione da fare riguarda i cookie di prima e di terza parte.

I cookie di prima parte vengono creati dal web server del sito che viene visitato dall'utente, e il cookie viene creato nel suo dominio, non in quello di siti terzi (la sua URL è la stessa del sito visitato). Questo tipo di cookie viene utilizzato generalmente per personalizzare l'esperienza di navigazione, riconoscendo automaticamente un utente che è già stato su quel sito (anche, ad esempio, "loggandolo" col suo username e password), recuperando e impostando le sue preferenze.

I cookie di prima parte sono leggibili solo sul dominio su cui sono stati creati, e non all'esterno. Questo vuol dire che le informazioni contenute in essi sono inefficaci per quanto riguarda l'erogazione di pubblicità personalizzata su altri siti.

I cookie di terza parte, invece, sono creati da domini diversi da quelli del sito che l'utente sta visitando (la loro URL, infatti, è diversa), e il più delle volte vengono utilizzati per il tracciamento degli utenti al fine di fornire annunci pubblicitari rilevanti e personalizzati.

Generalmente, questi cookie vengono utilizzati per monitorare e profilare gli utenti durante la navigazione, studiare i loro movimenti e le loro abitudini di consultazione del web o di consumo, ai fini del "*behavioural advertising"*. Essi vengono rilasciati da server "esterni", come server pubblicitari, servizi di *retargeting* (che seguono gli utenti che hanno precedentemente visitato un sito e mostrano loro prodotti che hanno visualizzato o con cui hanno interagito in precedenza) e pulsanti di condivisione social (che consentono agli utenti di condividere contenuti accedendo ai loro profili social).

[196] Panda Mediacenter, "*Cookie: cosa sono, come vengono usati e quando sono pericolosi*", in "*pandasecurity.com*"

I cookie di terza parte sono leggibili sia sul dominio su cui sono stati creati, sia su qualsiasi altro sito capace di leggere il codice del server che lo ha prodotto, quindi, potenzialmente, su un ampio numero di siti esterni. Ultimamente, molti browser stanno bloccando il loro utilizzo, in quanto reputano questo tipo di cookie poco controllabile dall'utente e lesivo della sua privacy.

Esistono poi anche i cookie di "seconda parte", col cui nome si indicano generalmente quei cookie che vengono trasferiti dall'azienda che li ha creati come cookie di prima parte a un'altra società, attraverso una partnership[197].

Per quanto riguarda la durata dei cookies, ci sono:

- Cookie temporanei di sessione (anche chiamati *session cookies* o *temporary cookies*): sono cookie lasciati temporaneamente nel computer dell'utente. Si cancellano automaticamente al termine della sessione di navigazione. In pratica questi cookie restano attivi soltanto mentre navighiamo in Internet. Quasi sempre servono per identificare l'utente e quindi evitare di eseguire la procedura di login ad ogni sezione del sito;
- Cookie permanenti o persistenti (anche chiamati *persistent cookie*): questo tipo di cookie resta attivo nel computer fino alla sua data di scadenza o alla sua cancellazione da parte dell'utente. Essi non vengono cancellati al termine della sessione e servono per fornire informazioni sulla navigazione al sito che li ha inviati.

Un'ulteriore distinzione da fare è quella tra cookie tecnici e *cookie analytics*. I cookie tecnici servono per poter effettuare la navigazione o a fornire un servizio richiesto sul sito internet visitato. Non vengono utilizzati per scopi ulteriori e sono normalmente installati direttamente dal titolare del sito web[198]. Senza il ricorso ai cookie tecnici alcune operazioni non potrebbero essere compiute o sarebbero più complesse e/o meno sicure, come ad esempio le attività di "*home banking"* (che comprendono la visualizzazione dell'estratto conto, i bonifici, il pagamento delle bollette, ecc.), per le quali i

[197] A. La Rosa, "*COOKIE DI PRIMA E TERZA PARTE. COSA SONO E COME FUNZIONANO*", in "*engage.it*", 2020.

[198] Garante Privacy, "*FAQ Cookie*", in "*Garanteprivacy.it*"

cookie, che consentono di effettuare e mantenere l'identificazione dell'utente nell'ambito della sessione, risultano indispensabili.

In linea di principio per l'uso di tali cookie non serve un consenso specifico ai sensi dell'art. 5, comma 3, Dir. 2002/58/CE.

I "*cookie analytics"*, invece, vengono utilizzati dai fornitori di servizi dell'informazione per raccogliere informazioni, in forma aggregata, sul numero degli utenti e su come essi visitano il sito web, ottimizzando e allineando, così, il sito web alle esigenze virtuali degli utenti.

I "*cookie analytics"* non appartengono alla tipologia dei cookie tecnici.

Il Garante della privacy nel 2016 ha tuttavia precisato che possono essere assimilati ai cookie tecnici se utilizzati a fini dell'ottimizzazione del sito direttamente dal titolare del sito stesso, il quale potrà raccogliere informazioni di tipo statistico in forma aggregata sul numero degli utenti e su come questi visitano il sito.

Qualora, invece, l'elaborazione di tali analisi statistiche sia affidata a soggetti terzi, i dati degli utenti dovranno essere preventivamente minimizzati e non potranno essere combinati con altre elaborazioni né trasmessi ad ulteriori terzi. A queste condizioni, per i *cookie analytics* valgono le stesse regole, in tema di informativa e consenso, previste per i cookie tecnici[199].

Infine, è utile menzionare anche gli "*evercookie"*, i "*cookie zombie*" e i "*supercookie*": questi, in realtà, non sono veri e propri cookie. Non costituiscono dei salvataggi di dati, ma routine in grado di autoreplicarsi anche dopo che la memoria cache del browser è stata svuotata[200].

Quando vengono eliminati, spesso sono in grado di installare copie di sé stessi in un'altra posizione. Questo è il caso dei plugin[201] video per i browser

---

[199] Garante Privacy, cfr. provvedimento dell'8 maggio 2014 e Linee guida cookie e altri strumenti di tracciamento del 10 giugno 2021

[200] "*La memoria cache è una memoria del computer. È usata come memoria interposta tra il processore (CPU) e la memoria RAM. La memoria cache è molto più veloce rispetto alla memoria RAM. È tuttavia meno capiente e più costosa*." Cit. A. Minini, "*La memoria cache*" in "*Andreaminini.com*"

[201] "*I plug-in sono piccoli programmi aggiuntivi che ampliano le funzioni delle applicazioni web e dei programmi desktop. Quando si installa un plug-in, il rispettivo software viene generalmente*

come *Microsoft Silverlight* o *Adobe Flash*, che consentono l'accesso agli stessi dati da più posizioni.

In genere, per gestire le preferenze relative ai cookie basta agire direttamente dalle impostazioni del proprio browser preferito impedendo, così, un'eventuale installazione degli stessi.

Tramite le impostazioni del proprio browser preferito è inoltre possibile eliminare definitivamente i cookie installati in passato senza correre alcun rischio, inclusi i cookie di cui è già stato dato eventualmente il consenso all'installazione. È importante però precisare che disabilitando l'installazione di tutti i cookie il funzionamento di alcuni siti potrebbe essere compromesso, con il risultato di ottenere un'esperienza di navigazione peggiore[202].

3.2 – La Normativa sui cookies

Alla luce della sempre crescente diffusione di nuove tecnologie e della loro invasività, i cookie sono da tempo al centro dell'attenzione dei Garanti privacy europei, un'attenzione che è cresciuta dopo l'entrata in vigore del GDPR[203].

Il 12 luglio 2002 è stata approvata la normativa UE sui cookie, nota anche con il nome ufficiale di Direttiva e-Privacy (dir. 2002/58/CE), la quale è stata poi sostituita dalla direttiva comunitaria 2009/136/CE.

La Direttiva e-Privacy è stata pensata per mettere in atto linee guida precise in materia di protezione dei dati con mezzi elettronici, compresi l'e-mail marketing e l'utilizzo dei cookie[204].

La finalità della direttiva era quella di far rispettare e garantire il diritto alla privacy attraverso la protezione dei dati, come sancito dalla Carta dei diritti fondamentali dell'UE, la quale stabilisce che: «*Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano*» e che «*Tali*

---

arricchito di una nuova funzione di cui prima non disponeva." Cit. Digital Guide Ionos, "Che cos'è un plug-in e per cosa si utilizza?" in "*ionos.it*"

[202] A. Barillaro, "*Cosa sono i cookie?*" in "*informaticapertutti.com*"

[203] T. Costantino, L. Liguori, G. Novellini, "*I cookie sotto la lente dei Garanti privacy: lo stato dell'arte in Italia e Ue*" in "*agendadigitale.eu*"

[204] Iubenda, "*Cookie e GDPR: cos'è davvero necessario?*", in "*iubenda.com*"

dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata»[205].

Il suo obiettivo principale era, infatti, garantire «*il rispetto della vita privata, la riservatezza delle comunicazioni e la tutela dei dati a carattere personale nel settore delle comunicazioni elettroniche*»[206].

Prima di essere abrogata definitivamente e sostituita con il più recente Regolamento e-Privacy dell'UE del 2021[207], la Direttiva e-privacy (detta anche "Cookie Law") non veniva applicata solo ai cookie, ma più in generale ad ogni tipo di tecnologia che memorizza o ha accesso alle informazioni sul dispositivo dell'utente (come *pixel tag*, impronta digitale del dispositivo, identificatori univoci, ecc.).

La "*Cookie Law"*, tuttavia, ha avuto effetti ambigui sull'esperienza di gestione dei cookie e del tracciamento da parte dell'utente, con un'attuazione giuridica a livello nazionale frammentata e talvolta inadeguata[208]. Infatti, questa direttiva, prima della modifica avvenuta nel 2009, presentava numerose criticità: in primo luogo, essa era divenuta ormai piuttosto obsoleta rispetto ai numerosi mutamenti a livello tecnologico intervenuti negli ultimi anni nel settore digitale.

In secondo luogo, il fatto che non si trattasse di un regolamento ma di una direttiva, quindi un atto non direttamente applicabile, ha implicato un'inevitabile frammentazione nelle modalità di recepimento all'interno dei diversi Stati membri. Inoltre, sono state sollevate preoccupazioni per il fatto che le implementazioni nazionali hanno creato condizioni di disparità tra le diverse realtà giuridiche. Infine, è da sottolineare la lacunosità del testo, causata anche dalla sua brevità: essa mancava di definire, infatti, numerosi aspetti salienti della materia.

Per la risoluzione delle problematiche evidenziate, sono state adottate alcune soluzioni, la prima delle quali viene posta dalla stessa direttiva che, all'art. 1, comma 2 prevedeva che «*le disposizioni della presente Direttiva*

[205] EU Charter of Fundamental Rights, art. 8, commi 1 e 2

[206] https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX%3A52017PC0010

[207] https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf

[208] Cookiebot, "*Legge UE sui cookie – Diritto alla privacy*", in "*cookiebot.com*", 2021.

precisano e integrano la Direttiva 95/46/CE», ossia la normativa (ora abrogata) che regolamentava l'ambito della privacy e che oggi è stata sostituita dal GDPR. Alla luce di ciò, e così come confermato dal parere n. 05/2019 emanato dall'EDPB[209] riguardante l'interazione tra le due normative, si riteneva che il Reg. 2016/679/U.E. fosse *lex generalis* nell'ambito in oggetto, mentre la Direttiva rimanesse *lex specialis*.

La Direttiva risultava dunque la prima normativa applicabile, mentre si ricorreva al GDPR solo in caso di lacune.

La seconda misura riguardava invece i vari pareri adottati dall'EDPB e le linee guida emanate dal WP29 che, derivando da organismi sovranazionali, risultano essere sempre vincolanti per tutti gli Stati membri, con l'obiettivo di risolvere le principali contraddizioni e lacune esistenti fornendo soluzioni uniformi alle problematiche più sentite[210].

La Direttiva e-Privacy stabiliva che nessun cookie o tracker può essere installato senza il consenso preventivo dell'utente, ad eccezione di quelli strettamente necessari per la funzionalità di base del sito.

La direttiva stabiliva poi l'obbligo di informativa e sanciva l'obbligo di comunicare agli utenti come disabilitare i cookie tramite il browser utilizzato dall'utente.

Ciò significa, in linea generale, che se il sito web fa uso di cookie è tenuto a:

- informare gli utenti che navigano nel sito che si utilizzano i cookie;
- spiegare, in modo semplice e comprensibile, come funzionano i cookie e perché vengono utilizzati;
- ottenere il consenso informato prima di memorizzare i cookie sul dispositivo dell'utente.

[209] "*Il comitato europeo per la protezione dei dati (EDPB) è un organo europeo indipendente, che contribuisce all'applicazione coerente delle norme sulla protezione dei dati in tutta l'Unione europea e promuove la cooperazione tra le autorità competenti per la protezione dei dati dell'UE*." Cit. in "edpb.europa.eu"

[210] D. Marchese, I.G. Bortolotto, "*Normativa sui cookie, uno scenario "spezzettato"*", in "*riskmanagement360.it*", 2021.

In pratica, il sito deve contenere al suo interno un "cookie banner" che deve essere mostrato alla prima visita dell'utente[211], deve predisporre e mostrare all'utente una cookie policy e permettergli di prestare il consenso, a meno che (eventualità molto improbabile) il sito non usi solo cookie esenti dall'obbligo di consenso preventivo.

Prima di aver ottenuto il consenso, nessun tipo di cookie, tranne quelli esenti, dev'essere installato o risultare attivo.

All'epoca, quindi, esisteva già l'obbligo di ottenere il consenso dall'utente, anche se esso poteva essere implicito[212].

Successivamente, la direttiva comunitaria 2009/136/CE ha modificato la direttiva 2002/58/CE, imponendo al gestore del sito web di informare l'utente del fatto che quel determinato sito web prevede l'utilizzo dei cookie, e in determinati casi ad ottenere il consenso preventivo all'uso degli stessi.

Al considerando 66 della direttiva, viene affermato che: «*possono verificarsi tentativi da parte di terzi di archiviare le informazioni sull'apparecchiatura di un utente o di ottenere l'accesso a informazioni già archiviate, per una varietà di scopi che possono essere legittimi (ad esempio alcuni tipi di marcatori, «cookies») o implicare un'intrusione ingiustificata nella sfera privata (ad esempio software spia o virus)*». Inoltre, è considerato di fondamentale importanza il fatto che gli utenti vengano informati in modo chiaro e completo nel momento in cui compiono un'attività che potrebbe implicare l'archiviazione o l'ottenimento dell'accesso. Si specifica anche che *«le modalità di comunicazione delle informazioni e di offerta del diritto al rifiuto dovrebbero essere il più possibile chiare e comprensibili. Eccezioni all'obbligo di comunicazione delle informazioni e di offerta del diritto al rifiuto dovrebbero essere limitate a quei casi in cui l'archiviazione tecnica o l'accesso siano strettamente necessari al fine legittimo di consentire l'uso*

---

[211] "*Il banner di consenso ai cookie è un avviso che viene mostrato su molti siti e app alla prima visita dell'utente. Ha lo scopo di informare gli utenti della presenza di eventuali cookie, dei loro diritti a riguardo e di chiederne il consenso all'installazione. Disporre di un cookie banner e di una cookie policy e bloccare i cookie prima di aver ottenuto il consenso dell'utente sono tutti requisiti previsti dalla Direttiva ePrivacy (Cookie Law) e dal GDPR*." Cit. in "Cookie banner – Requisiti, cosa scriverci e come crearne uno", in "iubenda.com"

[212] B. Saetta, "*Cookie law*", in "*protezionedatipersonali.it*"

di un servizio specifico esplicitamente richiesto dall'abbonato o dall'utente».
Sempre secondo il considerando n. 66, il consenso dell'utente al trattamento dei propri dati può essere espresso mediante le impostazioni di un motore di ricerca o di un'altra applicazione, se tecnicamente fattibile ed efficace. Infine, si afferma che «*l'esecuzione di detti requisiti dovrebbe essere resa più efficace tramite i maggiori poteri conferiti alle autorità nazionali competenti*».

La direttiva europea del 2009, che avrebbe dovuto essere recepita entro il 25 maggio del 2011 nelle legislazioni nazionali, si limitava a creare un quadro normativo all'interno del quale erano, eventualmente, i singoli Garanti nazionali a definire una regolamentazione di dettaglio.

Questo perché la direttiva in sé non spiega come dovrebbe essere fornita l'informativa né come dovrebbe configurarsi il consenso, precisando solo alcuni dettagli. Ciò ha comportato una frammentazione nell'attuazione della legislazione, in quanto i singoli Garanti potevano prevedere modalità attuative differenti[213].

In ambito nazionale, tale normativa è stata recepita dall'art. 122 del Codice Privacy italiano (D. Lgs 196/2003).

La normativa europea non è entrata subito in vigore per i ritardi dei Garanti nazionali nel predisporre la regolamentazione di dettaglio. L'8 maggio del 2014 anche il Garante per la Protezione dei Dati Personali italiano, come già in precedenza avevano fatto altri Garanti europei, ha emanato il Provvedimento "Individuazione delle modalità semplificate per l'informativa e l'acquisizione del consenso per l'uso dei cookie[214]" (Gazzetta Ufficiale n. 126 del 3 giugno 2014), contenente le regole sulle modalità di adempimento agli obblighi di rilascio dell'informativa e di acquisizione del consenso degli utenti in caso di utilizzo di cookie. Il provvedimento è entrato in vigore il 3 giugno del 2015[215].

La normativa, e il relativo provvedimento del Garante, si applica a tutti i siti che, a prescindere dalla presenza di una sede nel territorio dello Stato,

[213] B. Saetta, "*Cookie law: come è nel resto d'Europa*", in "*valigiablu.it*", 2015.
[214] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3118884
[215] B. Saetta, "*Cookie law*", in "*protezionedatipersonali.it*"

installano cookie nei dispositivi degli utenti, utilizzando quindi per il trattamento "strumenti situati sul territorio dello Stato"[216].

È da precisare che i cookie che vengono installati sul computer dell'utente si considerano come “strumenti situati nel territorio italiano” utilizzati al fine del tracciamento dell'utente. La normativa si applica anche alla navigazione da smartphone, tablet e vari dispositivi mobili, e non solo relativamente ai cookie, ma anche a tutti gli strumenti analoghi che consentono l'identificazione del dispositivo usato dall'utente.

L’evoluzione del quadro normativo europeo costituisce un chiaro rimprovero alle aziende che utilizzano termini di servizio poco chiari, troppo complessi e difficili da comprendere, ma anche a quelle che tendono a modificare troppo spesso i termini di servizio, determinando incertezza negli utenti su ciò che accade ai propri dati personali.

Il GDPR va a chiarire alcuni aspetti sui cookie, rafforzando la tutela dei dati delle persone. Il Considerando n. 30 menziona espressamente i cookie: «*Le persone fisiche possono essere associate a identificativi online prodotti dai dispositivi, dalle applicazioni, dagli strumenti e dai protocolli utilizzati, quali gli indirizzi IP, a marcatori temporanei (cookies) o a identificativi di altro tipo. Tali identificativi possono lasciare tracce che possono essere utilizzate per creare profili delle persone fisiche e identificarle*[217]*.*»

C’è anche il considerando n. 26 che, pur non menzionandoli, ci aiuta a capire che i cookie sono dati pseudonimi, e quindi dati personali, dove gli elementi identificativi vengono sostituiti da altri elementi quali stringhe di testo e numeri.

L’ultima novità normativa riguarda l’introduzione del cd. Regolamento e-Privacy del 2021, il quale nasce come proposta di regolamento da parte del Consiglio dell'UE, finalizzato a disciplinare tutte le comunicazioni elettroniche su servizi e reti disponibili al pubblico da parte di individui all'interno dell'Unione europea.

[216] Art. 5, comma 2, del Codice privacy
[217] Considerando n. 30 GDPR

Il 10 gennaio del 2017 era stata presentata all'Unione Europea la prima proposta del Regolamento sulla privacy, ma si sono riscontrate evidenti difficoltà nel trovare un testo al regolamento, dovute soprattutto alle divergenze tra la Commissione UE, il Parlamento UE e il Consiglio UE[218].
Il 10 febbraio del 2021 il Consiglio UE ha finalizzato e pubblicato la bozza finale del Regolamento e-Privacy. Sono poi iniziati i negoziati tra il Consiglio europeo, il Parlamento europeo e la Commissione per la pubblicazione del testo definitivo. La versione finale del regolamento e-Privacy potrà essere ragionevolmente pubblicata nel 2023 e potrà definitivamente entrare in vigore nel 2025 (a distanza di due anni, così com'è avvenuto per il GDPR).
Il Regolamento e-Privacy si inserisce nel quadro normativo sin qui esposto consolidandolo e, al tempo stesso, espandendolo.
Questo regolamento rimanda al codice delle comunicazioni elettroniche e precisamente alla Direttiva (UE) 2018/1972 dell'11 dicembre 2018.
La proposta di regolamento richiama espressamente le definizioni stabilite dai seguenti testi normativi:

- GDPR
- Direttiva (UE) 2018/1972 dell'11 dicembre 2018 che istituisce il codice europeo delle comunicazioni elettroniche;
- Direttiva 2008/63/CE della Commissione, del 20 giugno 2008, relativa alla concorrenza sui mercati delle apparecchiature terminali di telecomunicazione;
- Direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio del 9 settembre 2015 che prevede una procedura d'informazione nel settore delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione (codificazione) [219].

È necessario precisare che Il GDPR protegge i dati personali delle persone all'interno dell'UE, mentre il Regolamento e-Privacy andrà a tutelare la riservatezza delle comunicazioni elettroniche delle persone nell'UE, adattando e trasponendo il GDPR (e i suoi standard di consenso) al settore

[218] Legalblink, "*Regolamento ePrivacy: il testo definitivo*", in "*legalblink.it*", 2022.
[219] N. Fabiano, "*ePrivacy, a che punto siamo? Ecco lo stato dell'arte*", in "*agendadigitale.eu*", 2022.

della comunicazione tramite tecnologie quali Facebook, e-mail, messaggi di testo ecc.

Il 9 marzo 2021, il Comitato europeo per la protezione dei dati (EDPB) si è pronunciato sul Regolamento ePrivacy. L'Autorità ha sottolineato che il Regolamento e-Privacy deve integrare l'attuale GDPR fornendo ulteriori garanzie sulla riservatezza e la protezione di tutte le comunicazioni elettroniche.

L'EDPB ha evidenziato, altresì, che:

- è necessario ottenere un consenso autentico ed espresso liberamente: questo dovrebbe impedire ai siti di utilizzare pratiche sleali come le soluzioni di tipo "prendere o lasciare", che rendono l'accesso ai servizi e alle funzionalità subordinato al consenso dell'utente alla memorizzazione delle informazioni;
- è necessario includere nel Regolamento e-Privacy una norma esplicita contro il trattamento dei dati da parte dei siti che prescinda dal consenso dell'utente. Inoltre, devono essere implementati mezzi efficaci per accettare o rifiutare la profilazione;
- il Regolamento ePrivacy dovrebbe impedire di richiedere plurimi consensi agli utenti, quando non strettamente necessario[220].

Si può affermare che il Regolamento e-Privacy 2021 costituisce la *lex specialis* del GDPR, che invece rappresenta la *lex generalis*. Ciò significa che il nuovo Regolamento e-Privacy integra il GDPR con disposizioni che si applicheranno specificamente al settore delle comunicazioni elettroniche[221].

Con il regolamento e-Privacy, l'ambito di applicazione della protezione dei dati viene esteso, sul piano oggettivo, alle comunicazioni elettroniche che non costituiscono o ricomprendono dati personali e, sul piano soggettivo,

[220] Legalblink, "*Regolamento ePrivacy: il testo definitivo*", in "*legalblink.it*", 2022

[221] Cookiebot, "*Il Regolamento ePrivacy dell'UE e i cookie | Aggiornamenti 2021 Regolamento ePrivacy*", in "*cookiebot.com*"

alle informazioni riferite alle persone fisiche e giuridiche[222] che si trovano nel territorio UE[223].

Lo schema che verrà adottato prevede una regola generale sulla riservatezza dei dati relativi alle comunicazioni elettroniche e il divieto di qualsiasi interferenza con i medesimi (captazione, memorizzazione, monitoraggio, ecc.) da parte di chiunque non sia l'utente finale interessato: i margini consentiti dal Regolamento e-Privacy per l'impiego dei cookie e altri sistemi di tracciamento, pertanto, rappresentano eccezioni a tale regola.

Dopo la sua approvazione, il regolamento andrà a precisare e integrare il GDPR, nonché a tradurne i principi in regole specifiche.

Il centro nevralgico della tutela degli utenti è rappresentato, ancora una volta, dal consenso (il Regolamento e-Privacy richiama la disciplina del GDPR). Il consenso degli utenti finali sarà, infatti, condizione imprescindibile per il trattamento di qualsiasi tipo di comunicazione elettronica e del suo contenuto.

Nella bozza del regolamento viene precisato che, qualora sia possibile e fattibile, il consenso potrà essere espresso utilizzando le relative impostazioni tecniche di un software immesso sul mercato.

Si aggiunge anche che il consenso espresso direttamente dall'utente finale prevale sulle impostazioni del software e dovrà essere direttamente attuato, senza ulteriori ritardi.

Qualora, poi, il fornitore non sarà in grado di identificare la persona interessata, il protocollo tecnico che dimostra che il consenso è stato fornito dall'apparecchiatura terminale viene ritenuto sufficiente a dimostrare il consenso dell'utente finale[224].

Così com'è per il GDPR, anche nel regolamento "e-Privacy" il consenso potrà essere revocato: è previsto infatti l'obbligo di ricordare agli utenti finali

[222] L'art. 4a del regolamento "e-Privacy" richiama la disciplina del consenso prevista nel GDPR, aggiungendo che essa si applicherà anche alle persone giuridiche.

[223] J. Baieri, E. Lazzara, "*I cookie nel Regolamento e-Privacy: ecco tutte le novità*", in "*Altalex.com*", 2021.

[224] N. Fabiano, "*ePrivacy, a che punto siamo? Ecco lo stato dell'arte*", in "*agendadigitale.eu*", 2022.

la possibilità di revocare il consenso a intervalli periodici di non più di 12 mesi, finché il trattamento continua, a meno che non sia lo stesso utente finale a richiedere di non ricevere tali promemoria.

Proprio riguardo al consenso si registra un passo avanti rispetto al GDPR, in quanto il regolamento e-Privacy prevede chiaramente che il consenso (esplicito, liberamente prestato e non condizionato) possa essere espresso mediante software.

Con il Regolamento e-privacy si cercherà di rispondere ad un'ulteriore esigenza: cioè quella di estendere le norme anche ai cd. "*Over The Top*" (OTT), cioè Google, Amazon, Facebook e in generale aziende che forniscono contenuti e servizi attraverso la rete che non rientravano nell'ambito di applicazione della direttiva 2002/58/CE.

Con l'E-Privacy le norme si applicheranno, inoltre, anche all'IoT[225] (*Internet of Things*) e al mondo M2M[226] (*Machine to Machine*).

3.3 - Le linee guida e la raccolta del consenso tramite cookies

Le autorità di controllo nazionali hanno pubblicato varie raccomandazioni e linee guida relativamente alla normativa sui cookie.

---

[225] "L'espressione Internet of Things è stata formulata per la prima volta nel 1999, in stretta relazione con i dispositivi RFId (Radio Frequency Identification), dall'ingegnere inglese Kevin Ahston, cofondatore dell'Auto-ID Center di Massachussetts.
Per Internet of Things (IoT) o Internet delle Cose si intende quel percorso nello sviluppo tecnologico in base al quale, attraverso la rete Internet, potenzialmente ogni oggetto dell'esperienza quotidiana acquista una sua identità nel mondo digitale. L'IoT si basa sull'idea di oggetti "intelligenti" tra loro interconnessi in modo da scambiare le informazioni possedute, raccolte e/o elaborate." Cit. Politecnico di Milano – Dipartimento di Ingegneria Gestionale, "INTERNET of THINGS (IoT) Significato, esempi, ambiti applicativi e prospettive di mercato in Italia" in "blog.osservatori.net"

[226] "La comunicazione machine-to-machine, in breve M2M, rappresenta lo scambio di informazioni prevalentemente automatico tra apparecchiature tecniche quali macchine, dispositivi automatici, veicoli o strumenti di misura (ad esempio contatori di corrente elettrica, gas e acqua) tra loro oppure mediante un sistema di elaborazione dati centrale.
Nonostante generalmente non si verifichi alcun intervento umano, non si esclude che possa esservi una limitata interazione umana. Altre definizioni di M2M si concentrano sugli aspetti tecnici e sul funzionamento della comunicazione. Machine-to-machine descrive pertanto un dispositivo che rileva un evento e lo trasmette a un'applicazione tramite una rete. Tale applicazione ha il compito di tradurre l'evento trasmesso in un'informazione comprensibile." Cit. Ionos, *"Comunicazione Machine-to-machine (M2M): definizione, caratteristiche e vantaggi"* in "ionos.it"

In data 26 novembre 2020, il Garante Privacy aveva dato avvio alla pubblica consultazione sulle nuove "Linee Guida sull'utilizzo dei cookie e di altri strumenti di tracciamento". La consultazione si è conclusa in data 10 gennaio 2021 ed è divenuta operativa il 10 giugno 2021.

L'esigenza di predisporre delle linee guida nasce dall'esperienza che il Garante ha maturato circa gli effetti riscontrati sulle esperienze di navigazione, sui diritti e sulle tutele degli interessati e sulla ormai crescente diffusione di nuove tecnologie che spingono gli utenti a moltiplicare le proprie identità digitali con il rischio che le informazioni che rendiamo disponibili nel web vengano raccolte anche attraverso l'incrocio di dati che pian piano permettono di creare profili sempre più dettagliati[227].

Con le "Linea Guida cookie e altri strumenti di tracciamento" del 10 giugno 2021, il Garante per la Protezione dei Dati Personali ha fornito importanti chiarimenti in merito alla disciplina vigente sui cookies, adeguandola alle ultime novità normative, in particolare al GDPR. Infatti, il documento è volto ad aggiornare le indicazioni contenute nel provvedimento n. 229/2014[228].

Le principali novità contenute nelle nuove linee Guida riguardano le basi giuridiche del trattamento dei dati raccolti con i cookies e con gli altri strumenti di tracciamento, la regolamentazione della "zona grigia" che finora aveva permesso di adottare pratiche ai limiti della liceità, la responsabilità del Titolare del trattamento, il banner, l'acquisizione del consenso[229]. Il Garante ha riconosciuto che dalle nuove Linee guida possono derivare interventi tecnici anche piuttosto complessi e, per tale motivo, ha individuato un termine per permettere ai titolari del trattamento di adeguarsi, scaduto il 9 gennaio 2022[230].

---

[227] A. Citterio, "*Utilizzo di cookie e altri strumenti di tracciamento, le linee guida del Garante", in "riskmanagement360.it*", 2021

[228] "*Il Garante, con il provvedimento n. 229/2014, ha dichiarato il divieto di installazione dei cookie per finalità di profilazione e marketing da parte dei gestori dei siti senza aver prima informato gli utenti e aver ottenuto il loro consenso. Chi naviga on line può quindi decidere in maniera libera e consapevole se far usare o no le informazioni raccolte sui siti visitati per ricevere pubblicità mirata.*" Cit. A. Lombardo, "*Internet, Garante Privacy: no ai cookie per profilazione senza consenso*", in "*Altalex.com*", 2014.

[229] La cd. "zona grigia" è rappresentata da tutti quei servizi che rilasciano cookie di profilazione.

[230] V. Pandolfini, "*La regolamentazione dei cookies alla luce delle nuove Linee guida del Garante del 2021: come strutturare la cookie policy e il banner*", in "*assistenza-legale-imprese.it*", 2022.

L'obiettivo primario delle nuove linee guida sui cookie è quello di rafforzare il potere decisionale degli utenti riguardo all'uso dei loro dati personali durante la navigazione on line[231].

Con le nuove linee guida, il consenso all'installazione dei cookie di profilazione deve necessariamente corrispondere ad un atto positivo inequivocabile riconoscibile e registrabile da parte del titolare[232]. Ciò significa che il consenso deve essere richiesto palesemente all'utente, attraverso un banner chiaro e semplice che indichi tutte le modalità per accettare o rifiutare i cookie, altri eventuali soggetti a cui sono destinati i dati personali raccolti e il loro tempo di conservazione.

Il consenso, inoltre, non deve essere solo richiesto e accettato ma anche registrato nell'apposito "Registro Preferenze Cookie", che il titolare del sito web deve tenere per conservare tutte le preferenze raccolte e per eventuali verifiche future[233].

L'unica eccezione viene fatta per quei siti web che utilizzano esclusivamente cookie tecnici, ossia, come abbiamo visto in precedenza, quei cookie che vengono attivati per la trasmissione delle comunicazioni e nella misura strettamente necessaria a fornire il servizio richiesto dall'utente. In questo caso non sarà necessario predisporre un banner informativo, basterà indicare semplicemente nell'home page del sito o all'interno dell'informativa privacy che lo stesso utilizza esclusivamente cookie tecnici. Per quanto riguarda invece i *cookie analytics* (necessari per verificare l'efficacia di un servizio), essi devono essere utilizzati puramente a scopi statistici e in forma anonima.

Per garantire un'adeguata libertà di scelta all'utente, il Garante ha previsto l'adozione di un meccanismo in base al quale l'utente, accedendo per la prima volta ad un sito web, visualizzi immediatamente un banner contenente una "X" selezionabile in alto a destra, le cui dimensioni siano tali da costituire una percettibile discontinuità nella fruizione dei contenuti della

---

[231] A. Nucara, "*Nuove Linee Guida sui Cookies: cosa cambia?*", in "*privacylab.it*", 2022.

[232] Garante per la protezione dei dati personali, "*Linee guida cookie e altri strumenti di tracciamento – 10 giugno 2021*", par. 6.1

[233] Infodati, "*Nuova normativa sui cookie in vigore dal 10/01/2022*", in "*infodati.it*", 2022.

pagina web che sta visitando, ma anche tali da evitare il rischio che l'utente possa far ricorso a comandi e dunque compiere scelte indesiderate o inconsapevoli[234], (ad esempio, cliccando erroneamente sulla "X" di chiusura). Per questi motivi, le dimensioni del banner dovranno essere parametrate anche in base ai diversi dispositivi che l'utente potrebbe utilizzare per accedere al sito web. La "X" di chiusura dovrà inoltre avere la stessa evidenza grafica degli altri pulsanti forniti all'utente per selezionare le varie opzioni.

Il banner dovrà poi consentire in modo immediato, usabile e accessibile sia di proseguire la navigazione senza prestare alcun consenso, sia di acconsentire all'utilizzo di cookie di profilazione o strumenti di tracciamento non tecnici.

Proprio perché il banner deve causare una percettibile discontinuità nella fruizione del sito web e per le considerazioni che si sono dette sopra, la chiusura dello stesso tramite il click sulla "X" dovrà impedirne la riproposizione per un periodo di almeno sei mesi, salvo le eccezioni, specificate dal Garante, in cui può essere reiterata la richiesta di consenso. In questo modo si evita di inondare l'utente di eccessive richieste che rischierebbero di minare la percezione del valore del contenuto del banner[235].

L'Autorità elenca gli elementi che costituiscono il contenuto minimo del banner, ossia:

- l'avvertenza che la chiusura del banner cliccando sulla "X" comporterà il permanere delle impostazioni predefinite, senza pregiudicare la continuazione della navigazione in assenza di cookie o altri strumenti di tracciamento diversi da quelli tecnici;
- l'informativa minima, che specifica se vengono utilizzati cookie o altri strumenti tecnici e che cookie e strumenti di altro tipo potranno essere selezionati tramite i comandi appositamente forniti;

[234] A. Nucara, "*Nuove Linee Guida sui Cookies: cosa cambia?*", in "*privacylab.it*", 2022.
[235] M. Martorana, R. Savella, "*Cookie, nuove linee guida del Garante Privacy: 6 mesi per adeguarsi*", in "*Altalex.com*", 2021.

- il link all'informativa estesa, che deve essere reperibile anche nel *footer*[236] di ogni pagina e deve consentire all'interessato di accedere all'informativa tramite un solo click;
- un comando per esprimere il consenso al posizionamento di tutti i cookie o impiego di tutti gli strumenti di tracciamento;
- il link a un'ulteriore area in cui potranno essere selezionati analiticamente i cookie di profilazione o gli strumenti di tracciamento non tecnici, anche in base ai soggetti (di prima o di terze parti) e alle funzionalità, nell'ottica di consentire all'interessato di fornire un consenso specifico per ogni singolo trattamento.

Oltre al banner, dovrà essere presente nel *footer* delle varie pagine del sito web un apposito *link* che consenta di accedere ad un'area tramite cui l'utente potrà modificare, in qualsiasi momento, le scelte compiute in relazione ai cookie e agli altri strumenti di tracciamento.

Il Garante suggerisce inoltre di posizionare in ciascuna pagina del dominio un segno grafico, un'icona o qualsiasi altro accorgimento tecnico che indichi all'utente lo stato dei consensi prestati.

Infine, nel rispetto del principio di accountability sancito dall'articolo 24 del GDPR, tutte le azioni e le scelte degli utenti dovranno essere documentate da parte del titolare, anche attraverso l'utilizzo di appositi cookie tecnici. Inoltre, le nuove linee guida specificano che non sarà più possibile utilizzare metodi come:

- il "*cookie wall*", che consiste in una tecnica utilizzata dai siti web per negare l'accesso agli utenti che non acconsentano a tutti i cookie e tracker presenti su un determinato sito. In pratica si tratta di una sorta di barriera che mette l'utente in una situazione di "prendere o lasciare", in cui questi deve scegliere di accettare i cookie di

[236] "*Il footer è la parte conclusiva di un sito web, di solito contraddistinta da una sezione di colore differente che mostra una differenza cromatica con il resto del sito web*." Cit. R. Esposito, "*Cos'è il footer di un sito e come migliorarlo*", in "*mysocialweb.it*", 2021.

marketing e simili tecnologie di tracciamento, oppure vedersi precluso l'accesso al sito web e ai relativi servizi[237];

- lo "*scrolling"* (o lo *swiping* nel caso di dispositivi dotati di *touch screen*), il quale rappresenta una metodologia per l'ottenimento del consenso che si basa sullo scorrimento di una pagina web per eliminare il banner che si presenta all'ingresso dell'utente[238].

Il Garante poi, dedica un apposito paragrafo delle Linee guida ai *cookie analytics*. Nelle precedenti indicazioni del Garante, per la disciplina dei *cookie analytics*, era necessario distinguere tra cookie di prima parte, assimilabili a quelli tecnici, e cookie di terze parti, per i quali era possibile un'equiparazione ai cookie tecnici solo laddove i dati fossero anonimizzati. Nelle nuove linee guida viene ribadita la stessa regola, evidenziando le criticità dovute alla possibile aggregazione di dati, che potrebbe compromettere l'anonimizzazione[239].

3.4 – I Big Data e la privacy

È noto a tutti come l'evoluzione delle tecnologie per raccogliere dati, analizzarli e adottare decisioni correlate comporti delle sfide complesse e anche molti problemi, i quali non sono solo tecnologici, ma anche sociali, giuridici ed etici, sotto il profilo della individuazione e della responsabilità dei soggetti che utilizzano i dati, attualmente attestati su un "regime di sostanziale autodichia[240]", ma anche della legittimità e dei limiti della profilazione degli utenti, delle concentrazioni di mercato, dell'accesso fraudolento a dati sensibili, dell'influenza politica e sociale che lo sviluppo delle piattaforme di intelligenza artificiale può determinare[241].

---

[237] Cookiebot, "*Cookie wall, Linee guida dell'EDPB sui cookie wall e il consenso valido*", in "*cookiebot.com*", 2021.

[238] Startup Legal Team, "*SCROLLING, COOKIE WALL E CONSENSO VALIDAMENTE PRESTATO: IL CHIARIMENTO DEL GARANTE EUROPEO*" in "*startuplegal.it*", 2020.

[239] M. Martorana, R. Savella, "*Cookie, nuove linee guida del Garante Privacy: 6 mesi per adeguarsi*", in "*Altalex.com*", 2021.

[240] L'autodichia è la facoltà, di cui godono alcuni organi costituzionali, di decidere autonomamente ed in deroga al principio di separazione dei poteri i ricorsi avanzati dai propri dipendenti avverso atti di amministrazione prodotti dagli organi stessi.

[241] A. C. Di Landro, "*Big Data, Rischi e tutele nel trattamento dei dati personali*" ESI, 2020.

La più grande sfida che la maggior parte delle aziende deve affrontare oggi consiste nella capacità di acquisire un vantaggio competitivo lavorando sui dati. Tutte le aziende e tutte le Pubbliche Amministrazioni ormai sono diventate delle grandi "fabbriche di dati". Noi stessi contribuiamo costantemente, consapevolmente e spesso anche inconsapevolmente, alla produzione di dati[242].

Con l'espressione "*Big Data*" si fa riferimento ad una raccolta di dati digitali di grosse dimensioni, spesso eterogenei tra loro, che vengono acquisiti, elaborati e gestiti quotidianamente da società e aziende in tutto il mondo[243].

L'acquisizione dei dati avviene attraverso vari canali: tramite API[244] (ovvero interfaccia di programmazione di un'applicazione) utilizzate appositamente per raccogliere dati quando si accede ad un sito, con software appositi per la raccolta di documenti, importando dati da database preesistenti oppure interpretando ed estrapolando il flusso di dati che passa attraverso la rete, oppure ancora tramite i cookie attivati durante la navigazione web.

Al di là dei flussi di dati prodotti dai sistemi informatici e dalle infrastrutture a supporto della produzione, della distribuzione e dell'erogazione dei servizi, i big data sono un fenomeno associato a un'evoluzione massiva delle abitudini quotidiane della popolazione. Come abbiamo già affermato in precedenza parlando dei cookie, ogni volta che utilizziamo un computer, accendiamo lo smartphone o apriamo un'applicazione, sempre e comunque lasciamo delle tracce, costituite dai nostri dati.

I Big Data, ad esempio, provengono dai sensori integrati in migliaia di oggetti che, collegati alla rete, oggi chiamiamo "*Internet of Things".* Secondo il *McKinsey Global Institute* questi sensori oggi ammontano a già più di 30 milioni, vengono utilizzati nel settore automobilistico[245], industriale, nei

---

[242] M. Bellini, "*Big data: cosa sono, come utilizzarli, soluzioni ed esempi applicativi*", in "*bigdata4innovation.it*", 2022.

[243] Intelligenzaartificiale.it, "*Big Data, cosa sono?*", in "*intelligenzaartificiale.it*".

[244] Le API (Application Programming Interfaces) sono interfacce che permettono alle applicazioni di comunicare con altre applicazioni.

[245] Ad esempio, sono sempre più diffusi i cd. "veicoli connessi" chiamati anche con l'acronimo CAV ("*Connected and Automated Vehicles*"), per i quali l'EPDB, all'interno delle linee guida, dà una specifica definizione: "*i CAV sono veicoli dotati di numerose centraline elettroniche di controllo (ECU), collegate tra loro tramite una rete di bordo, e dotati di sistemi di connettività*

servizi pubblici, o nella vendita al dettaglio e il numero ogni anno lievita del 30%[246].

La definizione di Big Data non è però sufficiente per poter offrire un quadro completo del fenomeno. L'importanza dei big data, infatti, non ruota intorno alla loro quantità ma all'utilizzo che ne consegue.

Governare i processi di elaborazione e gestione dei dati non è affatto un compito semplice; la capacità di estrarre dai dati informazioni che abbiano un significato e siano funzionali, richiede infatti lo sviluppo di sofisticate tecnologie e di competenze interdisciplinari che operino a stretto contatto[247].

L'insieme delle tecniche utilizzate per l'analisi dei dati prende il nome di "*Data mining*". L'espressione indica proprio l'insieme di tutte quelle tecniche di estrazione delle informazioni estrapolate da grandi quantità di dati grazie a programmi e algoritmi adatti a questo scopo[248].

La finalità di tale analisi è quella di utilizzare le informazioni ottenute dall'estrazione dei dati in ambito scientifico, in quello aziendale, nel settore pubblico come in quello privato, sia sul piano giuridico che su quello economico e sociale[249]. Si pensi, ad esempio, a tutte quelle aziende che grazie all' analisi dei "*Big Data*" riescono ad orientare meglio le loro scelte produttive o anche ai *policy maker* che da questa analisi sono in grado di ottenere una conoscenza della realtà tale da riuscire a proporre politiche più consapevoli ed efficaci.

---

funzionali a consentire lo scambio di informazioni con altri dispositivi, sia all'interno che all'esterno dei veicoli stessi". I CAV, in particolare, raccolgono sia dati funzionali a consentire un'identificazione diretta dell'interessato, sia dati che ne consentono un'identificazione indiretta, attraverso l'incrocio di diverse banche dati.

Fra questi vi sono i dettagli dei viaggi fatti, i dati relativi alle modalità di utilizzo del veicolo (come lo stile di guida del conducente e le distanze percorse), oltre che i dati tecnici della macchina.

Oppure, un altro dispositivo che può essere installato all'interno di un autoveicolo, è la Dash Cam ("*dashboard camera*") la quale è un dispositivo elettronico per l'acquisizione di immagini. Viene posizionata all'interno dell'autovettura, precisamente sul parabrezza (rivolta verso l'esterno) per permettere di registrare gli eventi che accadono all'esterno.

[246] Redazione di Digital4marketing, "*Big Data: cosa sono e come le aziende competono con gli Analytics*", in "*digital4.biz*"

[247] I. Pattelli, "Privacy, sicurezza ed etica nell'utilizzo dei Big Data e dell'Intelligenza Artificiale", in "ictsecuritymagazine.com", 2021.

[248] Enciclopedia Treccani, voce "Data Mining".

[249] I. Cecere, "Il fenomeno dei big data e la protezione dei dati personali", in "4clegal.com", 2021.

Il concetto di "*Big Data*" si è diffuso in particolar modo agli inizi degli anni 2000, precisamente nel 2001, quando l'analista Douglas Laney, allora vicepresidente e *Service Director* dell'azienda Meta Group, definì in un report il modello che descrive in modo sintetico i Big Data con 3V[250]:

- Volume: rappresenta la dimensione effettiva del "*dataset*"[251]; l'ampio volume di dati che è possibile raccogliere oggi potrebbe apparentemente rappresentare un problema. In realtà quello del volume dei Big Data è un falso problema, in quanto grazie ai servizi di *cloud computing*[252] la gestione del grosso volume di dati disponibili viene semplificata, e con essa i processi di raccolta, immagazzinamento e accesso ai dati.
- Velocità: questa variabile è riferita alla rapidità con cui i dati affluiscono in tempo reale ed alla conseguente necessità di utilizzarli in modo tempestivo.
- Varietà: si riferisce alla natura dei dati, i quali possono essere:
  a) strutturati, cioè organizzati con lunghezza e formato definiti;
  b) semi strutturati (o semi organizzati): la loro principale caratteristica è quella di contenere informazioni sufficienti per consentire ai dati di essere catalogati, cercati e analizzati in modo più efficiente rispetto ai dati strettamente non strutturati[253].
  I file di registro costituiscono un tipico esempio di questo tipo di dati;
  c) non strutturati, cioè dati non organizzati, i quali, quindi, non si adattano perfettamente alla tradizionale struttura di righe e colonne del database relazionale. Testi, immagini e video costituiscono alcuni

[250] Assoknowledge, "Big Data", in "*assoknowledge.org*"
[251] "In informatica, il dataset è l'insieme di dati organizzati in forma relazionale. Ha una struttura tabellare, dove di solito ogni colonna rappresenta una variabile e ogni riga corrisponde a una osservazione. È usato anche in statistica." cit. In "Enciclopedia Treccani"
[252] "Con il termine Cloud Computing si intende una tipologia di servizi erogati via internet e accessibili da remoto. L'utente non ha bisogno di acquistare il software e installarlo sul proprio pc; infatti, è sufficiente collegarsi tramite browser. Non è costretto inoltre a sostenere un costo fisso: il prezzo varia, infatti, a seconda del tipo di consumo, che può subire cambiamenti di volta in volta." Cit in "Servizi Cloud Computing: cosa sono, caratteristiche e tipologie" in "apkappa.it", 2021.
[253] V. Lavecchia, "Differenza tra dati strutturati, non strutturati e semi-strutturati", in "vitolavecchia.altervista.org",

esempi di dati non strutturati che non possono essere archiviati sotto forma di righe e colonne.

Oggi si parla di 5V, infatti il paradigma di Laney è stato arricchito dalle variabili di:

- Veridicità: l'operazione di organizzazione dei dati non sempre si rivela semplice, poiché vengono a crearsi delle incongruenze, ridondanze, inconsistenze nella gestione dei dati stessi. Le masse di dati sono inoltre molto variabili e dinamiche e provengono da fonti diverse creando una potenziale confusione. In un mondo di dati così eterogenei è difficile stabilire cosa sia giusto e cosa sia sbagliato. La veridicità indica quindi il livello di affidabilità o inaffidabilità dei dati.
- Valore: questa è una variabile fondamentale perché l'importanza dei big data stessi è racchiusa nella possibilità di essere utili per le aziende quindi di portare dei benefici. Infatti, i dati fini a sé stessi non hanno alcuna importanza. Per essere davvero utili devono poter essere convertiti in informazioni preziose che permettono alle aziende di verificare ed eventualmente modificare le sue mosse[254].

A fronte dell'innumerevole quantità di informazioni, molte delle quali non risultano utili ai fini della successiva analisi, i Big Data devono essere accuratamente selezionati ed archiviati. Per questo motivo, nel corso negli ultimi anni, sono stati studiati e realizzati sistemi in grado di immagazzinare dataset di grandi dimensioni.

Oltre a computer sempre più capaci sia nella potenza della CPU, per una maggiore capacità elaborativa, sia nelle memorie di massa, esiste un elemento fondamentale per la creazione e la fruizione di questa enorme mole di dati: gli algoritmi.

Gli algoritmi sono, per definizione, quell'insieme di passi e istruzioni che consentono la risoluzione di un problema; nel caso dei Big Data gli algoritmi vengono creati per poter consentire uno studio del flusso dei dati, la loro analisi ma soprattutto il loro confronto, al fine di estrarre il risultato cercato. È per questa ragione che devono essere sempre più parametrici, multilivello

[254] Flyip, "LE 5V DEI BIG DATA: LE CARATTERISTICHE DI UNA MASSA DI DATI", in "flyip.it", 2020.

e precisi[255]. I Big Data, infatti, non avrebbero alcun valore se non fosse possibile analizzarli ed estrapolare informazioni fondamentali per studi futuri e questo può essere fatto solamente utilizzando gli algoritmi, ormai parti integranti delle scelte aziendali, non solo per quanto riguarda il marketing ma anche per la produzione, la manutenzione e la selezione del personale. Di conseguenza, negli ultimi anni il termine "intelligenza artificiale" si è imposto anche nel campo del marketing e delle strategie aziendali.

Con tale termine si intende la capacità di far svolgere alle macchine delle funzioni che sono tipiche dell'azione umana[256].

Per analizzare i Big Data, le organizzazioni utilizzano sempre più tecniche di analisi avanzate, predittive e prescrittive, che utilizzano spesso l'intelligenza artificiale e il *Machine Learning*[257] (ML) in particolare, per comprendere e raccomandare azioni basate sull'analisi di elevati volumi di dati da più fonti, interne o esterne[258].

Un altro aspetto che riguarda l'intelligenza artificiale è rappresentato dal *Recommendation System*[259], che riesce ad intuire le preferenze dell'utente in modo da personalizzare gli annunci e le informazioni che verranno mostrati.

---

[255] Intelligenzaartificiale.it, "Big Data, cosa sono?", in "intelligenzaartificiale.it".

[256] "L'intelligenza artificiale (IA) è un insieme di tecnologie differenti che interagiscono per consentire alle macchine di percepire, comprendere, agire e apprendere con livelli di intelligenza simili a quelli umani." Cit. in Accenture, "*Cos'è l'intelligenza artificiale*?" in "*accenture.com*", 2022.

[257] "*Il Machine Learning, o apprendimento automatico, è un ambito dell'Intelligenza Artificiale che racchiude metodi e tecniche che negli anni si sono sviluppati nel campo della matematica, della statistica e dell'informatica. In ambito informatico il Machine Learning può essere definito come una sorta di variante della programmazione tradizionale con cui i sistemi apprendono in modo autonomo senza istruzioni esplicite e regole predeterminate nel codice.*
Serve quando non è possibile risolvere i problemi progettando e programmando algoritmi espliciti e per funzionare necessita di grosse moli di dati e di infrastrutture affidabili, facilmente scalabili e con grandi capacità di risorse." Cit. in Itimpresa, "*Machine Learning e Deep Learning: quali sono le differenze*?", in "*it-impresa.it*", 2021.

[258] I. Pattelli, "Privacy, sicurezza ed etica nell'utilizzo dei Big Data e dell'Intelligenza Artificiale", in "ictsecuritymagazine.com", 2021.

[259] "*Per "Recommendation System" si intende un sistema software che ha il compito di prevedere quanto è forte l'interesse di un utente nei confronti di un oggetto, al fine di essere in grado di consigliare l'oggetto che più lo interessa. Un "Recommendation System" valuta sulla base del comportamento precedente, come ad esempio gli ordini precedenti nel medesimo shop, quanto sia forte l'attrazione che determinati prodotti esercitano su di un utente, per poi automaticamente cercare dei prodotti simili e potenzialmente ugualmente interessanti." Cit. in Ionos, "Recommendation System nel mondo e-commerce*", in "ionos.it", 2020.

Al giorno d'oggi il processo di analisi dei dati non può essere affrontato con le stesse metodologie utilizzate in passato poiché gli scenari, così come gli utenti, sono cambiati, ed il *data management* non può prescindere da considerazioni di base.

Innanzitutto, le fonti dalle quali hanno origine i Big Data sono in continua evoluzione e quindi un sempre maggior numero di informazioni arrivano e necessitano di essere analizzate in maniera rapida e precisa individuando anche le nuove fonti per includerle nelle piattaforme di *management*. Fino a pochissimi anni fa era impensabile poter gestire rapidamente ed a bassi costi una mole molto elevata di dati, ma grazie a nuove tecnologie come "Apache Hadoop", oggi tutto questo è possibile[260].

"Apache Hadoop" è un software open source ed è riconosciuto come la piattaforma di riferimento nell'ambito della gestione e della distribuzione dei big data.

Questo software è stato concepito per scrivere facilmente applicazioni che elaborano grandi quantità di dati in parallelo, su cluster di grandi dimensioni (costituiti da migliaia di nodi). Hadoop offre librerie che permettono la suddivisione dei dati da elaborare direttamente sui nodi di calcolo e permette di ridurre al minimo i tempi di accesso, questo perché i dati sono immediatamente disponibili alle procedure senza pesanti trasferimenti in rete.

Il *framework*[261] di Hadoop garantisce inoltre un'elevata affidabilità: le anomalie e tutti gli eventuali problemi del sistema sono gestiti a livello applicativo anziché utilizzare sistemi hardware per garantire alta disponibilità[262].

La presenza di questa enorme quantità di dati incoraggia le riflessioni sul tema della protezione dei dati personali e sulle tutele giuridiche collegate ai

---

[260] Intelligenzaartificiale.it, "*Il Data Management ed Apache Hadoop*" in "*intelligenzaartificiale.it*".

[261] "*In informatica, un framework è un sistema che consente di estendere le funzionalità del linguaggio di programmazione su cui è basato, fornendo allo sviluppatore una struttura coerente ed efficace al fine di effettuare azioni e comandi in modo semplice e veloce*." Cit. Redazione Reteinformaticalavoro, "*Framework: cosa sono e quali dominano le classifiche*", in "*reteinformaticalavoro.it*", 2020.

[262] G. Esposito, "*Introduzione ad Hadoop Apache*", in "*html.it*"

"Big Data" quando, una volta prodotti, vengono diffusi e messi a disposizione di chi trae vantaggio dalla loro analisi.

Attualmente, nei Paesi membri della UE, sappiamo che la normativa di riferimento in materia di protezione dei dati è il GDPR, il quale, sin dal Considerando n.1, specifica che "*la protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale […]*" dando immediatamente un'idea chiara dell'importanza di un simile tema.

Alla luce di ciò, il GDPR mira a fare in modo che il livello di protezione dei diritti e delle libertà delle persone fisiche, con riguardo al trattamento di tali dati, possa raggiungere pari livello in tutti gli Stati membri allo scopo di assicurarne una tutela elevata e coerente attraverso l'applicazione delle norme in materia di protezione dei dati personali.

Per raggiungere tale scopo, il Regolamento si pone come garante della certezza del diritto e trasparenza agli operatori economici, comprese le micro, piccole e medie imprese ed offre alle persone fisiche in tutti gli Stati membri il medesimo livello di diritti azionabili, di obblighi e responsabilità dei titolari del trattamento. Inoltre, il GDPR assicura un controllo coerente del trattamento dei dati personali, sanzioni equivalenti in tutti gli Stati membri e una cooperazione efficace tra le autorità di controllo all'interno di questi ultimi[263].

Sappiamo che uno dei capisaldi del GDPR è l'informativa sulla privacy da sottoporre all'interessato, in cui vengono chiaramente comunicate le finalità relative all'utilizzo dei dati prima ancora che questo abbia concretamente inizio.

Nell'ambito dei Big Data, invece, i dati vengono spesso trattati con scopi definiti solo in termini generali e le finalità non vengono, in realtà, individuate all'inizio.

Anche il metodo classico in base al quale il dato viene ottenuto direttamente dall'interessato dopo il suo consenso al trattamento va a scontrarsi con il

[263] I. Cecere, "*Il fenomeno dei big data e la protezione dei dati personali*", in "*4clegal.com*", 2021

fenomeno dell'acquisizione massiva di dati personali che il fenomeno dei Big Data comporta.

Eppure, proprio il GDPR rappresenta uno strumento capace di indicare la direzione anche al settore dei Big Data. Infatti, pur non trattando direttamente di tale materia, rappresenta, ad oggi, il corpo di norme più completo e moderno in fatto di riservatezza dei dati ed è in grado di arginare gli abusi anche nel settore dei Big Data.

Centrali, per il fenomeno dei Big Data, sono i temi riguardanti l'informativa da sottoporre agli interessati e i moduli di raccolta dei consensi, i quali devono essere in linea con i principi normativi: una descrizione non precisa, non corretta oppure generica delle finalità del trattamento dei dati, rende invalido il consenso.

Importante, sempre per quanto riguarda i Big Data, è che si crei il giusto equilibrio tra gli obiettivi del titolare e del responsabile del trattamento dei dati e gli obiettivi degli interessati.

Per questi motivi, è fondamentale che chi intende avvalersi di Big Data consideri il tema della protezione dei dati molto prima di avviare la fase di raccolta delle informazioni.

A questo punto, subentra il concetto di *Privacy by design*[264], che richiama l'attenzione dei titolari del trattamento sull'esigenza che la protezione dei dati personali venga garantita fin dalla fase di progettazione della raccolta.

Questo significa che il titolare non sarà in regola con la normativa privacy se applicherà misure di protezione standard a tipologie diverse di trattamento. Ma, al contrario, dovrà sempre eseguire un'analisi specifica del singolo contesto di riferimento, tenendo conto delle modalità di impiego dei dati raccolti, delle finalità per cui verranno utilizzati in azienda, delle tecnologie impiegate e dei vari soggetti coinvolti nel loro trattamento[265], nonché dei rischi specifici che possono derivare da quel trattamento per i diritti degli interessati (sui quali si dirà infra nel prossimo paragrafo).

---

[264] Art. 25 GDPR

[265] Itimpresa, "*GDPR e Big Data, la privacy nel trattamento automatizzato di grandi quantità di dati*" in "*it-impresa.it*", 2020.

In conclusione, considerando le nuove e sempre più numerose sfide che comportano le innovazioni tecnologiche, oltre all'aumento esponenziale del numero dei dati che chiunque può generare e mettere in circolazione, si può affermare che sia particolarmente rilevante la necessità di raggiungere un livello di tutela sempre maggiore dei dati personali per evitare abusi, pericoli e violazioni di un diritto che, al giorno d'oggi, risulta fondamentale per ognuno di noi.

3.5 – I rischi per la sicurezza dei dati online e alcune misure da adottare

Il web, nella società odierna, fa parte della nostra quotidianità. Internet, infatti, fornisce l'accesso a numerosi servizi e contenuti, le comunicazioni e le informazioni avvengono in tempo reale senza limiti territoriali, l'uso di Internet e dei social network è agevole e alla portata di tutti sia sotto il profilo tecnico sia sotto il profilo economico[266].

Secondo una ricerca effettuata nel 2019, si è stimato anche che gli italiani in media navigano ogni giorno circa sei ore da diversi dispositivi. Mentre è di circa 35 milioni il numero di italiani attivi sui social network, di cui circa 31 milioni ne fa uso da un dispositivo mobile, la media giornaliera del tempo che una persona passa sui social network è di circa 1 ora e 51 minuti[267].

I nostri dati personali, come già sappiamo, vengono raccolti e trattati in tanti modi diversi su internet, comportando spesso alcuni rischi[268].

A livello globale, le minacce informatiche continuano a evolversi rapidamente e il numero di violazioni di dati personali aumenta ogni anno.

---

[266] D. Di Leo, "*I rischi dei social network: dal phishing al cyberbullismo, i consigli per difendersi*", in "*cybersecurity360.it*", 2022.

[267] Ricerca di DIGITAL 2019: https://wearesocial.com/it/blog/2019/01/digital-in-2019/

[268] A questo proposito, è utile precisare che "*il titolare del trattamento deve adottare tutte le precauzioni utili, in relazione alla natura dei dati e ai rischi del trattamento, per preservare la sicurezza dei dati, e in particolare prevenirne l'accesso non autorizzato, l'alterazione o la perdita (artt. 5 e 32 GDPR). Per valutare i rischi del trattamento occorre prima di tutto identificare gli eventi temuti e valutarli in termini di gravità e probabilità. A seguito di tale stima potranno essere identificate le misure tese a eliminare o ridurre i rischi correlati. Non tutti i rischi possono essere eliminati del tutto, in alcuni casi sarà possibile solo ridurli, e la valutazione sulle misure proporzionate da implementare (oppure eventualmente la scelta di non procedere col trattamento) fa parte della "responsabilizzazione" del titolare del trattamento.*" Cit. B. Saetta, "*Gestione del rischio nel contesto della privacy*", in "*protezionedatipersonali.it*", 2021.

Il primo problema riguarda la trasparenza: quando noi forniamo informazioni per accedere a servizi online, pensiamo generalmente che i nostri dati personali verranno utilizzati dal titolare del trattamento unicamente per gestire la nostra richiesta o il processo in corso (ad esempio, una transazione bancaria, un ordine su un sito di e-commerce, ecc.). Tuttavia, spesso questi dati sono utilizzati anche per altri scopi e, proprio per questo motivo, nella privacy policy del titolare a cui stiamo comunicando i dati dovrebbe esserci una chiara specificazione.

Mentre compiliamo un *form* di raccolta dati, dovremmo avere a disposizione un *link* o veder comparire un "*pop-up*" che ci conduca alla sezione "Privacy" del sito web, dove dovrebbe apparire un'informativa al trattamento completa, chiara e semplice come previsto dal GDPR, con la descrizione dei possibili altri usi dei dati personali[269].

Sappiamo che, molto spesso, i dati personali comunicati per una finalità ben precisa vengono utilizzati (dal Titolare o da terze parti) anche per creare un identikit del nostro profilo, monitorando le nostre attività on line e, di conseguenza, arricchendo i nostri interessi. Il tutto serve poi a personalizzare le pubblicità che troviamo sul sito stesso oppure quando visitiamo altri siti o utilizziamo le varie applicazioni.

Alcune organizzazioni non rispettano i requisiti di trasparenza rispetto ai molteplici usi dei dati personali raccolti e non attribuiscono la giusta importanza all'esercizio dei diritti degli interessati[270]. Un esempio di questo comportamento scorretto è tipicamente rappresentato dalle privacy policy stilate in modo troppo generico e ambiguo, che indicano nelle finalità: "Utilizziamo i tuoi dati personali per migliorare il nostro servizio", senza fornire ulteriori dettagli.

Queste descrizioni molto vaghe non sono sufficienti e accettabili, in quanto non consentono all'utente di capire cosa intende fare il titolare con i dati personali che raccoglie. Altre anomalie frequenti nelle informative sono ad esempio la totale omissione dei vari tipi di trattamenti eseguiti, oppure il

[269] F. Fornasiero, "*Dati personali: i pericoli più comuni della rete e come evitarli*", in "*agendadigitale.eu*", 2022.
[270] GDPR, art. 15 e art. 22

tentativo di nascondere finalità particolari dietro scopi secondari e istituzionali (quali “ricerca e sviluppo, analisi statistica”).

Per cercare di tutelarsi da questo rischio è necessario che gli utenti del web siano consapevoli del fatto che ogni titolare del trattamento ha il dovere di essere chiaro rispetto all’uso dei dati che vengono forniti durante la navigazione.

Ogni utente dovrebbe prendersi il giusto tempo per leggere l’informativa sulla privacy e capire come i dati personali vengono utilizzati dal servizio al quale ci si sta iscrivendo e, in presenza di poca chiarezza o dubbi, valutare se effettivamente si desidera utilizzare tale servizio.

Le insidie possono trovarsi anche nei “pop up” o nei link denominati “leggi di più” che possono comparire in fase di iscrizione o di installazione in caso di app e che spesso non vengono consultati.

In generale, sarebbe opportuno evitare di fornire i propri dati personali ad un servizio online senza conoscere la modalità di utilizzo dei dati del servizio stesso, oppure fornire solo la quantità minima di dati personali necessari (in genere indicati con la dicitura “campi obbligatori”) per aderire al servizio che si desidera utilizzare[271].

Un altro rischio riguarda la non corretta classificazione dei cookie da parte del titolare del sito. Deve essere presente una Cookie Policy chiara e completa che spieghi in modo semplice quali cookie sono strettamente necessari per utilizzare il servizio e quali sono, invece, facoltativi.

Nei siti a norma di legge, i cookie non necessari possono essere accettati o rifiutati subito o anche in seguito, attraverso uno specifico link nel sito che riconduce l’utente alla finestra dei consensi.

Sappiamo già che un modo per proteggersi è offerto direttamente dalle impostazioni del browser che stiamo utilizzando, le quali ci permettono di modificare le nostre preferenze sulla gestione dei cookie.

Sicuramente però, i pericoli principali per un comune utente del web sono il furto dei propri dati personali e le truffe online.

[271] R. Razzante, “*I nostri dati nel web Quali i rischi*” in “*ilgiorno.it*”, 2022.

La vastità del tema e il grado attuale di pericolo, ci mostrano come la sicurezza informatica[272] sia molto importante per cercare di evitare di incorrere nelle "trappole" dei cybercriminali.

Una delle misure di sicurezza di base più efficaci da attuare riguarda un metodo che può risultare per certi versi banale, ma che spesso viene sottovalutato: l'uso di password sicure. Anche se possono apparire lunghe, poco intuitive e difficili da ricordare, risultano molto efficaci in termini di protezione dei propri dati[273].

Le password andrebbero create con una certa complessità e dovrebbero avere caratteristiche che le rendano difficili da indovinare, sia da parte di umani che di bot[274]. A volte, per la creazione di account in determinati siti web, è necessario che la password rispetti una determinata lunghezza, oppure che contenga almeno un numero, una lettera maiuscola o un carattere speciale. Alcuni servizi inoltre possono anche richiedere che le password siano aggiornate a intervalli regolari (Ad esempio, il sito dell'Università di Padova).

Per un maggiore livello di sicurezza, è fondamentale non riutilizzare la medesima password per l'accesso ai diversi siti web. Inoltre, esistono alcuni servizi che permettono di gestire tutte le password che un utente utilizza nei vari siti web, come il servizio "Kaspersky Password Manager" offerto dall'omonimo antivirus, che permette di memorizzare le varie password, di

---

[272] "*La cybersicurezza, conosciuta come sicurezza informatica o sicurezza delle informazioni elettroniche, è l'insieme dei mezzi e delle tecnologie destinati alla difesa di computer, server, dispositivi mobili, sistemi elettronici, reti e dati dagli attacchi dannosi. Si applica a vari contesti, dal business al mobile computing, e prevede il coinvolgimento di elementi tecnici, organizzativi, giuridici e umani*." Cit. in Softech, "*Human & Cybersecurity, Gestire il rischio informatico con tecnologie e consapevolezza*" in "*softech.it*", 2019.

[273] Ionos, "*Sicurezza informatica: proteggersi al meglio mentre si naviga su Internet*", in "*ionos.it*", 2019.

[274] "*In ambito informatico i bot (abbreviazione di robot) sono dei software che, accedendo alla rete e sfruttando gli stessi canali utilizzati da utenti in carne ed ossa, sono in grado di svolgere i compiti più vari in maniera completamente autonoma, grazie all'intelligenza artificiale e al machine learning*" Cit. in "*Cosa sono e come funzionano i bot per computer e smartphone*" in "*tecnologia.libero.it*"

categorizzarle e di accedere ad esse attraverso una password master lunga e sicura[275].

Però per una protezione di base completa sono indispensabili anche altri strumenti per la sicurezza informatica, che dovrebbero diventare degli standard per tutti gli utenti. Ad esempio, un *firewall* è imprescindibile: può essere presente sul computer e/o sul modem/router, l'importante è che venga sempre utilizzato. Infatti, un firewall serve ad impedire un eventuale accesso non autorizzato sul proprio computer o sulla propria rete.

Un firewall risulta particolarmente efficace se combinato con un programma antivirus che non si limita solo a rilevare virus, trojan e altre tipologie di malware, ma che riesce anche ad eliminarli o a risolvere la situazione velocemente. Inoltre, eseguire la scansione del proprio pc ad intervalli regolari alla ricerca di minacce informatiche è una prassi che spesso si sottovaluta e dovrebbe rientrare a far parte delle pratiche da impiegare per garantire la sicurezza informatica del proprio sistema[276].

Il software antivirus che noi installiamo nel nostro pc, ovviamente, non può proteggere contro ogni minaccia, ma eliminerà e rimuoverà la maggior parte dei malware, perciò bisognerebbe accertarsi che sia aggiornato.

È necessario quindi assicurarsi di essere al passo con gli aggiornamenti del sistema operativo, dell'antivirus e delle applicazioni che si utilizzano[277].

3.5.1 – Il Phishing

Un altro dei maggiori e più diffusi rischi che devono affrontare gli utenti del web è il fenomeno del phishing.

Il phishing è un genere di truffa telematica che ha l'obiettivo di rubare le informazioni e i dati personali degli utenti. Phishing deriva dal termine

---

[275] "*La password master è una singola password utilizzata da Kaspersky Password Manager per proteggere tutti i dati, incluse altre password. La password master viene creata durante la configurazione iniziale di Kaspersky Password Manager. Ogni volta che si tenta di accedere all'archivio credenziali per i dati, Kaspersky Password Manager richiede la password master. Per motivi di sicurezza, Kaspersky Password Manager non memorizza la password master in alcun dispositivo, né nell'archivio cloud.*" Cit. in "*support.kaspersky.com*", 2022.

[276] Ionos, "*Consigli per una maggiore sicurezza: come porre fine al furto dei dati*", in "*Ionos.it*"

[277] Kaspersky, "*La top 10 delle regole di sicurezza su Internet e cosa non fare online*", in "*kaspersky.it*", 2022.

inglese "*fishing*" che significa, per l'appunto, pescare, e infatti con tale attività, un soggetto cerca di appropriarsi di informazioni quali: numeri di carte di credito, dati relativi ad account, password o altre informazioni di natura personale, convincendo l'utente a fornirle mediante alcune tecniche di ingegneria sociale, attraverso le quali vengono studiate ed analizzate le abitudini delle vittime, al fine di carpirne potenziali informazioni utili.

Tale condotta integra, in primo luogo, il reato di trattamento illecito di dati personali di cui all'art. 167 del Codice privacy che, a seconda della gravità, prevede diverse sanzioni. In secondo luogo, tale fattispecie è punibile ai sensi dell'art. 630-ter c.p. comma 3 che, per la prima volta ha inserito nel Codice penale il concetto di identità digitale.

Il legislatore per il reato di "frode informatica commessa con sostituzione di identità digitale" ha previsto la pena della reclusione da due a sei anni e la multa da 600 euro a 3.000 euro nel caso in cui il fatto sia commesso mediante furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti; per tale delitto è prevista la querela della persona offesa salvo che ricorra l'ipotesi di cui al II o III comma dell'art. 640-ter ovvero altra circostanza aggravante.

La tecnica più diffusa per portare a termine un attacco di phishing consiste nell'inviare delle normali e-mail, con sembianze e caratteristiche molto simili a quelle riscontrabili su siti web noti e particolarmente diffusi come, ad esempio, istituti bancari, istituti postali, e servizi di pagamento online.

Oltre a questa tecnica ne esistono anche altre, le quali sono meno frequenti ma pur sempre efficaci:

- lo *spear phishing*: consiste in un attacco molto più mirato e preciso rispetto al semplice *phishing*. Le e-mail vengono scritte a regola d'arte, su misura per ogni vittima. Il *phishing* e lo *spear phishing* hanno dei tratti in comune, ma anche delle differenze sostanziali. Entrambi hanno come obiettivo quello di spingere le vittime a divulgare informazioni sensibili. Tuttavia, lo "*spear phishing"* richiede molto più sforzo ai truffatori, in quanto, per poter creare un'e-mail che

contenga elementi in grado di renderla credibile agli occhi del bersaglio è necessaria un'accurata ricerca sulla potenziale vittima[278];

- lo *smishing*: è una forma di phishing che utilizza i telefoni cellulari come piattaforma di attacco. Il criminale compie l'attacco con l'intento di raccogliere informazioni personali, compresi il codice fiscale e/o il numero di carta di credito. Lo *smishing* viene attuato attraverso messaggi di testo o SMS, da cui il nome "*SMiShing*". Questa forma di attacco è diventata sempre più popolare a causa del fatto che le persone sono più propense a fidarsi di un messaggio che arriva sul loro telefono attraverso un'app di messaggistica piuttosto che da un messaggio consegnato tramite e-mail[279];
- il *whaling*: Il *whaling* (caccia alle balene) è un tipo di *phishing* ancora più specifico e mirato. Consiste in una recente e ambiziosa tecnica che prende di mira dirigenti e vertici aziendali quali CEO[280], CFO[281], CIO[282] e in generale tutti quei profili, comunemente identificabili come C-Level, che all'interno di un'azienda sono in possesso sia di informazioni strettamente riservate che di elevati poteri decisionali e di spesa. L'obiettivo è quello di manipolare la vittima inducendola con l'inganno a divulgare informazioni in suo possesso o a fargli compiere specifiche azioni dannose per l'azienda ma remunerative per l'attaccante, come ad esempio autorizzare un bonifico a beneficio di quest'ultimo[283];
- il *vishing*: ha lo stesso obiettivo delle altre tipologie di attacchi di *phishing*, ma viene eseguito tramite una chiamata vocale (da qui la "v" al posto delle lettere "ph" nel nome).

---

[278] Proofpoint, "*Gli attacchi spear phishing*", in "*proofpoint.com*", 2022.
[279] Trend Micro Incorporated, "*Che cos'è lo smishing?*", in "*trendmicro.com*", 2022.
[280] CEO è l'acronimo inglese per "*Chief executive office*", termine che indica in tutto il mondo la figura corrispondente a quella che in Italia definiamo Amministratore delegato.
[281] Il CFO (*Chief Financial Officer*) è il manager responsabile della gestione delle attività finanziarie di un'azienda.
[282] Il CIO (*Chief Information Officer*) è il responsabile delle tecnologie inerenti all'informazione e alle comunicazioni aziendali.
[283] L. Gobbi, "*Attacchi whaling: la "caccia informatica alle balene" che minaccia CEO, CFO e tutti i C-Level*", in "*cybersecurity360.it*", 2020.

Questo tipo di truffa telefonica viene attuata attraverso le tecniche di ingegneria sociale, ossia una serie di tecniche che fanno leva su sentimenti innati nelle persone, quali la fiducia, la paura, l'avidità o l'altruismo. Il criminale informatico cerca di evocare questi sentimenti, suscitando panico o altre emozioni che potrebbero offuscare la capacità di giudizio della vittima, e ne approfitta per sottrarle denaro o dati sensibili[284].

Esistono alcune regole per difendersi da queste tipologie di attacchi:

1. Controllare sempre il link e il mittente della mail prima di cliccare qualunque indirizzo.
2. Prima di cliccare su un qualunque link, bisogna verificare che l'indirizzo mostrato sia davvero lo stesso indirizzo Internet al quale il link condurrà. Il controllo può essere effettuato in modo semplice, passando il mouse sopra il link stesso.
3. Usare solo connessioni sicure. Si consiglia di non sfruttare connessioni sconosciute né tantomeno le reti wi-fi pubbliche, senza una password di protezione. Se vogliamo usufruire di una maggiore sicurezza, abbiamo l'opportunità di installare una VPN[285].
4. Controllare che la connessione sia HTTPS[286] e verificare il nome del dominio all'apertura di una pagina. Questi fattori sono importanti soprattutto quando si usano siti che contengono informazioni sensibili, come pagine per l'online banking, i negozi online, i social media ecc.

---

[284] N26, "*Vishing: cos'è e come difendersi*", in "*n26.com*", 2021.

[285] "*Una VPN (Virtual Private Network) consente di creare una rete privata virtuale che garantisce privacy, anonimato e sicurezza dei dati attraverso un canale di comunicazione riservato tra dispositivi che non necessariamente devono essere collegati alla stessa LAN.*" Cit. S. Lombardo, "*VPN: cos'è, come funziona e a cosa serve una Virtual Private Network*", in "*cybersecurity360.it*", 2022.

[286] "*L'abbreviazione HTTPS sta per "Hypertext Transfer Protocol Secure", tradotto: "Protocollo di trasferimento per ipertesti sicuro". Con questo protocollo la comunicazione tra client web e server web è crittografata, per impedire a terzi non autorizzati di intercettare la comunicazione, consultando ad esempio il traffico della rete WLAN.*
Il server web viene autenticato inviando, all'inizio della comunicazione, un certificato al client web, che certifica l'affidabilità del dominio. Questa misura è utile per combattere la frode da parte di siti web falsi." Cit. Ionos, "*HTTPS: cosa significa e perché è così importante*", in "*ionos.it*", 2020.

5. Non condividere mai i propri dati sensibili con una terza parte. Le compagnie ufficiali non chiedono mai informazioni del genere via e-mail[287].

CAPITOLO IV – CASI SPECIFICI

4.1 – Il caso di Facebook e Cambridge Analytica

Nel 2014, Aleksandr Kogan, docente di psicologia a Cambridge, attraverso l'app "*This is your digital life*" collegata a Facebook, è riuscito ad ottenere la profilazione di 270.000 utenti, che ignari hanno dato il consenso per partecipare ad un'indagine a fini esclusivamente accademici[288].

Quest'app permetteva agli utenti di ottenere profili psicologici e previsionali del proprio comportamento sottoponendosi ad alcuni quiz. Per poterla utilizzare bisognava solamente registrarsi effettuando il login tramite Facebook. Una volta effettuato l'accesso al proprio account Facebook, si accettava la condizione che il sito ottenesse alcuni dei dati personali tra i quali: nome, cognome, e-mail, sesso ed età. Inoltre, la piattaforma aveva accesso anche ai dati riguardanti la rete delle amicizie[289].

Attraverso tale applicazione, la società di Kogan, la *Global Science Research* (GSR), ha raccolto oltre 270.000 iscrizioni e dati di più di 50 milioni di utenti del social[290].

Kogan fu quindi in grado di costruire un archivio enorme, comprendente informazioni sul luogo in cui vivono gli utenti, i loro interessi, fotografie e aggiornamenti di stato pubblici.

I problemi sono nati successivamente, quando Kogan ha condiviso tutte queste informazioni con Cambridge Analytica, violando i termini d'uso di Facebook. Il social network vieta infatti ai proprietari di app di condividere

[287] R. Rijtano, "*Phishing, cos'è e come proteggersi: la guida completa*", in "*cybersecurity360.it*", 2022.
[288] Tim, "*Cambridge Analytica – Facebook e lo scandalo dei dati personali*", in "*timbusiness.it*", 2021.
[289] S. Della Piazza, "*Il caso Cambridge Analytica*", in "*dirittoconsenso.it*", 2021.
[290] La stima proviene dal New York Times e dal Guardian

con società terze i dati che raccolgono sugli utenti[291], pena la sospensione dell'account.

Cambridge Analytica è un istituto di ricerca fondato da Robert Mercer[292] nel 2013 con l'obiettivo di occuparsi delle strategie di comunicazione politica per finalità elettorali e per "affrontare il vuoto nel mercato politico repubblicano negli Stati Uniti"[293].

Questo istituto è specializzato nell'analisi psicometrica[294] degli utenti dei social network: a partire dall'analisi dei "mi piace" lasciati su Facebook, gli esperti sono cioè in grado di costruire il profilo comportamentale e le caratteristiche più salienti della personalità di ogni singolo utente. Maggiore è il numero di "mi piace" analizzati, più sarà preciso il profilo psicometrico realizzato[295].

Questo modo di operare viene definito dalla stessa azienda "*microtargeting* comportamentale" (o *microtargeting* psicografico[296]), il quale consiste in una metodologia di raccolta e analisi di una grande quantità di dati aggregati, che permette di elaborare profili dei singoli utenti e, di conseguenza, mostrargli dei contenuti personalizzati, capaci di fare non soltanto leva su interessi e comportamenti delle persone (come fanno gli altri sistemi di marketing), ma addirittura sulle emozioni[297].

Secondo Christopher Wylie, ex dipendente di Cambridge Analytica e fonte del Guardian, del New York Times e di Channel 4 su questa vicenda,

---

[291] E. Menietti, "*Il caso Cambridge Analytica, spiegato bene*", in "*ilpost.it*", 2018

[292] Robert Mercer è un miliardario imprenditore statunitense con idee molto conservatrici che tra le altre cose è uno dei finanziatori del sito d'informazione di estrema destra *Breitbart News*, diretto da Steve Bannon (consigliere e stratega di Trump durante la campagna elettorale e poi alla Casa Bianca).

[293] Così ha affermato Alexander Nix, ex CEO di Cambridge Analytica, in un'intervista.

[294] "*La psicometria è l'insieme dei metodi d'indagine psicologica che tendono al raggiungimento di valutazioni quantitative del comportamento umano o animale*." Cit. in "*Enciclopedia Treccani*".

[295] R. Mantovani, "*Digital Life Il caso Facebook e Cambridge Analytica in 7 domande e risposte*", in "*focus.it*"

[296] "*La psicografia è lo studio e la classificazione dei consumatori in base al loro comportamento, atteggiamento, valori e scelte di vita. Esistono vari parametri che permettono di classificare le caratteristiche psicografiche dei consumatori, ma alcuni sono decisamente più diffusi di altri. Solitamente si analizza: la personalità degli utenti, il loro stile di vita, i loro interessi, le loro opinioni e i loro valori (come, ad esempio, l'attenzione per la salvaguardia dell'ambiente o dei diritti degli animali).*" Cit. in "*mailsenpai.com*"

[297] S. Sorte, "*Facebook, lo scandalo Cambridge Analytica spiegato in modo semplice*", in "*digitalflow.it*", 2020.

Facebook era al corrente della violazione nei confronti dei suoi termini d'uso fin dal 2016, senza che vi sia mai stato alcun intervento.

In base al GDPR, tale omissione avrebbe comportato una grave violazione della normativa in quanto non sarebbe stato rispettato uno degli obblighi previsti a carico di Facebook, titolare del trattamento[298].

In particolare, il titolare, deve comunicare l'evento all'autorità di controllo, a meno che "*sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche*".

Tale comunicazione deve avvenire "*senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza*"[299].

Il passaggio di informazioni dall'applicazione di Kogan a Cambridge Analytica era avvenuto, tra l'altro, senza che gli utenti fossero stati informati riguardo all'utilizzo che sarebbe stato effettuato nei confronti dei loro dati e senza che avessero prestato il proprio consenso.

Nonostante vi fossero già da anni articoli giornalistici che denunciavano la raccolta illecita di dati personali da parte di Cambridge Analytica, lo scandalo è esploso solamente nel marzo del 2018 in seguito alle dichiarazioni rese proprio da Christopher Wylie: «*Abbiamo sfruttato Facebook per raccogliere i profili di milioni di persone. E abbiamo costruito modelli per sfruttare ciò che sapevamo su di loro e mirare ai loro demoni interiori. È su questa base che l'intera società è stata costruita*»[300]. ha dichiarato l'ex dipendente.

Come sostengono anche i legali dell'azienda, temendo una sospensione fu la stessa Cambridge Analytica ad autodenunciarsi con Facebook, dicendo di avere scoperto di essere in possesso di dati ottenuti in violazione dei termini d'uso e di averne disposto subito la distruzione. Se così fosse, però, non è chiaro perché Facebook abbia deciso di sospendere Cambridge Analytica solo venerdì 16 marzo

[298] Per un approfondimento sul tema si rimanda a http://www.dirittoconsenso.it/2018/01/07/la-privacy-e-il-trattamento-dei-dati-personali/ e a http://www.dirittoconsenso.it/2021/11/26/il-gdpr/

[299] Garante Privacy, "*Violazioni di dati personali (data breach) in base alle previsioni del Regolamento (UE) 2016/679*", in "*garanteprivacy.it*"

[300] C. Wylie, "*Il Mercato Del Consenso*", Longanesi, 2019.

Il 16 marzo 2018 Facebook decise di sospendere l'account di Cambridge Analytica, dichiarando di aver ricevuto delle segnalazioni sull'uso improprio di alcuni dati raccolti sulla piattaforma.

Nel 2016 il comitato di Donald Trump affidò a Cambridge Analytica la raccolta dei dati per la sua campagna presidenziale[301].

Jared Kushner, il genero di Donald Trump, aveva assunto un esperto informatico, Brad Pascale, che era poi stato contattato da Cambridge Analytica per fargli provare le loro tecnologie.

Steve Bannon, all'epoca capo di Breitbart News e manager della campagna elettorale, sostenne l'utilità di avere una collaborazione con Cambridge Analytica, di cui era stato vicepresidente[302].

Le indagini hanno accertato che nel corso della campagna elettorale di Trump furono utilizzati numerosi account fake e bot col fine di diffondere *fake news* e altri contenuti finalizzati a screditare Hillary Clinton, avversaria di Donald Trump.

Ogni giorno venivano pubblicati decine di migliaia di post, soprattutto in occasione dei dibattiti in tv e degli altri grandi appuntamenti elettorali: l'efficacia dei post veniva analizzata in tempo reale (sulla base, per esempio, delle risposte "a caldo") così da potere privilegiare quelli che maggiormente erano in grado di influenzare le opinioni dell'elettorato.

In un video pubblicato qualche giorno dopo l'inchiesta e girato con una telecamera nascosta dai giornalisti di Channel 4[303], si vede Alexander Nix, amministratore delegato di Cambridge Analytica, spiegare ad un potenziale acquirente dei servizi della sua azienda (in realtà un giornalista sotto copertura) come fosse possibile incastrare un politico o un personaggio pubblico confezionando uno scandalo ad hoc grazie alla collaborazione di ex spie russe e britanniche e di qualche ragazza attraente.

[301] A metà del 2016 è nato il "Progetto Alamo", ideato da Brad Parscale con il fine di gestire la campagna elettorale di Donald Trump online.

[302] E. Menietti, "*Il caso Cambridge Analytica, spiegato bene*", in "*ilpost.it*", 2018

[303] https://www.youtube.com/watch?v=mpbeOCKZFfQ

Questo scandalo, ovviamente, ha sconvolto il mondo intero e in particolare quello del web; Facebook in particolare ha subito un fortissimo crollo in borsa dovuto ad un danno di immagine enorme.
Mark Zuckerberg ha dovuto difendere il suo intero business, messo in discussione da questa vicenda, davanti al congresso degli Stati Uniti e al Parlamento Europeo e ha dovuto anche rivedere alcuni processi e meccanismi riguardanti la privacy del suo social network.
Cambridge Analytica, dopo poco, ha dichiarato bancarotta.
Il Garante italiano per la protezione dei dati personali ha applicato a Facebook una sanzione di un milione di euro per gli illeciti compiuti nell'ambito del caso "Cambridge Analytica"[304].
Il Social Network ha invece patteggiato con la Federal Trade Commission americana per il pagamento di due sanzioni, rispettivamente di cento milioni e cinque miliardi di dollari agli enti federali. Avrebbe inoltre dovuto impegnarsi a sottostare a normative molto più rigide riguardanti la protezione della privacy degli utenti, regolate da un comitato indipendente, con un funzionario nominato direttamente dalla FTC.
Questo scandalo ha sicuramente messo in luce come le potenzialità dei big data a livello economico e sociale siano enormi ma, anche, quali siano i rischi legati alla diffusione dei dati personali, per la privacy, per gli utenti del web, per i diritti di libertà e per il futuro della democrazia.
È impossibile sapere con certezza quale sia stato l'impatto effettivo che l'attività svolta da Cambridge Analytica abbia avuto sulle elezioni americane e quale sia stata l'importanza del processo di targeting applicato agli utenti di Facebook. Fortunatamente però, oggi il GDPR contiene delle norme specifiche riguardanti la responsabilizzazione del titolare del trattamento e probabilmente l'applicazione delle nuove regole nell'ambito del trattamento dei dati personali avrebbe garantito una maggiore sicurezza a favore degli utenti iscritti a Facebook[305].

[304] https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9121352
[305] S. Della Piazza, "*Il caso Cambridge Analytica*", in "*dirittoconsenso.it*", 2021.

4.2 – Il caso di Faceapp

Faceapp è un'applicazione per dispositivi mobili che consente all'utente di creare una simulazione della propria immagine invecchiata, ringiovanita, oppure trasformata in altro sesso, o di intervenire sul proprio ritratto con modifiche diverse rispetto all'età e al genere, come ad esempio con la funzione di mixare il proprio volto con quello di qualche noto personaggio del mondo dello spettacolo[306].

Il forte impatto mediatico e i conseguenti download dell'applicazione sono avvenuti grazie alla funzione che consente di "invecchiare" l'immagine dell'utente, questo rappresenta l'aspetto che ha suscitato più interesse e che ha indotto milioni di persone a scaricare l'app[307].

Nel 2019 questa applicazione ha scatenato un enorme dibattito sulla questione della privacy, poiché presentava molte criticità per quanto attiene ai dati personali, in particolare presentava evidenti e notevoli deviazioni rispetto a quanto prescritto dal GDPR e una preoccupante mancanza di trasparenza rispetto alle informazioni fornite agli utenti[308].

Gli organi di informazione hanno affermato che Faceapp è stata rilasciata nel gennaio del 2017 da una società russa con sede a San Pietroburgo[309], aspetto che ha indotto molti a interrogarsi sull'applicabilità del GDPR all'attività di questa società, la quale non è indicata quale titolare del trattamento ma solo come destinataria di eventuali reclami nei termini di servizio dell'app.

Gli sviluppatori di Faceapp hanno dichiarato inoltre che i loro server sono situati nel territorio statunitense, ma se così fosse l'applicazione sarebbe fin

---

[306] C. Piluso, "*Cos'è FaceApp e come funziona?*" in "*bellacanzone.it*", 2020.

[307] Secondo Forbes, a luglio del 2019 oltre 100.000 milioni di persone avevano scaricato FaceApp dal Google Play Store e l'app risultava la prima in classifica sull'App Store di Apple in 121 paesi diversi. Per un approfondimento si rimanda a: https://www.mcafee.com/blogs/privacy-identity-protection/faceapp/

[308] L. Egitto, "*FaceApp: come fare a pezzi i principi del GDPR*", in "*altalex.com*", 2019.

[309] La società è la "Wireless Lab", con sede a San Pietroburgo. Secondo Wired.it, Faceapp dichiara di avere base negli Stati Uniti. Su Google Play si fa riferimento a un indirizzo a Wilmington, città del Delaware (considerato uno dei paradisi fiscali Usa), dove la società immobiliare Regus appoggia "uffici virtuali" per aziende straniere che vogliono mettere piede nel continente americano. A occhio, senza avere una vera scrivania là, ma solo una casella di posta.

da subito stata soggetta al Privacy Shield[310], ossia l'accordo avvenuto tra Washington e l'UE per tutelare anche oltreoceano i dati dei cittadini europei secondo le norme del GDPR. Tuttavia, la società non risultava essere presente nell'elenco delle aziende aderenti. Questo significa che non c'era alcuna garanzia per i cittadini europei che avessero reclami da fare in merito al trattamento dei loro dati personali[311].

In virtù dell'art. 2 del GDPR, il quale prevede che «*Il presente regolamento si applica al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano: a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato*», si può certamente affermare che il GDPR si applica anche a questa società e al trattamento dei dati effettuato tramite la sua app.

Sussistono pochi dubbi sul fatto che vi sia trattamento dei dati personali: l'utente scarica Faceapp dal Google Play Store o dall'App Store sul proprio dispositivo mobile, scambiando informazioni personali (relative al dispositivo e alla propria identità) con i sistemi del titolare del trattamento, inviando dati personali[312] che identificano l'interessato. L'applicazione, attraverso il dispositivo dell'utente, effettua una scansione del volto oppure acquisisce un'immagine dalla cartella del dispositivo dell'utente ed elabora tale immagine presso i propri sistemi extraeuropei per simularne una variante invecchiata, ringiovanita o, in generale, modificata.

Se il GDPR viene applicato correttamente e avviene di fatto un trattamento di dati personali, l'utente in genere ha la possibilità di visualizzare

[310] https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/5306161

[311] PrivacyOS, "*Faceapp e privacy: perché è scoppiata la bomba privacy?*", in "*privacyos.com*", 2021.

[312] È necessario precisare che i dati inviati non sono dati biometrici. La foto in sé non costituisce un dato biometrico. Infatti, in base all'art 4 par. 14 del GDPR, solo se combinata a decine di altre informazioni simili potrebbe permettere a un sistema di identificarci con certezza.

l'informativa sul trattamento dei dati personali prima che vengano raccolte le informazioni che lo riguardano[313].

Nel caso specifico di Faceapp, una volta scaricata l'app era possibile utilizzare immediatamente le sue funzionalità senza che vi fosse la verifica dei termini e delle condizioni d'uso e senza poter visualizzare l'informativa sul trattamento dei dati personali[314].

Se l'utente fosse stato intenzionato a prendere visione dell'informativa, sarebbe stato costretto ad effettuare una ricerca su internet per trovare nel sito di Faceapp i "*terms of service*" e la "*privacy policy*"[315].

È palese quindi che vi fosse una violazione del Regolamento per il semplice fatto di avere omesso di sottoporre all'interessato l'informativa prima che lo stesso inviasse informazioni personali.

Tuttavia, anche se fosse stata comunicata correttamente, la privacy policy di FaceApp, all'epoca dei fatti, risultava inidonea a soddisfare in requisiti del GDPR.

Erano molti, infatti, i punti critici dell'applicazione: in primis, leggendo la privacy policy gli utenti non erano in grado di capire quali dati venissero trattati, a chi fossero comunicati e per quanto tempo potessero essere conservati (informazione che, ai sensi dell'art. 12 GDPR, dovrebbe essere segnalata per ciascuna tipologia di trattamento). A questo proposito, stando ad un'intervista effettuata da TechCrunch, gli sviluppatori hanno spiegato che, nella maggior parte dei casi, i dati non venivano conservati per più di 48 ore[316].

---

[313] Art. 13 GDPR

[314] L. Egitto, "*FaceApp: come fare a pezzi i principi del GDPR*", in "*altalex.com*", 2019.

[315] Ora, in Google Play Store e nell'App store, effettuando la ricerca di Faceapp, appare la sezione "privacy dell'app", in cui viene specificato che "*lo sviluppatore ha indicato che le procedure per la tutela della privacy dell'app potrebbero includere il trattamento dei dati descritto di seguito. Per ulteriori informazioni, consulta l'informativa sulla privacy dello sviluppatore*". Per un approfondimento si rimanda a https://www.faceapp.com/privacy-en.html (Informativa privacy) - https://www.faceapp.com/terms-en.html (Terms of service) https://apps.apple.com/it/app/faceapp-editor-viso-ia/id1180884341 (App Store) - https://play.google.com/store/apps/details?id=io.faceapp&hl=it&gl=US (Google Play Store)

[316] V. Berra, "*FaceApp, quali sono (davvero) i rischi per la privacy: risponde l'esperto di diritto informatico*", in "*open.online*", 2019.

Secondo un'indagine condotta da Altalex, Faceapp violava sotto diversi aspetti il GDPR: in primo luogo, era impossibile comprendere chi fosse il titolare del trattamento, dove si trovasse e come contattarlo per informazioni relative al trattamento dei dati personali.

Non vi era alcuna menzione del rappresentante del titolare, che pure dovrebbe essere designato se consideriamo che il titolare del trattamento non risiede nell'UE ma offre servizi a cittadini dell'Unione[317] che comportano un trattamento di dati personali su larga scala.

Le finalità del trattamento erano indicate in maniera incompleta, imprecisa e poco trasparente: c'erano diversi riferimenti a trattamenti presentati come necessari e puramente tecnici mentre l'informativa era parecchio vaga sulla questione della profilazione.

La privacy policy inoltre non specificava minimamente quali fossero le basi giuridiche sulla finalità del trattamento. L'utente, infatti, non aveva alcun riferimento per comprendere su quali basi si fondasse il trattamento, neppure indirettamente, né aveva alcuno spunto per capire se il titolare stesse perseguendo interessi legittimi coerenti con il Regolamento.

Un altro aspetto che non era in regola con i requisiti del Regolamento era la questione del trasferimento delle informazioni personali al di fuori dell'Unione Europea. Come già anticipato, i dati raccolti da Faceapp vengono trasferiti verso i sistemi del titolare del trattamento. Sulla base delle pochissime informazioni che venivano rese disponibili sul sito è ragionevole sostenere che i dati fossero trasferiti in Russia.

Inoltre, consultando la privacy policy di Faceapp, l'indagine di Altalex rivela che nemmeno le prescrizioni del punto f) dell'art. 13 del Regolamento erano state rispettate: non veniva esplicitata, infatti, l'intenzione di trasferire i dati verso paesi terzi e non erano neppure indicate le garanzie e gli accorgimenti necessari per rispettare i principi previsti dagli articoli 44 e 49 del GDPR.

Mancava poi l'indicazione dei destinatari dei dati personali: la privacy policy aveva una sezione dedicata ai soggetti con cui venivano condivisi i dati ma questi erano raggruppati in macrocategorie troppo semplificate e generiche

[317] Art. 3, par. 2 GDPR; art. 27 GDPR

che non consentivano di comprendere, nemmeno indirettamente, che tipo di attività svolgessero i soggetti a cui i dati venivano comunicati.

Tutte queste criticità, secondo Altalex, hanno comportato molteplici violazioni dei principi di liceità, correttezza, trasparenza[318], nonché delle prescrizioni dell'art. 12 e dell'art. 13 GDPR che lasciano pochi dubbi sul livello di conformità al Regolamento.

Le gravi lacune presenti nell'informativa dell'applicazione non hanno comportato solo una violazione dei principi di trasparenza e correttezza nei confronti dell'interessato, ma hanno costituito una diretta e seria lesione e violazione dei diritti di quest'ultimo.

Infatti, la privacy policy di Faceapp ometteva completamente l'indicazione dei diritti e delle facoltà degli interessati di cui ai punti b)-f) del secondo comma dell'art 13 GDPR, sostanzialmente impedendo all'interessato di conoscere i propri diritti previsti dagli artt. 15 a 22 del Regolamento.

Tuttavia, ciò che è più grave, probabilmente, era la totale assenza di strumenti necessari all'interessato per esercitare i propri diritti: infatti, oltre a non informare gli utenti sui propri diritti, Faceapp non offriva loro nemmeno punti di contatto o strumenti pratici per esercitare le facoltà previste a favore dell'interessato nel Regolamento. In questo caso si tratta di una violazione specifica dell'art. 11 comma 2 del GDPR che impone al titolare di agevolare l'esercizio dei diritti dell'interessato ai sensi degli artt. 15-22 del Regolamento.

Oggi, a seguito delle polemiche, sono intervenute delle modifiche nell'informativa privacy, il cui ultimo aggiornamento risale al 4 giugno 2020.

È cambiato innanzitutto il titolare del trattamento, che non più Wireless Lab, ma "FaceApp Inc.", società con sede negli Stati Uniti e contattabile per l'esercizio dei propri diritti ad un indirizzo e-mail specifico.

È stata, inoltre, inserita una sezione dedicata agli utenti europei con l'indicazione della base giuridica dei trattamenti e dei diritti che il GDPR riconosce agli interessati.

[318] Art. 5 e Art. 12 GDPR

Secondo quanto indicato nell'informativa privacy, FaceApp richiede l'autorizzazione ad accedere alla fotocamera o alla galleria immagini, ma non raccoglie altre fotografie oltre a quelle che si scelgono di modificare. La fotografia che si carica sull'app per la modifica viene crittografata e la chiave viene memorizzata localmente sul dispositivo, in modo che questo sia l'unico in grado di visualizzarla.

Le informazioni cui FaceApp ottiene accesso non si limitano, tuttavia alle immagini, potendo riguardare anche il sistema operativo, il produttore, il modello e l'ID del dispositivo, il tipo di browser utilizzato, la risoluzione dello schermo, l'indirizzo IP e il Paese di localizzazione, l'ID di Google Advertising e di Apple Advertising e il sito web visitato prima di FaceApp.

Vengono trattate, inoltre, informazioni sull'uso dell'app, come ad esempio la lingua scelta, la data e l'ora dell'installazione e dell'ultimo utilizzo, ma anche informazioni sui social media, nel caso in cui venga scelta tale modalità di accesso all'app.

Infine, le informazioni raccolte vengono conservate sui cloud di Amazon Web Services (negli USA) e Google Cloud Platform (nel Paese più vicino a quello dell'utente tra quelli disponibili), per un periodo massimo di 48 ore. L'utente che lo desideri, comunque, può richiedere la cancellazione dei propri dati prima delle 48 ore[319].

[319] M.E. Iafolla, "*FaceApp, cambiare sesso con un filtro. E la privacy?*", in "*studiolegaleiafolla.it*", 2020.

Conclusioni

Con l'emanazione del Regolamento UE 679/2016 (GDPR) il legislatore europeo ha voluto dimostrare la sempre più crescente attenzione verso il trattamento dei dati personali posto in essere con l'evoluzione delle nuove tecnologie. Attraverso una serie di strumenti come cookies, big data ecc. si possono raccogliere quantità molto elevate di informazioni, con conseguenti rischi in tema di privacy che gli utenti sono costretti ad affrontare.

A tal riguardo, il GDPR si pone come obiettivo principale la protezione dei dati personali, prevedendo una serie di principi per il loro trattamento, ma intende anche instaurare un'area in cui tali dati possano circolare liberamente.

In quest'ottica si è discusso del concetto di mercato dei dati personali e della loro conseguente commercializzazione, giungendo alla conclusione che l'offerta di un bene o di un servizio contro la prestazione del consenso al trattamento dei dati è ammessa nei limiti imposti dalla norma in materia di libertà del consenso al trattamento. L'obiettivo del legislatore sembra dunque essere quello di ammettere lo scambio ma solamente con specifici requisiti, in modo da tutelare la parte debole del rapporto contrattuale, cioè l'utente/consumatore.

A mio avviso, la protezione dei dati incentrata sul tema del consenso per quanto riguarda il tema dei cookies, non risulta del tutto efficace, poiché abbiamo visto che utilizzare i cookies comporta alcuni rischi per la privacy degli utenti.

Quando un utente naviga in un sito web, si trova di fronte ad un banner dove legge "*Utilizziamo cookie e altre tecnologie simili necessari per migliorare le tue esperienze di acquisto e per fornire i nostri servizi, come descritto in dettaglio nella nostra informativa sui cookie. Utilizziamo questi cookie anche per capire come i clienti utilizzano i nostri servizi per poterli migliorare (ad esempio, analizzando le interazioni con il sito)*". L'utente medio di Internet solitamente accetta tutti i cookie per poter proseguire nella navigazione, senza investire il suo tempo nel provare a leggere e comprendere l'informativa. Inoltre, le informative sui cookie e sulla privacy solitamente

presentano un linguaggio con contenuti tecnici e normativi che non risultano di facile comprensione a tutti. Abbiamo visto però che, nel corso degli anni, sono state create normative comunitarie e nazionali che regolano l'uso dei cookies, sempre più restrittive, con lo scopo di proteggere i dati personali degli utenti.

In particolare, il legislatore europeo e le Autorità per la protezione dei dati personali si sono da tempo orientati su una regolamentazione che prevede tutta una serie di adempimenti per i siti web che fanno uso di cookie di terze parti.

Per quanto riguarda gli utenti, questi possono anche non accettare i cookies, dovendo reinserire alcune informazioni ogni volta che si accede ad un sito web, non potendo navigare con impostazioni personalizzate.

Bisogna ricordare che i cookie creati durante la sessione nel web vengono salvati per personalizzare la navigazione dell'utente e di per sé i cookie non sono malware, ma esiste sempre la possibilità che un hacker riesca ad accedere ai dati che contengono e, in questo modo, alla cronologia di navigazione.

Per una maggiore sicurezza, gli utenti possono sempre svuotare la cache e consentire l'utilizzo dei cookies solo relativamente a siti che vengono considerati attendibili. Infine, è sempre consigliato installare un programma antivirus per eseguire una scansione completa del dispositivo e rimuovere eventuali minacce presenti.

Relativamente alle aziende, la tendenza negli ultimi anni è quella di abbandonare progressivamente l'utilizzo dei cookie di terze parti, ma di conseguenza emerge la necessità di disporre di soluzioni alternative.

Ricordiamo che le aziende hanno la necessità di una relazione diretta con l'utente, pena la perdita dell'utente stesso. Esse sono chiamate non solo ad adempiere agli obblighi normativi, ma anche ad una necessaria comprensione di ciò che il loro target e la loro audience richiede: maggiore protezione dei dati personali e trasparenza.

Tuttavia, nonostante le decisioni del legislatore siano note da tempo, la maggior parte delle aziende che si occupano di advertising non hanno ancora assunto soluzioni efficaci.

Esistono comunque delle proposte di strategie alternative per la creazione di audience targettizzabili, come per esempio quella della piattaforma "LiveRamp", con una soluzione chiamata "*Authenticated Traffic Solution*" (ATS) che consente una pubblicità basata sulle persone anziché sui cookie. Enrico Ciampini, *Publisher Director* in LiveRamp, dichiara che ATS aiuta a connettere marketer ed editori, mantenendo l'*addressability*[320] e, cosa più importante, il rispetto e la fiducia dei consumatori.

Questa soluzione permette inoltre la traduzione in tempo reale delle informazioni di identificazione personale in ID pseudonimizzati, nel totale rispetto della normativa sulla protezione dei dati personali[321].

Altre soluzioni che potrebbero essere adottate, nel frattempo, potrebbero riguardare un rafforzamento dei ruoli delle autorità per la protezione dei dati personali, le quali potrebbero essere in grado di controllare con maggior precisione il processo di raccolta dei dati tramite cookies da parte delle aziende, con un conseguente inasprimento delle sanzioni nei casi in cui venissero riscontrate violazioni delle normative.

Infine, casi come quello di Facebook e Cambridge Analytica e quello di Faceapp ci insegnano che, nonostante le numerose normative vigenti, i nostri dati personali sono sempre soggetti a dei rischi, i quali possono certamente essere limitati attraverso l'attuazione di misure di sicurezza, ma non possono, purtroppo, essere totalmente azzerati. Il caso di Faceapp in particolare mostra come un'applicazione che all'apparenza può risultare innocua e creata principalmente ad uno scopo di intrattenimento, possa in realtà nascondere delle insidie relative alla nostra privacy; di conseguenza è necessario prestare molta attenzione ai contenuti e alle applicazioni che scarichiamo e utilizziamo.

---

[320] L'*Addressability* è la capacità di identificare e raggiungere persone specifiche attraverso una campagna pubblicitaria.

[321] Per un approfondimento, si rimanda a https://liveramp.it/blog/chrome-annuncia-la-fine-dei-cookie-di-terze-parti-un-anno-dopo/

La speranza è che in un futuro noi utenti e navigatori del web avremo un controllo sempre maggiore sul modo in cui i nostri dati personali vengono raccolti attraverso i cookies.

In conclusione, possiamo dire che, al di là della reale applicabilità delle normative recenti, la crescente attenzione degli utenti del web, dell'opinione pubblica e dei media sul tema della privacy e della protezione dei dati personali ha sicuramente contribuito a responsabilizzare maggiormente le aziende che raccolgono e analizzano i nostri dati, indipendentemente dal metodo di raccolta da esse utilizzato.

Bibliografia

- Addante A., “La Circolazione negoziale dei dati personali nei contratti di fornitura di contenuti e servizi digitali”, Giustizia Civile, fac. 4, 1° aprile 2020.
- Astone F., “Il rapporto tra gestore e singolo utente: questioni generali”, in Ann. It. Dir. Aut., 2011, p. 108
- Bravo F., “Lo scambio di dati personali nei contratti di fornitura di servizi digitali e il consenso dell’interessato tra autorizzazioni e contratto”, Contratto e Impresa 2019, 1, 34.
- Bravo F., “L’architettura del trattamento e la sicurezza dei dati e dei sistemi”
- Caggiano I. A., “Il consenso al trattamento dei dati personali nel nuovo Regolamento europeo. Analisi giuridica e studi comportamentali”, Il Mulino, Rivisteweb, Fascicolo 1, 2018.
- Camardi C., “Prime osservazioni sulla Direttiva (UE) 2019/770 sui contratti per la fornitura di contenuti e servizi digitali” p. 499 e ss.
- Caterina R., “Cyberspazio, social networks e teoria generale del contratto”, in ann. It. Aut., 2011 p. 96.
- Chiarloni S., “Diritto Processuale Civile” Giurisprudenza Italiana, 2020.
- Cuffaro V., “Il diritto europeo sul trattamento dei dati personali e la sua applicazione in Italia: elementi per un bilancio ventennale”.
- Cuffaro V. (a cura di), D'Orazio R. (a cura di), Ricciuto V. (a cura di), “I dati personali nel diritto europeo”, Giappichelli, 2019.
- D’ippolito G., “Commercializzazione dei dati personali: il dato personale tra approccio morale e negoziale”, Diritto dell’informazione e dell’informatica (II), Fasc.3,1, 2020.
- De Franceschi A. “European Contract Law and the Digital Single Market”, Cambridge, Intersentia, 2016, p. 51 ss.
- Di Landro A. C., “Big Data, Rischi e tutele nel trattamento dei dati personali”, ESI, 2020.
- Floridi L., “Philosophical Conceptions of Information”.

- Locoratolo B., “Il Trattamento Dei Dati Personali E La Privacy”, Simone, 2021.
- Perlingieri C., “Profili civilistici dei social networks”, Napoli, 2014
- Ravarotto M, “Il Mercato dei dati personali. In particolare, il caso Mediaworld”, 2019/2020, Dipartimento di Diritto Privato e Critica del diritto, Università Degli Studi di Padova.
- Resta G. e Zeno-Zencovich V., “Volontà e consenso nella fruizione dei servizi in rete”, 2018.
- Ricciuto V., “La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno”.
- Sommaruga G., “Formal Theories of Information: From Shannon to Semantic Information Theory and General Concepts of Information”, Springer, 2009.
- Versaci G., “La Contrattualizzazione Dei Dati Personali Dei Consumatori”, ESI, 2020.
- Wylie C., “Il Mercato Del Consenso”, Longanesi, 2019.
- Zech H., “Information us a property”, 6 JIPITEC 192, par 1, 2015.
- Zech H., “A legal framework for a data economy in the European Digital Single Market: rights to use data”, Journal of Intellectual Property Law & Practice, vol. 11, n. 6, 2016.
- Zech. H, “Data as a Tradeable Commodity – Implications for Contract Law”, 2017.

Sitografia

- 4clegal.com: www.4clegal.com
- Accenture: www.accenture.com
- Agenda Digitale: www.agendadigitale.eu
- Altalex: www.altalex.it
- Andreaminini.com: www.andreaminini.com
- Apkappa.it: www.apkappa.it
- Apogeo Editore: www.apogeonline.com
- Apple Store: https://apps.apple.com
- Assistenza-legale-imprese.it: https://assistenza-legale-imprese.it/
- Assoknowledge: www.assoknowledge.org
- Bellacanzone.it: www.bellacanzone.it
- Bigdata4Innovation: www.bigdata4innovation.it
- Bruno Saetta – Internet e Diritto: www.brunosaetta.it
- Cookiebot: www.cookiebot.com/it/
- Cyberlaws: www.cyberlaws.it
- Cybersecurity360: www.cybersecurity360.it
- Data Protection Manager: www.privacymanager.eu
- Datalog, software a dimensione uomo: www.datalog.it
- DGRS Studio Legale: www.dgrs.it
- Digital4: www.digital4.biz
- Digitalflow.it: www.digitalflow.it
- Dirittoconsenso.it: www.dirittoconsenso.it
- Enciclopedia Treccani: https://www.treccani.it/enciclopedia/
- European Data Protection Board: https://edpb.europa.eu/edpb_en
- Engage: www.engage.it
- Eur-lex.europa.eu: https://eur-lex.europa.eu/
- Faceapp.com: www.faceapp.com
- Flyip: www.flyip.it
- Focus.it: www.focus.it

- Formula Impresoft: https://blog.impresoftgroup.com/formula-impresoft
- Frareg Frafor: www.frareg.com/it/
- Garante Privacy: www.garanteprivacy.it
- Gli Stati Generali: www.glistatigenerali.com
- Google Play Store: https://play.google.com
- Html.it: www.html.it
- ICT Security Magazine: www.ictsecuritymagazine.com
- Ilgiorno.it: www.ilgiorno.it
- Ilpost.it: www.ilpost.it
- InfoCuria - Giurisprudenza: www.curia.europa.eu
- Infodati.it: www.infodati.it
- Informatica Per Tutti: www.informaticapertutti.com
- Insic, l'informazione per la sicurezza tecnica, professionale, online: www.insic.it
- Intelligenzaartificiale.it: www.intelligenzaartificiale.it
- Ionos: www.ionos.it
- IT Impresa soluzioni informatiche: www.it-impresa.it
- Iubenda: www.iubenda.com/it/
- Jus Civile: www.juscivile.it
- Kaspersky: www.kaspersky.it
- La legge per tutti – Informazione e consulenza legale: www.laleggepertutti.it
- Legalblink: www.legalblink.it
- Legaldesk: www.legaldesk.it
- L&T'S Network: https://letsnetwork.it/
- Libero Tecnologia: https://tecnologia.libero.it/
- Mailsenpai.com: www.mailsenpai.com
- Mcafee.com: www.mcafee.com
- Mondo Diritto: www.mondodiritto.it
- Mondo Privacy: https://mondoprivacy.it/

- My Social Web: www.mysocialweb.it
- N26.com: www.n26.com
- Net Informatica: www.net-informatica.it
- Open Online: www.open.online
- Osservatori.net: https://blog.osservatori.net/it_it
- Ottimizzazione-pc.it: www.ottimizzazione-pc.it
- Panda Security: www.pandasecurity.com
- Pmi.it: www.pmi.it
- Privacy.it – Consulenza legale e informazione: www.privacy.it
- Privacydati.it: https://privacydati.it/
- Privacylab: www.privacylab.it
- PrivacyOS – Marketing Data Protection Platform: www.privacyos.com
- Proofpoint.com: www.proofpoint.com
- Protezione dati personali - data protection: www.protezionedatipersonali.it
- Reteinformaticalavoro.it: www.reteinformaticalavoro.it
- Risk Management 360: www.riskmanagement360.it
- Scicchitano Studio Legale: www.studioscicchitano.it
- Sinergetica Consulting: https://sinergetica.it/
- Softech.it: www.softech.it
- Soiel International, informazione – innovazione – imprese: www.soiel.it
- Startup Legal: www.startuplegal.it
- Studio Legale Iafolla: www.studiolegaleiafolla.it
- Studio Legale Pozzato, soluzioni legali etiche per aiutare le aziende a realizzare i loro obiettivi di crescita (Dirittoprivacy.it): www.studiolegalepozzato.net
- Tecnologico.wiki: https://tecnologico.wiki/
- Timbusiness.it: www.timbusiness.it
- Trendmicro.com: www.trendmicro.com

- ValigiaBlu.it: www.valigiablu.it
- Vitolavecchia.altervista.org: https://vitolavecchia.altervista.org/
- Wearesocial.com: www.wearesocial.com
- Wired.it: www.wired.it
- Youtube: www.youtube.com

Riferimenti Normativi

- AGCM, Decisione CV154, 11 maggio 2017.
- AGCM, Decisione IP330, 17 febbraio 2021.
- Carta dei Diritti Fondamentali dell'UE, (2000/C 364/01).
- Decreto-legge 8 ottobre 2021, n. 139, convertito con modificazioni dalla Legge 3 dicembre 2021, n. 205, recante «Disposizioni urgenti per l'accesso alle attività culturali, sportive e ricreative, nonché per l'organizzazione di pubbliche amministrazioni e in materia di protezione dei dati personali.»
- Decreto Legislativo 30 giugno 2003, n. 196, "Codice in materia di protezione dei dati personali", pubblicato nella Gazzetta Ufficiale n. 174 del 29 luglio 2003.
- Decreto legislativo 6 settembre 2005, n. 206 (Codice del Consumo), modificato dalla Legge 23 dicembre 2021, n. 238.
- Decreto Legislativo 10 agosto 2018, n. 101 "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)".
- Direttiva (UE) 2019/770 del Parlamento Europeo e del Consiglio del 20 maggio 2019 relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali.

- Legge n. 675 del 31 dicembre 1996 - Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali.
- Linee Guida Cookie e altri strumenti di tracciamento, 10 Giugno 2021, Gazzetta Ufficiale 163, 9 Luglio 2021.
- Regolamento UE n. 2016/679 (GDPR).
- Proposta di Regolamento del Parlamento Europeo e del Consiglio relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche e che abroga la direttiva 2002/58/CE (regolamento sulla vita privata e le comunicazioni elettroniche).
- Trattato sul funzionamento dell'UE (TFUE) del 13/12/2007.