Capitolo 1

PROTEZIONE DELLA PRIVACY E DEI DATI PERSONALI NELLE ATTIVITÀ DI MARKETING

1. Introduzione

In una società in cui la digitalizzazione e l'accesso ad Internet sono sempre più comuni e ramificati, l'identità personale e la rappresentazione sociale dell'individuo si dilatano per includere anche la dimensione delle sue attività svolte online. Questo accade perché l'individuo proietta la propria identità nel mondo digitale attraverso i dati che egli stesso lascia ogni giorno in rete.

Oggi esiste un diffuso interesse allo studio delle attività svolte dagli utenti sul web, in particolare all'interno dei *social network*, giustificabile anche dal bisogno di conoscenza della domanda di mercato da parte delle imprese. La raccolta di dati personali svolta online rappresenta, infatti, un prezioso strumento per le strategie di marketing aziendale, in cui è fondamentale la comprensione dei bisogni e dei valori dei consumatori per identificare la situazione presente e gli sviluppi futuri del mercato. In questo senso, interessi personali, consumi e altre tracce lasciate dagli utenti del web rappresentano linfa vitale per le attività di marketing.

In tale cornice complessiva, i dati personali costituiscono pertanto sia ciò che per le imprese sono fonti di informazione per analisi delle scelte di consumo sia ciò che per l'individuo sono frammenti della propria personalità. Da un lato, infatti, la pratica commerciale di raccolta ed elaborazione dei dati degli utenti finalizzata alla creazione di gruppi omogenei per gusti e comportamenti (c.d. profilazione) consente la fornitura di pubblicità e prodotti personalizzati, dall'altro lato, questa attività può menomare l'individuo nella sua identità e nella effettiva libertà di esprimere il proprio pensiero, il proprio modo d'essere, le proprie scelte. Ciò può accadere, per esempio, quando queste attività creano il presupposto perché gli venga associato un profilo che lo condiziona, oppure che potrebbe essere sbagliato, o perché quel profilo svela dei

particolari dell'individuo che lui non avrebbe voluto fossero conosciuti in contesti diversi da quelli originari.

L'incessante sviluppo della società dei dati (c.d. *data society*) e di tecnologie emergenti come intelligenza artificiale, prodotti e servizi dell'Internet delle cose (IoT, *Internet of Things*) ed i *big data* riaffermano continuamente l'esigenza di tutela dei dati personali [1]. È necessario porsi, dunque, un duplice ordine di interrogativi. Innanzitutto è opportuno domandarsi come abilitare il corretto ed efficace funzionamento dei sistemi economici e delle società basati sui dati, anche personali; allo stesso tempo, ci si deve chiedere come affrontare l'incidenza dello studio delle impronte digitali lasciate dall'utente quale elemento di vulnerabilità nella tutela della sua sfera privata (c.d. *data privacy*).

Questo spiega perché negli ultimi decenni il tema della protezione della privacy e dei dati personali sia apparso, e riapparso periodicamente, nei panorami legislativo e mediatico, soprattutto nel contesto della profilazione degli individui, nella loro triplice valenza di consumatori, utenti e cittadini. Nel 2018 il dibattito sulla centralità della tutela della sfera privata dell'individuo nell'ambiente online si è esteso all'opinione pubblica mondiale con il caso *Cambridge Analytica*. Questa vicenda – la cui protagonista era una società di analisi dei dati che aveva raccolto i dati personali di oltre 50 milioni di utenti statunitensi di Facebook per costruire un programma software in grado di prevedere e influenzare le scelte elettorali – ha dimostrato come abusi nell'utilizzo dei dati personali possano costituire un rischio sia per la libera costruzione della personalità degli individui sia per la tenuta democratica dei paesi [2].

Anche alla luce di questo scandalo, è evidente come la fluidità dei dati all'interno dei sistemi telematici è vitale quanto la loro qualità e sicurezza, e che la fluidità non può prescindere dal diritto degli individui di scegliere se, e come, permettere l'uso dei propri dati.

Dopo oltre quattro anni di tortuosi negoziati, nell'Unione Europea è nato un nuovo quadro regolamentare che mantiene i caposaldi della *data privacy* europea enucleati dalla precedente Direttiva 95/46/CE (anche nota come "Di-

[1] Sull'importanza del fenomeno dei *big data* e delle nuove tecnologie digitali nell'attività di marketing si rinvia al capitolo successivo.

[2] Questa vicenda di marketing elettorale ha rivelato il condizionamento delle opinioni dei cittadini profilati in base al loro comportamento in rete. Difatti, non soltanto ha rivelato l'uso, scorretto, di un'enorme quantità di dati prelevati dal social network Facebook per costruire profili comportamentali e di interessi di milioni di utenti statunitensi ma ha altresì originato interrogativi sui fini, e sugli effetti collaterali, dell'utilizzo delle tracce digitali lasciate in rete.

rettiva madre") e aggiunge ulteriori elementi di tutela, senza costituire un vero elemento di discontinuità. Attualizzando gli strumenti per la protezione dei dati personali per mezzo di norme giuridiche comuni a tutti gli Stati Membri, il nuovo Regolamento europeo in materia di protezione dei dati personali 2016/679 (*General Data Protection Regulation*, GDPR) promette di rafforzare la protezione dei dati personali quale diritto fondamentale, nonché quello di consolidare e promuovere il mercato interno legato ai servizi digitali.

Lo scopo del presente capitolo è quello di analizzare il quadro normativo dell'Unione Europea per il trattamento dei dati personali e la loro libera circolazione. Di conseguenza, il capitolo è così organizzato: nel par. 2 si darà conto dell'origine ed evoluzione del diritto alla protezione dei dati personali; nel par. 3 si spiegherà la terminologia introdotta dalla legislazione europea sui dati personali e la portata della stessa; nel par. 4 ci si soffermerà sui principi che regolano l'utilizzo dei dati personali; mentre nel par. 5 si discuteranno i diritti che il soggetto titolare dei dati personali può esercitare. Nei paragrafi 6 e 7 si valuteranno invece due temi differenti: il ruolo delle autorità di controllo, autorizzate ad infliggere sanzioni, e le modalità secondo le quali il trasferimento dei dati personali può avvenire tra paesi UE e paesi extra UE.

2. Origine ed evoluzione della tutela dei dati personali

Il diritto alla privacy è nato negli Stati Uniti alla fine dell'Ottocento come libertà alla non ingerenza nella propria sfera personale (*right to be let alone*), arricchendosi in seguito di ulteriori punti di vista. Le variegate esigenze di tutela dell'identità personale hanno determinato una concettualizzazione dinamica della privacy, che negli anni è stata interpretata secondo diverse soluzioni, prendendo in considerazione vari aspetti del rapporto tra sfera individuale e società.

Le progressive trasformazioni tecnologiche hanno ampliato la manifestazione del diritto alla privacy nella protezione contro la pubblicità, l'appropriazione del nome o dell'immagine, la falsa informazione o l'intrusione non desiderate, così come nel controllo dell'individuo sui propri dati personali, sulle proprie sfere fisiche, mentali o digitali, sulla raccolta e l'utilizzo dei dati personali.

Il valore del diritto alla privacy è stato riconosciuto dalla Dichiarazione Universale dei Diritti dell'Uomo (UDHR), adottata nel 1948, come uno dei diritti umani fondamentali protetti [3]. Poco dopo l'adozione della dichiarazio-

[3] L'art. 12 sancisce che "Nessun individuo potrà essere sottoposto ad interferenze arbitrarie nella sua vita privata, nella sua famiglia, nella sua casa, nella sua corrispondenza, né a lesione

ne, nel 1950, l'Europa sancì questo diritto nella Convenzione Europea dei Diritti dell'Uomo (CEDU)[4]. L'UDHR e la CEDU nascono in un periodo storico antecedente alla diffusione delle tecnologie informatiche e di Internet, e dell'ingresso nella società della conoscenza (c.d. *knowledge society*) in cui attualmente viviamo. Queste successive innovazioni che hanno determinato vantaggi significativi in grado di migliorare la qualità della vita della società nel suo complesso – fornendo alle persone un livello più ampio di accesso a diverse informazioni e servizi a costi ridotti, offrendo alle comunità la possibilità di comunicare e catalizzare interessi, alimentando l'efficienza e la produttività delle imprese, abilitando i principi di trasparenza e partecipazione della Pubblica Amministrazione – non sono tuttavia prive di rischi.

Con la progressiva "datificazione" dell'economia e della società si sono creati strumenti per elaborare le informazioni che hanno condotto a pericoli inediti per il diritto alla privacy e che hanno portato al riconoscimento internazionale dell'esigenza di rinnovata tutela per i dati personali.

Tra i paesi OCSE (Organizzazione per la Cooperazione e lo Sviluppo Economico) si è mostrato un generale consenso sui principi fondamentali e sulle regole di base della *data privacy*. Tale consenso ha trovato espressione e formalizzazione nelle Linee Guida sulla Privacy del 1980, che nascono sulla scorta dei FIPPs (*Fair Information Practice Principles*) sviluppati alla fine degli anni '70 dalla Commissione Federale del Commercio statunitense (*US Federal Trade Commission, FTC*) in risposta al crescente uso dei sistemi di dati automatizzati. Benché prive di efficacia vincolante e comprendenti soltanto uno schema di massima per la tutela dei dati personali, le Linee Guida OCSE e la loro miscela di principi sostanziali (per esempio, qualità dei dati, limitazione all'uso) e principi procedurali (per esempio, consenso, accesso) hanno rappresentato un'importante fonte di ispirazione per le legislazioni interne dei suoi paesi

---

del suo onore e della sua reputazione. Ogni individuo ha diritto ad essere tutelato dalla legge contro tali interferenze o lesioni". Traduzione italiana disponibile al link https://www.ohchr.org/en/udhr/pages/Language.aspx?LangID=itn [ultimo accesso il 10 settembre 2019].

[4] La Convenzione, adottata dal Consiglio d'Europa alla fine della seconda guerra mondiale con l'intento di promuovere i diritti delle persone nei paesi europei, all'art. 8 sancisce che "1. Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza. 2. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui". Disponibile al link https://www.echr.coe.int/Documents/Convention_ITA.pdf [ultimo accesso il 10 settembre 2019].

membri e anche per altri strumenti internazionali e di autoregolamentazione [5].

Nonostante ciò, e a dispetto della portata internazionale dell'esigenza di *data privacy*, nei fatti gli approcci legislativi nazionali ancora divergono. Paradigmatica, ed estremamente rilevante per l'intenso scambio di dati transfrontalieri, è la distanza tra gli approcci europeo e statunitense alla tutela. Laddove l'Unione Europea ha adottato in materia una legge generale, ossia la Direttiva Madre prima e il GDPR poi, che copre tendenzialmente l'intera gamma delle possibili modalità di trattamento dei dati personali (approccio omnibus), gli Stati Uniti si sono dotati di una legislazione frammentaria, che non ha portata generale, bensì disciplina uno ad uno, singoli e specifici ambiti di trattamento dei dati (approccio settoriale). Inoltre, benché i due paesi riconoscano quale fine e mezzo della legislazione in materia di dati personali la creazione di un sistema di controlli ed equilibri volti a proteggere i dati delle persone, la disciplina europea regolamenta rigorosamente l'impiego dei dati personali ed impedisce che questi ultimi siano utilizzati per finalità diverse da quelle dichiarate, mentre la legislazione statunitense consente più ampie possibilità di uso dei dati e, quindi, una maggiore penetrazione nella sfera personale degli individui.

In Europa, come negli Stati Uniti, la protezione dei dati personali è iniziata negli anni '70, con l'adozione di normative, da parte di alcuni Stati, finalizzate a controllare il trattamento dei dati personali da parte delle autorità pubbliche e delle grandi imprese [6]. I successivi passi in avanti nel concetto giuridico di *data privacy* sono avvenuti a partire dal decennio successivo, proprio in Europa. Nel 1981 il Consiglio d'Europa approvò la Convenzione di Strasburgo, anche nota come Convenzione 108, la quale rimane tuttora l'unico strumento giuridicamente vincolante a livello internazionale in materia, potendo ad essa aderire anche Stati non membri del Consiglio d'Europa. Si è giunti poi all'adozione della Direttiva 95/46/CE, la Direttiva Madre che ha istituito il primo quadro generale per il trattamento dei dati personali all'interno dell'Unione Europea [7]. L'evoluzione in via giurisprudenziale della

[5] OCSE, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1980, riviste nel 2013, disponibili al link http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf [ultimo accesso 10 settembre 2019].

[6] Nel 1970 il Land tedesco dell'Assia adottò la prima legge sulla protezione dei dati, applicabile tuttavia solo in questo Stato. La prima normativa nazionale in materia di protezione dei dati al mondo venne introdotta in Svezia nel 1973. Alla fine degli anni '80, diversi Stati europei (Francia, Germania, Paesi Bassi e Regno Unito) avevano una legislazione in materia di protezione dei dati personali.

[7] Direttiva 95/46/CE del Parlamento Europeo e del Consiglio del 24 ottobre 1995 sulla protezione delle persone con riferimento al trattamento dei dati personali e alla loro circolazione (GUCE L 281, 23 novembre 1995, 31).

definizione di *data privacy*, nel senso di protezione dell'informazione riferita all'individuo e al suo uso, ha infine permesso che con il trattato di Lisbona la protezione dei dati personali diventasse un diritto fondamentale dell'Unione Europea [8], distinto dal diritto al rispetto della privacy, riconosciuto dal Trattato sul Funzionamento dell'Unione Europea e dalla Carta dei diritti fondamentali dell'Unione Europea [9].

La privacy e la protezione dei dati personali sono dunque diritti distinti e al contempo connessi. Entrambi sono tesi a salvaguardare valori simili, ossia l'autonomia e la dignità umana degli individui, accordando loro una sfera privata nella quale possano sviluppare liberamente la loro personalità. D'altro canto i due diritti differiscono in termini di formulazione e portata del concetto di vita privata. Il diritto alla privacy consta di un diritto di scegliere cosa vogliamo rendere conoscibile agli altri e di un divieto generale di ingerenza, assoggettato ad alcuni criteri di interesse pubblico che possono giustificarla in determinati casi. Il diritto alla protezione dei dati personali si basa su un diritto di "autodeterminazione informativa", che si estrinseca nel diritto di scegliere l'uso di ciò che abbiamo reso conoscibile e conferisce alla persona il potere di controllo sulle informazioni riguardanti la sua vita privata. Questa distinzione – accolta nella Carta dei diritti fondamentali dell'Unione Europea che riconosce il diritto alla protezione dei dati personali (art. 8) come diritto autonomo, separato dunque da quello "al rispetto della propria vita privata e familiare" (art. 7) – è sostanziale oltre che formale: mentre il diritto alla privacy prevede una tutela statica e negativa, esaurendosi nell'escludere ingerenze altrui, il diritto alla tutela dei dati personali prevede una tutela dinamica e positiva, concretizzandosi in strumenti di controllo e d'intervento nella circolazione dei dati.

---

[8] Trattato di Lisbona che modifica il trattato sull'Unione Europea (TUE) e il trattato che istituisce la Comunità europea (TCE) (G.U. C 306 del 17 dicembre 2007); entrato in vigore in data 1 dicembre 2009.

[9] Lo si sancisce all'art. 16 del Trattato sul Funzionamento dell'Unione Europea ("Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano" disponibile al link https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:12012E/TXT:IT:PDF [ultimo accesso 10 settembre 2019]) e all'art. 8 della Carta dei diritti fondamentali ("Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano. 2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica. 3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente" disponibile al link https://www.europarl.europa.eu/charter/pdf/text_it.pdf [ultimo accesso 10 settembre 2019].

3. Terminologia e portata della legislazione europea sui dati personali

La disciplina europea, al fine di dettare una linea uniforme di tutela e intervento, ha introdotto nel discorso sulla privacy e la protezione dei dati personali un nuovo lessico, di cui occorre quindi dare conto nelle pagine che seguono.

3.1. La nozione di dati personali

Nel quadro del diritto europeo, i "dati personali" sono definiti come qualsiasi informazione riguardante una persona fisica identificata o identificabile. È anzitutto importante sottolineare che tanto il GDPR quanto la precedente disciplina della Direttiva Madre limitano l'ambito di applicazione della tutela esclusivamente alle persone fisiche, escludendo la sua estensione alle persone giuridiche. Ciò si giustifica sia dall'inquadramento del diritto alla tutela dei dati personali come diritto fondamentale, sia dall'esigenza di evitare contrasti con i principi di trasparenza e certezza dell'attività di impresa [10].

Inoltre, è opportuno precisare che ai sensi dell'art. 4 del GDPR "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". Ciò vale a significare che si tratta di dati che concernono una persona la cui identità è chiara o che può essere comunque accertata. L'identificazione si basa su elementi che rappresentano una persona in modo tale da renderla distinguibile da tutte le altre persone e riconoscibile come individuo. Per decidere dell'identificabilità di un individuo è richiesta una valutazione costante, che considera tutti i mezzi di cui è possibile avvalersi per identificarlo, direttamente o indirettamente "tenendo conto sia delle tecnologie disponibili al momento del trattamento, sia degli sviluppi tecnologici" [11].

Se dunque è ben evidente che i dati anagrafici (per esempio il nome ed il cognome di una persona) sono un esempio primario di attributi che possono identificare una persona direttamente, altri elementi possono avere un effetto simile, rendendo una persona identificabile indirettamente: il codice fiscale,

---

[10] Cfr. Sentenza della Corte di giustizia dell'Unione Europea del 9 marzo 2017, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce c. Salvatore Manni*, causa C-398/15, ECLI:EU:C:2017:197.

[11] Regolamento generale sulla protezione dei dati, considerando 26.

il numero di targa di un veicolo, sono tipici esempi di informazioni che possono rendere identificabile una persona. Con l'evoluzione delle nuove tecnologie informatiche, altri dati personali hanno assunto un ruolo significativo, come: i) i dati di localizzazione, che forniscono informazioni sui luoghi frequentati e sugli spostamenti; ii) i dati biometrici, come le impronte digitali, la conformazione fisica della mano o del volto, dell'iride o della retina, nonché il timbro e la tonalità della voce; iii) i dati online, come l'indirizzo IP [12] e i cookie [13]; iv) gli indirizzi email – da cui deriva la violazione del diritto alla tutela dei dati personali da parte chi li utilizza per l'invio generalizzato di email (c.d. *spamming*), senza il consenso degli interessati, anche se reperiti in rete.

Esiste poi una categoria particolare di dati personali, riconosciuta per la prima volta nella Convenzione 108, e in seconda battuta nella Direttiva Madre con la dicitura di "dati sensibili", che richiede una maggiore protezione e, pertanto, è soggetta a un regime giuridico specifico. I dati sensibili sono quei dati a carattere personale che rivelano l'origine razziale, le opinioni politiche, le convinzioni religiose o altre convinzioni, nonché i dati a carattere personale relativi alla salute o alla vita sessuale. In virtù di quanto disposto nell'art. 6 della Convenzione 108, questi dati non possono essere elaborati automaticamente a meno che il diritto interno preveda delle garanzie appropriate.

3.2. La nozione di trattamento di dati

Il concetto di trattamento dei dati personali è inteso in maniera ampia nell'ambito del diritto dell'Unione Europea intendendosi "qualsiasi operazione […], 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", compiuta sui dati personali [14].

[12] L'indirizzo IP è un numero univoco in tutto il mondo che identifica ogni computer collegato a Internet: al momento del collegamento, tramite modem, con un provider, questi assegna al chiamante automaticamente un indirizzo IP valido.

[13] I cookie sono file di informazioni che i siti web memorizzano sul computer dell'utente di Internet durante la navigazione. Tale memorizzazione permette di realizzare meccanismi di autenticazione, usati ad esempio per i login; di memorizzare dati utili alla sessione di navigazione, come le preferenze sull'aspetto grafico o linguistico del sito; di associare dati memorizzati dal server, ad esempio il contenuto del carrello di un negozio elettronico; di tracciare la navigazione dell'utente, ad esempio per fini statistici o pubblicitari.

[14] Regolamento generale sulla protezione dei dati, art. 4, par. 2.

È sufficiente anche una sola delle operazioni elencate per ritenere in corso un trattamento di dati personali.

La protezione dei dati si applica anzitutto al trattamento dei dati negli archivi manuali, ossia i fascicoli cartacei appositamente strutturati, ma anche, e soprattutto, al trattamento automatizzato di dati personali. Il trattamento automatizzato di dati personali riguarda il "trattamento interamente o parzialmente automatizzato di dati personali" [15]. Ciò si traduce concretamente nel fatto che qualsiasi trattamento di dati personali compiuto attraverso mezzi automatizzati con l'ausilio, ad esempio, di un personal computer, un dispositivo mobile o un router, è disciplinato dalle norme del GDPR.

3.3. Le parti in gioco

Il GDPR (art. 4), così come faceva la Direttiva Madre, individua i principali soggetti protagonisti del trattamento dei dati nelle figure dell'Interessato, del Titolare e del Responsabile.

L'Interessato al trattamento (anche detto, *data subject*) è la persona fisica a cui si riferiscono i dati personali. Poiché il diritto alla tutela dei dati personali si riferisce soltanto alle persone fisiche, Interessato può essere solo una persona fisica, e non una persona giuridica, un ente o un'associazione. È bene sottolineare che in considerazione del fatto che i trattamenti dei dati personali coinvolgono l'intera società, lo status di Interessato è molto più diffuso rispetto al passato. Basti pensare alle telecamere di controllo del traffico, le *fidelity card*, le *mobile app*, i *social media*, per cogliere come, in ogni momento, ogni individuo è potenziale Interessato di un trattamento.

Diversamente, il Titolare del trattamento (anche detto, *data controller*) è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina il motivo e le modalità del trattamento di dati personali. Al fine di determinare chi è il Titolare si fa affidamento a parametri sostanziali: chi concretamente determina le finalità e i mezzi del trattamento è a tutti gli effetti il Titolare, indipendentemente da qualsiasi designazione formale. Non manca tuttavia un'eccezione a questa regola: quando le finalità e i mezzi del trattamento sono stabiliti dalla legge – sia essa dell'Unione Europea o degli Stati membri – anche il Titolare del trattamento (o i criteri specifici applicabili alla sua identificazione) può essere individuato dalla legge stessa.

Il nuovo Regolamento (art. 26) ha introdotto la possibilità che vi siano più Titolari del medesimo trattamento (Contitolari) quando due o più Titolari del

[15] Regolamento generale sulla protezione dei dati, art. 2, par. 1 e art. 4, par. 2.

trattamento determinano congiuntamente le finalità e i mezzi del trattamento. Dalla decisione di trattare insieme i dati per una finalità comune nasce il rapporto di contitolarità, che deve essere regolato in modo trasparente attraverso un accordo interno in cui i Contitolari si suddividono le diverse responsabilità in merito all'osservanza degli obblighi di legge. A prescindere dalle suddivisioni di responsabilità stabilite con l'accordo, a garanzia di un'effettiva tutela dei diritti dell'Interessato, quest'ultimo può esercitare i propri diritti nei confronti e contro ciascun Contitolare del trattamento.

Un'altra grande novità del GDPR è la maggior responsabilizzazione (*accountability*) del Titolare. Il Titolare deve mettere in atto (nonché riesaminare ed aggiornare) adeguate misure tecniche ed organizzative, per garantire ed essere in grado di dimostrare che le operazioni di trattamento vengano effettuate in conformità al Regolamento. Peraltro il nuovo Regolamento non si limita a stabilire questa responsabilità in termini astratti. Al contrario specifica la necessità di tenere in considerazione la natura, l'ambito di applicazione, il contesto e le finalità del trattamento, chiedendo che queste valutazioni si traducano sia nella scelta delle misure tecniche e organizzative da adottare nel contesto aziendale sia nell'attuazione di *privacy policy* conformi [16].

È inoltre utile precisare che sebbene le persone fisiche possono essere Titolari del trattamento, i privati non rientrano nell'ambito di applicazione delle norme del GDPR quando trattano dati personali di altre persone nell'ambito di attività a carattere esclusivamente personale o domestico [17]. I dati di persone identificate o identificabili all'interno di un diario personale, ad esempio, sono esonerati dalle norme del GDPR. Non sfugge, tuttavia, che queste attività a carattere personale o domestico possano essere svolte online e attraverso l'uso di *social network*. Se queste attività abbiano carattere esclusivamente personale o domestico dipende dalle circostanze, e il sempre più diffuso accesso dei privati ai *social media* e ad altri strumenti elettronici di condivisione dell'informazione che ampliano la loro sfera "privata" rende sempre più arduo separare il trattamento personale da quello professionale.

Infine, occorre ricordare il Responsabile del trattamento (anche detto, *data processor*). Questi è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare. Come nel caso di contitolarità, anche il rapporto tra Titolare e Responsabile del trattamento deve essere disciplinato da un accordo tra le parti, che vada altresì a specificare la durata del trattamento, la natura e le finalità del trattamento nonché il tipo di dati personali e le categorie di Interessati a cui gli stessi dati

[16] Regolamento generale sulla protezione dei dati, art. 24.

[17] Regolamento generale sulla protezione dei dati, considerando 18.

si riferiscono. Quando la scelta delle modalità del trattamento è delegata al Responsabile, al Titolare è comunque chiesto di esercitare un appropriato controllo sulle decisioni del Responsabile in merito ai mezzi del trattamento. Poiché la responsabilità generale rimane in capo al Titolare, egli deve poter verificare che le scelte del Responsabile siano conformi alle disposizioni in materia di protezione dei dati e alle sue istruzioni. Il Responsabile che non rispetta dette istruzioni diventa Titolare del trattamento, nella misura in cui non si è attenuto alle condizioni prescritte dal Titolare. Infine il GDPR precisa che il Responsabile del trattamento non può, di propria iniziativa e senza previa autorizzazione del Titolare, ricorrere ad altro Responsabile del trattamento. Nei casi in cui questa autorizzazione sussista, il Responsabile di secondo livello è soggetto agli stessi obblighi a cui è soggetto il primo Responsabile nei confronti del Titolare. Qualora il Responsabile di secondo livello ometta di adempiere ai propri obblighi risponde il Responsabile iniziale, che conserva nei confronti del Titolare l'intera responsabilità [18].

In aggiunta alle figure finora considerate, il GDPR ne ha prevista una quarta: il Rappresentante del trattamento nell'Unione Europea (anche detto, *representative*), ossia colui che fa le veci del Titolare e del Responsabile del trattamento, e da questi designato, quando essi non sono stabiliti nell'Unione. Il GDPR ha introdotto questo nuovo ruolo alla luce dell'estensione del suo campo di applicazione territoriale rispetto alla precedente Direttiva. Sancendo l'applicabilità delle sue disposizioni i) ai Titolari e ai Responsabili del trattamento che si trovano nell'Unione, a prescindere dal luogo in cui sia effettuato il trattamento dei dati personali, e ii) ai Titolari e ai Responsabili non stabiliti nell'Unione nel caso in cui il trattamento abbia ad oggetto dati personali di Interessati che si "trovano" (anche virtualmente) nell'Unione, il Regolamento produce un'efficacia "extraterritoriale". Esso è infatti applicabile sia se l'Interessato si trovi realmente o virtualmente nel territorio europeo, sia se il Titolare e/o il Responsabile del trattamento siano stabiliti nell'Unione, ed anche se il trattamento viene effettuato all'esterno dell'Unione stessa. Dalla condizione che il Regolamento si applica anche al trattamento dei dati personali di Interessati che si trovano nell'Unione ma effettuato da un Titolare o da un Responsabile del trattamento stabiliti fuori dall'Unione, nasce in capo a loro l'obbligo di designare un Rappresentante in uno degli Stati membri in cui si trovano gli Interessati i cui dati personali sono trattati. Il Rappresentante funge da interlocutore verso le Autorità di controllo e verso gli Interessati per tutte le questioni inerenti il trattamento [19].

---

[18] Regolamento generale sulla protezione dei dati, art. 28.

[19] Regolamento generale sulla protezione dei dati, art. 3.2; art. 27.

4. I principi che regolano l'utilizzo dei dati personali

Il trattamento dei dati personali deve avvenire conformemente ai principi sanciti all'art. 5 del Regolamento. Essi rappresentano la base giuridica del trattamento e traggono spunto dai FIPPs statunitensi per accentuarne la portata. Questi principi comprendono:

- liceità, correttezza e trasparenza;
- limitazione della finalità;
- minimizzazione dei dati;
- esattezza dei dati;
- limitazione della conservazione;
- integrità e riservatezza.

Di seguito, se ne propone una breve illustrazione, muovendo dal principio di liceità, correttezza e trasparenza, in ragione del quale, perché sia lecito, il trattamento di dati personali richiede il consenso dell'Interessato o un'altra base giuridica legittima prevista dalla legislazione in materia di protezione dei dati. In altri termini, affinché i dati siano trattati in modo lecito, il trattamento deve essere conforme a uno dei suoi presupposti elencati all'art. 6 per i dati personali non sensibili, e all'art. 9, per le categorie particolari di dati (o dati sensibili).

Il consenso è tra questi il presupposto principale per il trattamento lecito dei dati. Per consenso s'intende "qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'Interessato" [20]. In altri termini, il consenso deve essere espresso mediante un atto positivo chiaro (tanto un'azione come una dichiarazione), con il quale l'Interessato manifesta l'intenzione libera (vale a dire, per esempio, che se un servizio è condizionato al consenso questo non può essere considerato come liberamente dato), specifica, informata (con una descrizione precisa e facilmente comprensibile dei motivi rispetto alla quale è richiesto il consenso) e inequivocabile, di accettare il trattamento dei propri dati personali. Affinché il consenso sia inequivocabile non è necessario che il consenso sia esplicito, potendo anche essere implicito (anche se non tacito) purché non sussista alcun dubbio che con il suo comportamento l'Interessato abbia voluto comunicare il proprio consenso (per esempio, l'inerzia non può costituire manifestazione di consenso, come anche i moduli precompilati e caselle già pre-spuntate). In due casi specifici è invece richiesto che il consenso sia esplicito: i) per le categorie particolari di dati (anche detti "dati sensibili"), e ii) per le decisioni basate su trattamenti auto-

[20] Regolamento generale sulla protezione dei dati, art. 4, par. 11.

matizzati, compresa la profilazione. Inoltre, in quanto necessariamente specifico, laddove il consenso sia richiesto mediante una dichiarazione scritta che copre anche altri aspetti (per esempio, i termini di servizio di un sito web) la richiesta di consenso deve essere espressa utilizzando un linguaggio semplice e chiaro e in forma comprensibile e facilmente accessibile, in modo che distingua chiaramente il consenso dalle altre questioni [21].

Il Regolamento introduce una protezione specifica per il consenso dei minori, ponendo attenzione ai rischi e alle conseguenze del trattamento dei loro dati online. Dall'entrata in vigore del GDPR, quindi, quando i fornitori di servizi della società dell'informazione trattano dati personali di minori di età inferiore a 16 anni sulla base del consenso, il trattamento può considerarsi lecito "soltanto se e nella misura in cui tale consenso è prestato o autorizzato dal titolare della responsabilità genitoriale" [22].

In ogni caso, l'Interessato deve avere il diritto di revocare il consenso in qualsiasi momento, con la stessa facilità con cui è stato fornito.

Oltre al consenso, però, l'art. 6, del GDPR prevede altri cinque presupposti che rendono lecito il trattamento dei dati: quando il trattamento dei dati personali è necessario (1) per l'esecuzione di un contratto; (2) per l'esecuzione di un compito connesso all'esercizio di pubblici poteri; (3) per adempiere un obbligo legale; (4) per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, o; (5) se necessario per la salvaguardia degli interessi vitali dell'interessato.

Tra questi, la condizione legittimante che più rileva nella prassi commerciale è rappresentata dalla esistenza di un contratto o di trattative pre-contrattuali. Lo scambio di volontà sul rapporto contrattuale sovrastante assorbe lo scambio di volontà necessario per il trattamento dei dati personali. Da ciò consegue che questo presupposto vale soltanto negli stretti confini delle prestazioni dedotte nel contratto e di quanto necessario per l'adempimento contrattuale.

Quanto invece al principio di limitazione della finalità, esso prevede che il trattamento di dati personali venga effettuato per una finalità specifica e ben definita, e solo per scopi ulteriori e compatibili con la finalità iniziale. Si rivela pertanto illecito il trattamento dei dati per finalità non definite o illimitate, basato unicamente sulla considerazione che potrebbero essere utili in futuro: ogni nuova finalità di trattamento richiede una nuova base giuridica distinta [23], a dimostrazione di come l'Interessato debba sempre essere messo nelle condi-

[21] Regolamento generale sulla protezione dei dati, art. 7.

[22] Regolamento generale sulla protezione dei dati, art. 8, par. 1.

[23] Regolamento generale sulla protezione dei dati, art. 5, par. 1, lett. b).

zioni di avere il controllo dell'uso che i terzi fanno dei suoi dati personali. A ben vedere, però, fa eccezione al principio di limitazione della finalità il trattamento dei dati a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica e a fini statistici, ancorché per questo ulteriore trattamento devono essere previste garanzie adeguate, come l'anonimizzazione, la criptatura o la pseudonimizzazione dei dati e la limitazione dell'accesso ai dati [24].

Per ciò che invece concerne il principio di minimizzazione dei dati, esso legittima il trattamento di dati che siano "adeguati, pertinenti e limitati rispetto alle finalità per le quali sono trattati" [25]. I dati personali scelti per il trattamento devono cioè essere necessari per conseguire l'obiettivo generale dichiarato dal Titolare, al quale è dunque richiesto di confinare la raccolta ai dati direttamente pertinenti allo scopo specifico perseguito dal trattamento. E sempre in questo solco si colloca il principio di esattezza dei dati che richiede, sempre al Titolare del trattamento, di adottare le misure volte a garantire con ragionevole certezza che i dati personali siano esatti e aggiornati. In base alla finalità del trattamento, potrebbe cioè essere preteso il controllo regolare e costante dei dati, aggiornandoli per garantirne l'esattezza, a causa del potenziale danno per l'Interessato, qualora i dati dovessero rimanere inesatti [26].

A ciò si aggiunge il principio della limitazione della conservazione. Esso esige che i dati personali siano "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" [27]. Quando queste finalità sono state soddisfatte i dati devono essere cancellati o comunque anonimizzati. Al fine di garantire che i dati non siano conservati più a lungo del necessario, il Titolare del trattamento dovrebbe dunque stabilire un termine per la cancellazione o per la verifica periodica [28]. Così, il rispetto del principio dell'integrità e riservatezza pretende che il Titolare utilizzi misure di sicurezza tecniche ed organizzative adeguate per proteggere i dati personali da trattamenti non autorizzati o illeciti, dalla loro perdita o distruzione o dal danno accidentale. La sicurezza non interessa, quindi, il solo dato bensì l'intero ciclo del suo trattamento [29]. A questo proposito il Regolamento precisa al Titolare e al Responsabile che sono richieste quelle misure tecniche e organizzative

[24] Regolamento generale sulla protezione dei dati, art. 6, par. 4.

[25] Regolamento generale sulla protezione dei dati, art. 5, par. 1, lett. c).

[26] Regolamento generale sulla protezione dei dati, art. 5, par. 1, lett. d).

[27] Regolamento generale sulla protezione dei dati, art. 5, par. 1, lett. e).

[28] Regolamento generale sulla protezione dei dati, considerando 39.

[29] Regolamento generale sulla protezione dei dati, art. 5, par. 1, lett. f).

tali da garantire "un livello di sicurezza adeguato al rischio" [30]. Nel valutare l'adeguato livello di sicurezza essi devono tenere conto non solo del rischio derivante da accessi non autorizzati, ma anche dai rischi propri, come la perdita o la distruzione di dati.

Complessivamente, dunque, i principi che disciplina il trattamento dei dati personali, oltre a rendere protagonista l'Interessato, facendo transitare da questi le decisioni tramite il consenso informato, mirano a garantire un uso dei dati personali che sia strettamente necessario nelle quantità, nei tempi e nei modi agli obiettivi espressamente dichiarati per i quali il Titolare ha deciso di raccogliere i dati.

5. I diritti dell'Interessato

Con l'obiettivo di limitare gli squilibri di potere tra il Titolare del trattamento e il *data subject*, il Regolamento attribuisce a quest'ultimo determinati diritti affinché possa esercitare un maggiore controllo sul trattamento dei propri dati personali. Anche di questi se ne offre una spiegazione concisa.

In ragione del diritto di trasparenza e informativa, i dati personali devono essere trattati in modo chiaro nei confronti dell'Interessato. La trasparenza è un requisito sistemico, che comprende l'informativa sul trattamento dei dati per l'espressione del consenso ma che va oltre alla stessa, includendo esemplificativamente anche i flussi di informazioni dovuti all'Interessato riguardo ai suoi diritti, l'assistenza all'Interessato per la risposta alle sue istanze di trasparenza, come pure le comunicazioni delle violazioni dei suoi dati (*data breach*) [31].

Per quanto invece concerne il diritto di accesso ai propri dati personali, esso è anzitutto un elemento del diritto fondamentale alla protezione dei dati personali della Carta dei diritti fondamentali dell'UE [32]. Viene altresì riconosciuto nel nuovo Regolamento, stabilendo che ogni *data subject* ha il diritto di ottenere dal Titolare la conferma o meno dell'esistenza dei propri dati, del tipo di trattamento e, più in generale, di ottenerne l'accesso [33]. Tutte le informazioni comunicate all'Interessato devono essere fornite in forma comprensibile, tale per cui abbreviazioni tecniche, termini codificati o acronimi non

[30] Regolamento generale sulla protezione dei dati, art. 32.

[31] Regolamento generale sulla protezione dei dati, art. 12.

[32] Carta dei diritti fondamentali dell'Unione Europea, art. 8, par. 2.

[33] Regolamento generale sulla protezione dei dati, art. 15.