LUISS

Corso di laurea in Economia e Management

Cattedra Diritto Commerciale

# Privacy e gestione dei dati personali nella compravendita online.


Prof. Raffaele Lener

RELATORE

Matr. 261461

CANDIDATO


Anno Accademico 2022/2023

# *Privacy e gestione dei dati personali nella compravendita online.*

## *Indice*




*Manfredi Albanese Ginammi - 261461*

# INTRODUZIONE

Nell'era digitale in cui viviamo, la privacy e la gestione dei dati personali sono diventate tematiche di fondamentale importanza. Con l'avvento di Internet e delle tecnologie digitali, siamo costantemente connessi e interagiamo con una miriade di piattaforme e servizi online. Questo ha comportato una crescita esponenziale nella raccolta e nell'elaborazione dei dati personali, generando una serie di interrogativi e preoccupazioni riguardo alla nostra privacy.

I dati personali sono informazioni che identificano o possono essere utilizzate per identificare un individuo. Questi includono nome, indirizzo, numero di telefono, indirizzo email, dati finanziari, posizione geografica e persino le nostre preferenze personali. Le organizzazioni, sia pubbliche che private, raccolgono e trattano questi dati per vari scopi, come ad esempio fornire servizi personalizzati, migliorare la pubblicità mirata o condurre ricerche di mercato.

Tuttavia, la raccolta e l'elaborazione dei dati personali possono comportare rischi significativi per la privacy degli individui. I dati possono essere oggetto di accesso non autorizzato, di perdite o di utilizzo improprio. Inoltre, l'interconnessione di molteplici servizi e piattaforme può creare un profilo estremamente dettagliato degli utenti, che può essere utilizzato per scopi indesiderati come la discriminazione o la manipolazione delle scelte degli individui.

La gestione responsabile dei dati personali è diventata una priorità fondamentale per le organizzazioni e per le autorità di regolamentazione.

In tutto il mondo, sono state introdotte leggi e normative specifiche per garantire la protezione dei dati personali e il rispetto della privacy degli individui.

Ad esempio, il Regolamento Generale sulla Protezione dei Dati (GDPR) nell'Unione Europea stabilisce una serie di diritti degli utenti e obblighi per le organizzazioni che raccolgono e trattano dati personali.

Inoltre, le violazioni dei dati personali sono diventate sempre più frequenti, con casi di risonanza che coinvolgono grandi aziende e organizzazioni. Questi episodi hanno sollevato preoccupazioni tra il pubblico riguardo alla sicurezza dei propri dati personali e alla responsabilità delle organizzazioni nel proteggerli adeguatamente.

Nel contesto della crescente digitalizzazione, è essenziale che gli individui comprendano i loro diritti e le implicazioni della condivisione dei propri dati personali. La consapevolezza degli utenti è fondamentale per prendere decisioni informate sulla condivisione delle informazioni personali e sulla fiducia nelle organizzazioni che le trattano.

# CAPITOLO I: *Il diritto alla privacy*

## 1. Considerazioni generali

Il diritto alla privacy è riconosciuto come un diritto umano fondamentale dalla maggior parte delle costituzioni e delle leggi in tutto il mondo. In Europa, il diritto alla privacy è protetto dal Regolamento Generale sulla Protezione dei Dati (GDPR), che è entrato in vigore il 25 maggio 2018.

Il GDPR armonizza le leggi sulla privacy nell'Unione Europea e fornisce una base uniforme per la protezione dei dati personali. Il regolamento si applica a tutte le organizzazioni che gestiscono dati personali di cittadini europei, indipendentemente dalla loro sede o dalla loro nazionalità.

Il GDPR stabilisce regole chiare per la raccolta, l'elaborazione e la conservazione dei dati personali, e garantisce che i cittadini europei abbiano il diritto di controllare le proprie informazioni personali. Tra i diritti garantiti dal GDPR ci sono il diritto di accesso ai propri dati, il diritto di correggere o cancellare i propri dati e il diritto di limitare o opporsi all'elaborazione dei propri dati.[1]

Inoltre, il GDPR impone alle organizzazioni che gestiscono dati personali di designare un Responsabile della Protezione dei Dati (RPD), che ha il compito di garantire il rispetto del regolamento e di fornire assistenza e consulenza alle organizzazioni in materia di protezione dei dati.

Anche in Italia esiste una legge sulla privacy che regola la gestione dei dati personali. La legge italiana sulla privacy si basa sulla Direttiva europea sulla protezione dei dati del 1995 ed è stata aggiornata con il Regolamento europeo del 2018.[2]

La legge italiana sulla privacy fornisce una serie di norme e obblighi per la protezione dei dati personali, tra cui il consenso esplicito per la raccolta e l'elaborazione dei dati personali, l'obbligo

[1] D, N Ellison, Social Network Sites: Definition, History, and Scholarship' Journal of Computer-Mediated Communication, Vol. 13(1) (2007)

[2] Gelman A., Carlin J. B., Stern H. S., Dunson D. B., Vehtari A., and D. Rubin B., "Bayesian Data Analysis," Third Edition, CRC Press, 2013.

di informare le persone sui loro diritti in materia di protezione dei dati e l'obbligo di notificare le violazioni dei dati.

L'evoluzione storica del diritto alla privacy risale almeno al XIX secolo, quando il concetto di privacy cominciò a essere discusso in modo più ampio nel contesto della legge e della filosofia.

Nel 1890, i giuristi americani Warren e Brandeis pubblicarono un articolo intitolato "Il diritto alla privacy", nel quale argomentavano che la legge dovrebbe riconoscere e proteggere la privacy individuale come un diritto naturale. Questo articolo è stato uno dei primi a sostenere che la privacy individuale dovrebbe essere protetta legalmente, in quanto considerata una componente essenziale della libertà e dell'autonomia individuali.

Nel corso del XX secolo, il diritto alla privacy si è evoluto in risposta alle sfide poste dallo sviluppo della tecnologia e dalla crescente raccolta e utilizzo di dati personali. Nel 1948, l'Assemblea Generale delle Nazioni Unite ha adottato la Dichiarazione Universale dei Diritti Umani, che sancisce il diritto alla privacy come un diritto umano fondamentale.

Negli anni '60 e '70, la crescente preoccupazione per la privacy individuale ha portato alla promulgazione di leggi come l'Electronic Communications Privacy Act (ECPA) negli Stati Uniti e la Data Protection Act del 1974 nel Regno Unito, che hanno cercato di proteggere i cittadini dalle intrusioni nella loro privacy causate dall'uso delle tecnologie dell'informazione.

Negli ultimi anni, il diritto alla privacy è stato influenzato dalla diffusione di Internet e delle tecnologie digitali. Nel 2016, l'Unione Europea ha adottato il Regolamento Generale sulla Protezione dei Dati (GDPR), una legge estremamente ambiziosa che unifica le normative sulla privacy in Europa e introduce nuovi diritti per i cittadini europei, come il diritto alla portabilità dei dati e il diritto all'oblio.

Negli anni, la protezione della privacy è stata oggetto di numerosi interventi da parte della giurisprudenza europea e nazionale, che hanno ridefinito il concetto di tutela della riservatezza. Si è passati da una nozione "statica" ad una "dinamica", dovuta probabilmente all'interazione tra i diversi ambiti giuridici interessati dall'istituto della privacy e ad altri diritti fondamentali. Questo ha reso il sistema di tutela della privacy complesso, poiché interessa molteplici settori e si è evoluto in sintonia con le mutate condizioni ambientali e sociali.[3]

[3] E. Saraceni, Privacy. Nota di rinvio, in questa Rivista, 3, 2008, pp. 1017-1019: 1017.

La metafora biologica utilizzata per descrivere le due forme di tutela del diritto alla riservatezza è molto appropriata. La tutela 'statica' della privacy può essere paragonata ad un sistema monocellulare, che funziona come una barriera per proteggere la privacy individuale da intrusioni esterne. D'altra parte, la tutela 'dinamica' può essere paragonata ad un organismo pluricellulare complesso, in cui le cellule interagiscono, metabolizzano e rielaborano gli stimoli esterni per creare qualcosa di nuovo.

In altre parole, la tutela 'dinamica' non si limita a proteggere la privacy individuale, ma considera anche il contesto in cui si verifica la violazione della privacy e cerca di adeguarsi alle mutevoli condizioni sociali ed ambientali. Questo sistema è in grado di adattarsi e di creare nuove forme di protezione della privacy, proprio come un organismo pluricellulare può evolversi per adattarsi alle condizioni ambientali mutevoli.

La plasticità morfogenetica menzionata nella metafora biologica si riferisce alla capacità di questo sistema di tutela dinamica di modificare la sua struttura in risposta ai cambiamenti ambientali. Questo significa che, se il contesto sociale o ambientale cambia, il sistema di tutela della privacy può evolversi per adeguarsi a tali cambiamenti.

Successivamente, nei progressivi stadi vitali dell'istituto in commento, l'intervento dell'attività ermeneutica effettuata dalle Corti nazionali ed europee ha permesso la 'differenziazione' della tutela dell'identità personale e morale attraverso l'opera di bilanciamento giurisprudenziale, adottando così una nuova chiave interpretativa segnata e, al contempo, segnante la profonda plasticità del diritto alla riservatezza.

Per quanto attiene alle pronunce della Corte Europea dei Diritti dell'Uomo, occorre segnalare come, nell'anno in corso, esse abbiano definito in maniera 'plastica' la soglia di tollerabilità massima dell'invasione della riservatezza sulla base delle fattispecie esaminate.

A tal proposito, si segnala la sentenza del 12 giugno 2014[4] che affronta il mancato rinnovo di un contratto di insegnamento della religione cattolica in una scuola pubblica basato, fondamentalmente, sulla diffusione di alcune informazioni personali riguardanti il docente a cui era stato affidato precedentemente l'insegnamento medesimo.

[4] Ci si riferisce alla Sentenza della Corte di Cassazione, 3 aprile 2014, n. 7783

La Corte, esaminando la fattispecie in commento alla luce del contenuto normativo dell'art. 8 della Convenzione Europea dei Diritti dell'Uomo, nonché dei precedenti in materia, ha proceduto a verificare la proporzionalità della mi-sura adottata per il caso specifico, tenendo in particolare considerazione quanto disposto dalle norme che disciplinano l'insegnamento della religione cattolica all'interno delle scuole pubbliche spagnole.

Conseguentemente, richiamati i criteri utili al fine di accertare la violazione della riservatezza, nonché le norme interessate dal Concordato e dal Codice di Diritto Canonico, è stata appurata l'insussistenza della violazione della riservatezza alla vita privata e familiare, giacché il diniego a rinnovare il contratto di insegnamento era stato ritenuto una misura proporzionata alla fattispecie esaminata.

Proseguendo la rassegna, si segnala una pronuncia collocantesi in un ambito interdisciplinare, ovverosia, tra il diritto all'obiezione di coscienza alle trasfusioni di sangue, da un lato, ed il dovere (ritenuto prevalente) di riservatezza di tale dato contenuto all'interno delle cartelle cliniche, dall'altro.

Infine, sempre in ambito interdisciplinare si pone un'ulteriore pronuncia della Corte Europea dei Diritti dell'Uomo riguardante le conversazioni telefoniche effettuate all'interno di un penitenziario turco.[5]

Nella fattispecie in questione, i ricorrenti (detenuti all'interno di una prigione turca) si dolevano di non poter parlare in lingua curda nel corso delle telefonate loro concesse dal penitenziario. Conseguentemente la Corte, dopo aver preso in esame gli interessi contrapposti, vale a dire, le esigenze di sicurezza del penitenziario, da un lato, ed il diritto alla riservatezza delle comunicazioni, dall'altro, ha accolto il ricorso ritenendo che il divieto di parlare in lingua curda fosse una misura eccessiva e sproporzionata per le esigenze del carcere. Per quanto concerne le pronunce provenienti dal territorio nazionale, si può rilevare un'interessante sentenza della Terza Sezione della Corte di Cassazione inerente il bilanciamento tra diritto alla privacy e diritto alla difesa.

Invero, la Corte ha affermato che, in conformità al filone giurisprudenziale in materia, possono essere assunti alcuni dati personali necessari alla difesa di un diritto, purché la produzione di tali

[5] R. Clarke, Internet privacy concerns confirm the case for intervention. Communications of the ACM, 1999, 42(2), 60-67.

informazioni sia pertinente alla tesi difensiva e non eccedente alle sue finalità e che, quindi, essi siano utilizzati esclusivamente nei limiti di quanto necessario al legittimo ed equilibrato esercizio della propria difesa.

In tale senso, seguendo il criterio di proporzionalità nel bilanciamento tra il diritto alla riservatezza ed il diritto alla difesa, si inserisce la maggior parte della giurisprudenza di legittimità del corrente anno. Difatti, sia la pronuncia del Consiglio di Stato che la pronuncia del T.A.R. Firenze affrontano la questione relativa all'ostensibilità dei dati sensibili e supersensibili per motivi difensivi.

Entrambe le pronunce, richiamando un preciso filone giurisprudenziale, sono concordi nell'affermare che la produzione di tali dati non possa essere legata a qualsivoglia posizione giuridica finale, bensì occorra comparare quest'ultima al diritto alla riservatezza, al fine di valutare se tale diritto riceva eguale protezione giuridica dall'ordinamento.

Per quanto di rilievo nell'ambito della titolarità del trattamento dei dati sensibili si può segnalare la sentenza della Corte di Cassazione dell'8 aprile 2014, n. 8184 che precisa come la gestione di tali dati spetti esclusivamente alla persona giuridica titolare del trattamento e che, in seguito alla stipulazione di un contratto di affitto, spetti alla persona giuridica affittuaria la gestione di tali dati e non più alla precedente persona giuridica.[6]

In merito a questa tematica si segnalano, inoltre, gli interventi del Garante della Privacy in merito al trattamento dei dati genetici (Autorizzazione 8/2013) ed al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale del paziente (Autorizzazione 2/2013).

Quest'ultima autorizzazione permette di poter trattare (per taluni casi specifici) i dati relativi allo stato di salute ed alla vita sessuale del paziente, mentre, il provvedimento inerente ai dati genetici attiene al trattamento di materiale biologico volto a diagnosi pre-impianto od a procedure di fecondazione assistita. [7]

In merito a tali interventi dell'Authority occorre porre in rilievo come l'oggetto delle autorizzazioni abbia avuto un decisivo mutamento nel corso degli ultimi anni, giacché non sembra più interessare solamente l'archiviazione di meri dati statistici, ma la vera e propria

[6] P. Perri, Il diritto alla riservatezza, Giuffrè Editore, 2019, p. 367.
[7] Freedman D., "Statistics," Fourth Edition, W.W. Norton & Company, 2007.

conservazione e catalogazione di parti biologiche, andando così a riscrivere il concetto di archiviazione di dati sensibili che oggi sembrano estendersi fino a quelli contenuti nel codice genetico.

## 2. Il rapporto fra privacy e trattamento dei dati personali

La privacy e il trattamento dei dati personali sono concetti strettamente correlati ma non sono la stessa cosa.

La privacy si riferisce al diritto di ogni individuo di mantenere il controllo sulla propria vita privata, compresa la propria immagine, la propria reputazione e le proprie informazioni personali. In altre parole, la privacy riguarda la protezione della sfera privata dell'individuo e delle sue informazioni personali.[8]

Il trattamento dei dati personali, invece, si riferisce alle attività che coinvolgono la gestione e l'utilizzo di informazioni personali, come la raccolta, la conservazione, l'elaborazione e la condivisione di tali informazioni. Il trattamento dei dati personali può influire sulla privacy dell'individuo se questi dati vengono utilizzati in modo improprio o non autorizzato.

In sintesi, la privacy è un concetto più ampio che riguarda il diritto all'autodeterminazione informativa, mentre il trattamento dei dati personali riguarda le operazioni specifiche effettuate su tali dati. La protezione della privacy individuale richiede quindi anche una protezione efficace del trattamento dei dati personali. Inoltre, la regolamentazione del trattamento dei dati personali è un modo importante per proteggere la privacy delle persone.[9]

## 3. Privacy e protezione dei dati personali in rete

Anche la privacy e la protezione dei dati personali in rete sono due concetti correlati ma distinti.

---

[8] Ziccardi G., Privacy, big data e internet delle cose, Giappichelli Editore, 2018, p. 45.
[9] Gelman A. et al., , "Bayesian Data Analysis," Third Edition, CRC Press, 2013, p. 4.

La privacy in rete si riferisce alla capacità dell'individuo di mantenere il controllo sulla propria vita privata quando si naviga in Internet e utilizza i servizi online. Questo include la protezione dell'identità, delle informazioni personali e della reputazione online.

La protezione dei dati personali in rete si riferisce alle misure adottate per garantire che i dati personali dell'utente vengano trattati in modo corretto, trasparente e sicuro quando si utilizzano servizi online. Queste misure comprendono l'utilizzo di password sicure, la crittografia dei dati, l'autenticazione a due fattori e altre tecnologie di sicurezza.

In sintesi, la privacy in rete riguarda il diritto dell'individuo di mantenere la propria vita privata anche quando si utilizzano servizi online, mentre la protezione dei dati personali in rete riguarda le misure adottate per garantire che i dati personali dell'utente vengano trattati in modo sicuro e trasparente quando si utilizzano tali servizi. Entrambi questi concetti sono importanti per garantire una navigazione sicura e protetta in rete e sono regolamentati da normative specifiche, come il GDPR nell'Unione Europea e la California Consumer Privacy Act negli Stati Uniti.[10]

## 4. Il diritto alla privacy e i Big Data

Nell'era digitale, il diritto alla privacy e i Big Data rappresentano una sfida sempre più importante.

I Big Data si riferiscono a enormi quantità di dati raccolti da diverse fonti e utilizzati per identificare modelli e tendenze utili per le aziende, i governi e altri soggetti. Tuttavia, l'utilizzo dei Big Data può rappresentare una minaccia per la privacy, in quanto questi dati possono essere utilizzati per creare profili dettagliati degli individui, raccogliendo informazioni sensibili come la salute, le preferenze politiche, le opinioni personali e altro ancora.

Il diritto alla privacy e la protezione dei dati personali sono fondamentali in questo contesto, poiché gli individui hanno il diritto di controllare e limitare l'accesso e l'utilizzo dei propri dati personali. Il GDPR (General Data Protection Regulation) nell'Unione Europea impone regole rigide sul trattamento dei dati personali, inclusi i Big Data.

In base al GDPR, i dati personali devono essere trattati in modo lecito, corretto e trasparente, e solo per scopi specifici, espliciti e legittimi. Inoltre, le persone hanno il diritto di accedere ai

[10] G. Ziccardi, Cybercrime, identità digitale e diritto alla privacy, Giappichelli Editore, 2020, p. 56.

propri dati personali, di correggerli, di cancellarli e di opporsi al loro trattamento in determinate circostanze.

Le aziende che raccolgono e utilizzano i Big Data devono rispettare queste regole e ottenere il consenso degli individui per raccogliere e utilizzare i loro dati personali.
È importante che gli enti che raccolgono e utilizzano i Big Data rispettino le leggi sulla privacy e garantiscano che le informazioni raccolte vengano utilizzate solo per scopi leciti e specifici. Ciò significa che gli individui devono essere informati sulla raccolta e l'utilizzo dei propri dati personali e devono essere in grado di esercitare il proprio diritto di accesso, correzione e cancellazione dei dati personali.[11]

Per garantire la protezione dei dati personali, le aziende devono adottare misure di sicurezza adeguate a proteggere i dati raccolti da accessi non autorizzati, perdite, alterazioni o divulgazioni indebite. Inoltre, le informazioni sensibili devono essere protette con misure di sicurezza più rigorose, come la crittografia.

È importante che le aziende rispettino il principio di minimizzazione dei dati, ovvero che raccolgano solo le informazioni strettamente necessarie per il loro scopo e che non conservino i dati personali più a lungo di quanto necessario per raggiungere lo scopo per cui sono stati raccolti. Le informazioni personali dovrebbero essere eliminate una volta che non sono più necessarie.

Inoltre, le aziende dovrebbero ottenere il consenso esplicito degli individui per la raccolta e l'utilizzo dei loro dati personali e informarli in modo chiaro e completo su come verranno utilizzati tali dati. Gli individui devono anche avere il diritto di revocare il proprio consenso in qualsiasi momento.

Quando parliamo, invece, di "big data" ci riferiamo a grandi insiemi di dati costituiti da frammenti elementari di informazioni, che possono essere raccolti e analizzati in modo massivo utilizzando specifici processi statistici, come il data mining predittivo. Questo tipo di analisi è reso possibile dalle attuali tecnologie informatiche, che offrono una potenza di calcolo sufficiente per elaborare l'intero insieme di informazioni anziché soltanto un campione rappresentativo.

[11] G. Priora, Privacy e diritto all'oblio: profili civilistici, Maggioli Editore, 2019, p .89.

Ci sono molti vantaggi nell'elaborare i big data invece di utilizzare i campioni. Ad esempio, mentre i campioni devono essere creati in modo specifico per ogni singola indagine, i dati grezzi possono essere utilizzati più volte e da più soggetti, anche per scopi diversi e combinati con altri set di dati. Tuttavia, la disciplina sulla protezione dei dati personali rappresenta un ostacolo poiché richiede il consenso informato dell'interessato per qualsiasi trattamento o trasferimento di dati personali.[12]

Ciò significa che l'uso e la combinazione delle informazioni acquisibili attraverso le tecniche di analisi dei big data possono essere frenati dalle normative sulla protezione dei dati personali. In sintesi, i big data offrono numerose opportunità di analisi e utilizzo di informazioni, ma al contempo rappresentano una sfida per le normative sulla privacy.

Spesso l'analista prende decisioni basate sulla presenza di correlazioni tra i dati, piuttosto che capire logicamente le ragioni di tali connessioni.

Questo perché le correlazioni più frequenti sono spesso indicative di una futura ripetizione di queste connessioni. Un esempio di questo è la decisione di Amazon di suggerire libri su come avere una scrivania ordinata a chi aveva acquistato libri sullo zen. Tuttavia, ci sono casi in cui i metodi di analisi dei dati producono risultati "non interpretabili", cioè basati su formule e algoritmi che utilizzano un gran numero di variabili, rendendo impossibile ricostruire il processo decisionale a posteriori, ovvero risultano impossibili da comprendere logicamente . In questi casi, si pone la questione se tali metodi possano avere lo stesso valore di quelli "interpretabili" e, in caso contrario, se possano comunque avere un ruolo da svolgere.[13]

Questo può rappresentare un problema per chi subisce gli effetti di tali decisioni e ha una ragionevole pretesa di conoscere le motivazioni dietro di esse per poter opporsi. In altre parole, se le decisioni prese attraverso l'analisi dei dati sono basate su algoritmi troppo complessi per essere interpretati dall'uomo, può essere difficile per gli individui comprendere come sono state prese tali decisioni e contestarle in caso di effetti negativi.

La questione dell'interpretabilità dei metodi di analisi dati diventa particolarmente rilevante quando tali metodi vengono utilizzati nell'esercizio dei poteri pubblici o in situazioni che

[12] S. Alibrandi, Il diritto alla privacy nell'era digitale, Aracne Editrice, 2021, p.23.
[13] A. Mantelero, Diritto alla privacy e protezione dei dati personali nell'era digitale, Giappichelli Editore, 2017, p. 56.

coinvolgono valori costituzionalmente tutelati. Infatti, in queste circostanze, è importante garantire la trasparenza e la comprensibilità dei processi decisionali, in modo che i cittadini possano conoscere le ragioni alla base delle scelte che li riguardano e possano eventualmente contestarle.

In relazione, invece, al diritto alla riservatezza è uno dei diritti fondamentali tutelati dalla Costituzione italiana e dalle norme dell'Unione Europea. In particolare, l'articolo 2 della Costituzione italiana sancisce il principio di uguaglianza di fronte alla legge, mentre gli articoli 3, 13, 14 e 15 sanciscono il diritto alla vita privata, alla libertà personale, alla libertà di domicilio e alla segretezza della corrispondenza e di ogni altra forma di comunicazione.

In aggiunta, l'articolo 8 della Convenzione Europea per la tutela dei diritti dell'uomo e delle libertà fondamentali (CEDU) e l'articolo 8 della Carta di Nizza sanciscono il diritto al rispetto della vita privata e familiare e, alla protezione dei dati personali.

La disciplina interna italiana sulla privacy si basa principalmente sul Regolamento Generale sulla Protezione dei Dati dell'Unione Europea, che, come abbiamo detto, è entrato in vigore nel 2018 in sostituzione della Direttiva Data Protection del 1995.

Il GDPR ha introdotto il concetto di privacy come "autodeterminazione informativa", che significa che l'individuo ha il diritto di avere un controllo completo sui propri dati personali e di impedire il loro utilizzo da parte di terzi.[14]

Per esercitare tale diritto, l'individuo deve prestare il proprio consenso al trattamento dei propri dati personali attraverso un contratto, che deve essere basato su una completa informativa sul trattamento dei dati e sulle conseguenze del consenso. Inoltre, l'individuo ha il diritto di accedere alle informazioni che lo riguardano, di richiedere la rettifica o la cancellazione dei dati in caso di errori o violazioni e di opporsi al loro trattamento per specifici scopi.

Tale costruzione giuridica deriva dalla concezione della privacy come un diritto inviolabile, fondamentale per l'autonoma formazione della personalità e delle relazioni interpersonali. Tuttavia, questo diritto viene spesso compromesso da esigenze economiche e di sicurezza. La Corte di Giustizia dell'Unione Europea ha affermato che la privacy dovrebbe, in linea di

[14] D. S. Sivia, "Data Analysis: A Bayesian Tutorial," Second Edition, Oxford University Press, 2006, p. 34.

principio, prevalere sugli interessi economici, ma attualmente viene sacrificata per il trattamento di enormi quantità di dati a fini di lucro.

Anche il bilanciamento tra privacy e sicurezza deve avvenire in modo proporzionato: la sorveglianza su vasta scala può avvenire solo in correlazione con un sospetto di reato e su indicazione ex lege delle Autorità competenti.

L'attuale disciplina del consenso, tuttavia, sembra insufficiente alla tutela della privacy. Da un lato, il consumatore e l'imprenditore intrattengono una trattativa iniqua, e dall'altro non viene considerato adeguatamente l'interesse collettivo che sottostà all'autodeterminazione informativa. A seguito dell'annullamento disposto dalla Corte sulla Direttiva Data Retention, il Legislatore dovrà introdurre ulteriori garanzie per la privacy, come richieste dal Giudice europeo.

In genere, si ritiene che la titolarità di una prerogativa inviolabile sia irrinunciabile, ma non necessariamente il suo esercizio. Ciò perché l'ordinamento democratico cerca di limitare il meno possibile le libertà individuali, in quanto ritiene che nessuno, più dell'individuo stesso, sia qualificato a scegliere circa la propria personalità e il proprio progetto di vita, anche quando ciò comporta l'accettazione di effetti negativi nella propria sfera giuridica.

Tuttavia, è importante notare che ogni libertà deve essere bilanciata con le esigenze di uguale tutela dei diritti che sono insite nel sistema costituzionale. [15]

In questo senso, una maggiore indisponibilità dei dati personali è spesso necessaria per proteggere due beni di rilevanza collettiva: l'uguaglianza sostanziale nel godimento del diritto alla privacy e l'interesse della comunità alla riservatezza. Il primo bene viene in rilievo nella misura in cui, come evidenziato dall'art. 3, secondo comma, della Costituzione, una vera autodeterminazione è possibile solo quando si è liberi dal bisogno economico.

Pertanto, è importante trovare un equilibrio tra la tutela dei diritti individuali e la protezione dei beni collettivi, attraverso l'imposizione di limitazioni formali alla libertà personale, che mirino a una maggiore attuazione sostanziale della libertà stessa. In questo contesto, una maggiore indisponibilità dei dati personali può essere giustificata in alcune situazioni della vita quotidiana, e anche su Internet, dove spesso l'acconsentimento alla cessione dei propri dati è l'unico modo per accedere a servizi necessari per la vita di tutti i giorni.

[15] Marozzi M., "Inferenza statistica," Esculapio, 2013, p .3.

L'autodeterminazione è un diritto fondamentale di ogni individuo, ma per poter esercitare questo diritto in modo effettivo, è necessario che l'individuo goda di una certa libertà economica. Infatti, solo quando si è liberi dal bisogno economico si può scegliere liberamente il proprio progetto di vita e realizzare la propria personalità.

Questo concetto è sottolineato anche nell'art. 3, secondo comma, della Costituzione, che afferma che tutti sono uguali davanti alla legge, senza distinzione di sesso, di razza, di lingua, di religione, di opinioni politiche, di condizioni personali e sociali.

L'uguaglianza sostanziale nel godimento del diritto alla privacy richiede quindi un'attenzione particolare per le persone che si trovano in situazioni economiche e sociali più deboli, in modo da garantire che anche loro possano godere di una protezione adeguata della loro privacy.

Diversamente, possono esservi alienazioni che sono solo apparentemente volontarie, dettate in realtà da uno stato di necessità.

Ad esempio, con ogni probabilità ricorre alla vendita di organi solo chi non ha altri mezzi di sostentamento; analogamente, sono sospette le rinunce e transazioni sui diritti nascenti dal rapporto di lavoro, perché potrebbero essere frutto della situazione di debolezza in cui si trova il prestatore rispetto al datore. [16]

Per questo il Legislatore legittimamente vieta le prime e sottopone le seconde a specifiche procedure: si tratta di una compressione formale della libertà volta a una sua maggiore attuazione sostanziale. Nel medesimo senso si giustifica un’accentuata indisponibilità dei dati personali.

Lo stesso Legislatore europeo ha preso atto di questa situazione, e come nel caso delle transazioni sul rapporto di lavoro ha assistito l’alienazione con analitiche garanzie.

La regolazione attuale però non sembra aver risolto il problema, il che fa auspicare un intervento più profondo in questa direzione; soprattutto, resta ancora tutta da affrontare la disuguaglianza sostanziale di fondo nella distribuzione dei proventi dei big data.

Tale disuguaglianza, infatti, rafforza quegli ostacoli che impediscono al consumatore un’opzione realmente volontaria. Il secondo interesse pubblico che legittima e impone una maggiore indisponibilità dei propri dati è l’autodeterminazione informativa della comunità. È incontestato

[16] Jaynes E. T., "Probability Theory: The Logic of Science," Cambridge University Press, 2003, p. 45.

che le posizioni giuridiche individuali possono essere sacrificate per un superiore interesse collettivo, purché si rispettino i principi di ragionevolezza, proporzionalità e l'intangibilità del loro «nocciolo duro». Talvolta, come in questo caso, un diritto può essere assicurato ai singoli solo se garantito all'intera società: con riguardo alle malattie infettive, ad esempio, basta qualche ammalato perché il morbo si propaghi. [17]

Per questo l'art. 32, comma 2, della Costituzione ammette che in simili ipotesi un trattamento sanitario possa essere imposto pure a chi non vuole sottoporvisi, purché esso sia anche nell'interesse dell'individuo e non leda la sua dignità; ciò in palese deroga del primo comma, che attribuisce a ciascuno un inviolabile diritto a rifiutare qualsiasi cura medica.

Anche la libertà di informazione ha valore solo se protetta in capo a tutti: scopo finale dell'art. 21 della Costituzione è assicurare un dialogo tra una pluralità di voci, perché solo in presenza di questa condizione ognuno può arricchirsi con il contributo dell'altro. È naturale quindi che lo Stato debba dettare una disciplina talvolta pervasiva per contemperare gli opposti interessi, evitare la formazione di posizioni di potere e creare la possibilità di accesso attivo e passivo ai mezzi di diffusione del messaggio.

Ebbene, anche la riservatezza oggi è un interesse di questo tipo, collettivo, oltre che individuale: rectius, può essere tutelato in capo a ciascun individuo solo se garantito a tutti, perché l'atto dispositivo di uno ha effetti negativi anche su terzi.

Tre ragioni sostengono la necessità di una regolamentazione generale che limiti il diritto individuale in materia di trattamento dei dati. La prima ragione si basa sul fatto che ogni nuovo consenso al trattamento dei dati contribuisce al dominio di pochi centri di potere economico-sociale, che possono compromettere la sovranità popolare. Ad esempio, alcune aziende del web, come Google, diventano arbitri della diffusione dei contenuti sulla rete e hanno conquistato una posizione dominante attraverso i dati personali. Ciò comporta un pericolo per la libertà di informazione, poiché il potere di mercato acquisito attraverso il possesso delle informazioni dei naviganti si traduce in un controllo sulla diffusione dei contenuti.

La seconda ragione è che il potere di mercato in sé rappresenta un pericolo per la libertà di informazione, anche se raggiunto ed esercitato in modo lecito. Ciò perché se c'è una gestione

[17] G. F. Ferrari, La tutela della privacy, Giappichelli Editore, 2021, p .67.

solitaria del mezzo, non può esserci quella pluralità di opinioni che l'art. 21 della Costituzione considera necessaria. La terza ragione è che ogni nuovo cliente, quindi ogni nuova cessione di dati all'azienda, produce un pregiudizio per l'intera comunità perché contribuisce a un dominio sulla diffusione dei contenuti in rete che mette a repentaglio i diritti di tutti.[18]

## 5. I cosiddetti cookies

I cookie sono piccoli file di testo che vengono salvati sul computer o sul dispositivo mobile dell'utente quando si visita un sito web. Questi file contengono informazioni sulle attività dell'utente sul sito, come le preferenze di navigazione e le informazioni di login, e vengono utilizzati per personalizzare l'esperienza di navigazione dell'utente e migliorare la funzionalità del sito.[19]

I cookie possono essere suddivisi in diverse categorie a seconda della loro funzione:

- Cookie tecnici: questi cookie sono necessari per il corretto funzionamento del sito web e includono ad esempio quelli utilizzati per autenticare l'utente o per ricordare le sue preferenze di navigazione.
- Cookie di profilazione: questi cookie sono utilizzati per raccogliere informazioni sul comportamento dell'utente e creare un profilo personalizzato basato su di esse. Questi cookie vengono spesso utilizzati a fini pubblicitari per fornire annunci mirati all'utente.
- Cookie di terze parti: questi cookie sono installati da siti web di terze parti e vengono utilizzati per raccogliere informazioni sulla navigazione dell'utente a fini statistici o pubblicitari.[20]

La gestione dei cookie è regolamentata dalla normativa sulla privacy, in particolare dal GDPR nell'Unione Europea. Gli utenti hanno il diritto di accettare o rifiutare l'installazione dei cookie sul proprio dispositivo e di richiedere la cancellazione dei dati raccolti attraverso i cookie. Molti browser web consentono di gestire le impostazioni dei cookie e di disattivare quelli non necessari

[18] F. Pizzetti, La tutela della privacy nella società dell'informazione, Laterza, 2018, p. 67.
[19] A. Capobianco and S. Mignani, "Metodi Statistici per le Decisioni," McGraw-Hill Education, 2017, p .34.
[20] M. Timiani, Come la privacy può rimodellare le prerogative dei consiglieri regionali, in Quaderni Costituzionali, 2, 2014, pp. 415-421

o di terze parti. Inoltre, i siti web devono fornire informazioni chiare e trasparenti sull'utilizzo dei cookie e richiedere il consenso dell'utente prima di installarli sul proprio dispositivo.

## 6. Cosa ci aspetta in futuro

Le prospettive future della privacy sono in continua evoluzione, in parallelo all'espansione del digitale e alla crescente raccolta e analisi di dati personali.

Ci sono alcune tendenze emergenti che potrebbero avere un impatto significativo sulla privacy nel futuro:

1. L'intelligenza artificiale e il machine learning potrebbero migliorare la raccolta e l'analisi dei dati personali, ma potrebbero anche aumentare le preoccupazioni sulla privacy. Ad esempio, i sistemi di riconoscimento facciale potrebbero essere utilizzati per tracciare gli individui in modo più preciso.
2. La crescente importanza dei dispositivi mobili e delle smart home potrebbe aumentare la quantità di dati personali raccolti, poiché questi dispositivi possono monitorare l'attività dell'utente in modo costante.
3. La diffusione della tecnologia blockchain potrebbe migliorare la sicurezza dei dati personali, poiché i dati verrebbero archiviati in modo distribuito e protetto da crittografia avanzata.
4. L'evoluzione della normativa sulla privacy, come il GDPR nell'Unione Europea, potrebbe continuare a imporre regole sempre più stringenti per la raccolta e l'uso dei dati personali.
5. La crescente attenzione sulla privacy potrebbe portare a una maggiore consapevolezza da parte degli utenti e a una maggiore richiesta di strumenti per il controllo dei propri dati personali.[21]

Un'altra prospettiva futura importante riguarda la privacy nell'ambito dell'Internet delle cose (IoT).

[21] Daniele Negri, Diritto alla privacy e protezione dei dati personali, Giuffrè Editore, 2020, p. 56.

L'IoT si riferisce alla connessione di oggetti di uso quotidiano a Internet, consentendo la raccolta di dati in tempo reale. Questi oggetti possono includere qualsiasi cosa, dai sensori ambientali ai dispositivi medici.

Questa tendenza rappresenta un'enorme opportunità per le aziende e i governi per migliorare la loro efficienza e offrire nuovi servizi, ma al tempo stesso presenta importanti sfide per la privacy.

Ad esempio, i dispositivi IoT possono raccogliere dati in modo costante e dettagliato sulla vita degli utenti, come i loro movimenti, i loro comportamenti e le loro abitudini. Questi dati possono essere utilizzati per creare profili dettagliati degli utenti e per tracciare la loro vita quotidiana in modo molto preciso.[22]

Ciò può rappresentare una minaccia per la privacy degli utenti, che potrebbero non essere consapevoli della quantità di dati che vengono raccolti e di come vengono utilizzati.

Per rispondere a queste sfide, sono stati sviluppati standard di sicurezza per l'IoT, come il protocollo di sicurezza Zigbee, che garantiscono la protezione dei dati degli utenti.

Tuttavia, il controllo sulla privacy degli utenti deve essere garantito non solo attraverso i protocolli di sicurezza, ma anche attraverso politiche e regolamenti che stabiliscano i diritti degli utenti sui propri dati.

In conclusione, la crescente diffusione dell'IoT rappresenta una sfida importante per la privacy, ma può anche offrire importanti opportunità per migliorare la vita degli utenti, se si riesce a trovare un equilibrio tra l'uso dei dati e la protezione della privacy.

In generale, la privacy continuerà a rappresentare una sfida sempre più importante in un mondo digitale sempre più interconnesso, e sarà necessario trovare un equilibrio tra la raccolta e l'utilizzo dei dati e la protezione dei diritti individuali alla privacy.

[22] Marozzi M., "Inferenza statistica," Esculapio, 2013, p .45.

## CAPITOLO II: *Un confronto tra il modello europeo e americano in tema di privacy*

1. Principi della privacy

È necessario comprendere i principi internazionali della privacy, soprattutto perché questi sono stati legalmente riconosciuti dai trattati. Questi trattati possono essere utilizzati per valutare gli approcci europei e americani alla privacy.

L'Organizzazione per la Cooperazione e lo Sviluppo Economico ("OCSE") è un'organizzazione internazionale con sede in Europa, creata il 14 dicembre 1960 e composta da 36 Paesi membri, tra cui gli Stati Uniti. Il precursore dell'OCSE è stata l'Organizzazione per la Cooperazione Economica Europea ("OEEC") che ha iniziato nel 1948 a supervisionare il Piano Marshall, il quale ha contribuito a ripristinare la salute economica in Europa dopo la Seconda Guerra Mondiale. Il 23 settembre 1980, l'OCSE ha approvato le Linee guida sulla protezione della privacy e dei flussi transfrontalieri di dati personali ("Linee guida OCSE"). Le Linee guida OCSE non sono obbligatorie, ma forniscono un quadro di riferimento per la legislazione sulla privacy e i pareri dei tribunali. [23]

I principi comprendono:

- Principio della limitazione della raccolta: garantisce che la raccolta dei dati personali sia lecita;

- Principio della qualità dei dati: specifica che l'uso dei dati personali deve essere accurato, completo e aggiornato;

- Principio di specificazione dello scopo: stabilisce che lo scopo della raccolta di informazioni personali deve essere esplicito prima della raccolta dei dati;

- Principio delle garanzie di sicurezza: richiede che le informazioni personali siano ragionevolmente protette contro i rischi di distruzione, perdita di informazioni, modifica, accesso non autorizzato e utilizzo;

[23] Reidenberg, J. R. (2013). American and European privacy: The past, present, and future of the debate. Journal of Comparative Law, 7(1), 98-114.

- Principio di trasparenza: richiede che le pratiche e le politiche di raccolta delle informazioni personali siano prontamente disponibili;

- Principio di partecipazione individuale: richiede che gli individui abbiano il diritto di acquisire le informazioni personali raccolte o di verificare l'esistenza dei dati.

- Principio di responsabilità: garantisce che le organizzazioni di controllo dei dati siano responsabili del rispetto dei principi di cui sopra.[24]

Negli Stati Uniti, i principi della privacy sono specificati in modo tale da non obbligare le aziende statunitensi a proteggere le informazioni personali. Tuttavia, alcuni statuti statali e federali classificano i doveri e gli obblighi in materia di privacy per quanto riguarda le informazioni personali.

Le differenze riguardano i tipi di informazioni personali e le tipologie di aziende coinvolte e riflettono i principi della privacy di notifica, scelta, trasferimento verso l'esterno, accesso, sicurezza, integrità dei dati e applicazione.

2. Approccio europeo al diritto alla privacy

I dati personali sono inequivocabilmente protetti dalla Carta dei diritti fondamentali dell'Unione europea ("EUCFR"). L'articolo 7 del Titolo II afferma che "ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle proprie comunicazioni". L'articolo 8 del Titolo II afferma che "ogni persona ha diritto alla protezione dei dati personali che la riguardano". L'articolo 8 amplia il diritto alla privacy proclamando che "tali dati devono essere trattati in modo lecito e per finalità determinate, sulla base del consenso dell'interessato o di un'altra base legittima prevista dalla legge". Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica". L'articolo 8 osserva che "l'osservanza di queste norme è soggetta al controllo di un'autorità indipendente".

[24] Clayton, R., Gellman, R., & Jochai, C. (2017). Model Privacy Notice Project: Building a user-centric privacy notice. In 26th USENIX Security Symposium (USENIX Security 17) (pp. 521-538).

Se si confrontano gli articoli 7 e 8 del Titolo II dell'EUCFR con le Linee guida dell'OCSE, è chiaro che i due documenti sono coerenti. L'articolo 7 del Titolo II garantisce che le informazioni personali siano accurate, complete e aggiornate. Si tratta di un principio fondamentale che dimostra che un'organizzazione che raccoglie e controlla le informazioni personali rispetta i diritti alla privacy delle persone e delle famiglie. Anche l'articolo 8, sezione 1, del titolo II è conforme ai principi dell'OCSE sulla qualità dei dati.

L'articolo 8, sezione 2, del titolo II tratta il principio della limitazione della raccolta, il principio della specificazione delle finalità, il principio dell'apertura e il principio della partecipazione individuale. I dati personali delle persone devono essere trattati in modo equo e con il loro consenso. L'articolo 8, sezione 3, del Titolo II intreccia il principio di salvaguardia della sicurezza e il principio di responsabilità. Pertanto, è evidente che gli articoli 7 e 8 del Titolo II soddisfano le linee guida dell'OCSE sulla privacy.

Il caso Costeja González è significativo perché esemplifica la convinzione europea che, in alcune circostanze, il diritto alla privacy sia in un certo senso il diritto all'oblio. Nella causa ”Google Spain SL, Google Inc. contro Agencia Española de Protección de Datos, Mario Costeja González (2014)”, la Corte di giustizia dell'Unione europea ("CGUE") ha stabilito che Google Spain SL e Google Inc. devono rimuovere i link alle pagine web quando le persone ne richiedono la rimozione. Il risultato della sentenza della CGUE è che un motore di ricerca su Internet deve rispondere alle richieste dei singoli che chiedono la cancellazione dei link in modo che terzi non possano accedere alle informazioni.

Quando i risultati della ricerca sono di fatto inadeguati, non più pertinenti o eccessivi dato il tempo trascorso, i link devono essere eliminati. Se il motore di ricerca si rifiuta di farlo, un cittadino dell'Unione europea può rivolgersi ai tribunali dell'UE per ottenere un risarcimento. I tribunali possono richiedere al motore di ricerca di rimuovere i link in questione.

La sentenza Costeja González è significativa perché bilancia il diritto alla privacy dell'individuo e le norme sulla protezione dei dati dell'Unione Europea con il diritto del pubblico di sapere. La sentenza garantisce che le questioni relative al giusto processo siano prese in considerazione quando si eliminano i link indesiderati.

Costeja González ha anche fatto una distinzione tra individui pubblici e privati. La CGUE ha stabilito che i diritti individuali alla privacy prevalgono sugli interessi economici delle aziende e

sul diritto del pubblico a sapere. Tuttavia, se Costeja González fosse stato un personaggio pubblico, la CGUE ha osservato che la decisione sarebbe stata diversa.

Dopo la decisione del caso, Google ha pubblicato un modulo online in cui i cittadini dell'Unione Europea o dell'Associazione Europea di Libero Scambio ("EFTA") potevano chiedere a Google di rimuovere i link con l'intesa che i dati erano inadeguati, irrilevanti, non più rilevanti o eccessivi. Nel primo giorno di pubblicazione, Google ha ricevuto oltre 12.000 richieste di rimozione di link specifici dal motore di ricerca dell'azienda. Consumer Watchdog, un gruppo di difesa dei consumatori, ha presentato un reclamo alla Federal Trade Commission ("FTC") chiedendo a Google di concedere agli americani questi stessi diritti, ma l'azienda si è rifiutata.

Rilevante a riguardo è il Regolamento generale sulla protezione dei dati è un regolamento dell'UE sulla protezione dei dati personali entrato in vigore il 25 maggio 2018. Ha sostituito la Direttiva sulla protezione dei dati dell'UE del 1995, ufficialmente nota come Direttiva 95/46/CE.

Il GDPR è importante perché, in primo luogo, si applica a tutte le organizzazioni che "controllano o possiedono dati personali di residenti nell'UE quando il trattamento è correlato all'offerta di beni e servizi", indipendentemente dal fatto che sia richiesto o meno un pagamento. In secondo luogo, il costo della non conformità per le organizzazioni è sostanziale: la sanzione pecuniaria può essere al massimo di 20 milioni di euro o del quattro per cento del fatturato annuo a livello mondiale, a seconda di quale sia il valore più alto. Il GDPR regola il trattamento dei dati personali dei residenti nell'UE. [25]

Esso regolamenta il trattamento dei dati personali, definiti all'articolo 4 come "qualsiasi informazione relativa a una persona fisica identificata o identificabile che può essere identificata, direttamente o indirettamente con riferimento a un identificatore". Gli identificatori elencati nell'articolo 4 comprendono nome, numero di identificazione, dati relativi all'ubicazione, nonché fattori culturali, mentali e fisici.

Per la Commissione Europea ("CE"), il GDPR è uno dei pilastri della priorità del Mercato Unico Digitale ("DSM") della CE, che trasformerà 28 mercati nazionali in un mercato unico destinato ad operare nell'era digitale. Il GDPR rinnova e armonizza la protezione dei dati in tutta l'UE. Il vantaggio per gli Stati membri è che non devono più gestire i propri statuti e regolamenti in

[25] Nissenbaum, H. (2010). Privacy in context: Technology, policy, and the integrity of social life. Stanford University Press.

materia di protezione dei dati. Il GDPR livella il campo di gioco per le organizzazioni che raccolgono informazioni personali. L'enfasi non è più sul fatto che un'azienda sia domiciliata nell'UE, ma sul fatto che le informazioni personali raccolte, archiviate e conservate siano o meno di dominio pubblico.

Il GDPR è composto da 11 capitoli, 99 articoli e 173 considerando. Il GDPR prevede una serie di requisiti fondamentali che le organizzazioni devono rispettare. Gli obblighi generali per i responsabili del trattamento dei dati sono elencati nell'articolo 24, mentre l'articolo 28 elenca le misure tecniche e organizzative per i responsabili del trattamento dei dati. Va notato che se le misure sono implementate in un'organizzazione che è conforme al GDPR, le multe applicate per la mancata conformità possono essere ridotte di gravità. Secondo l'articolo 6, il trattamento dei dati personali deve basarsi su almeno una base giuridica, tra cui il consenso, l'adempimento di un obbligo legale, l'esecuzione del contratto, la protezione degli interessi vitali dell'interessato e il legittimo interesse del titolare del trattamento. Se l'interessato revoca il consenso, il trattamento dei dati personali deve cessare. [26]

L'articolo 9, paragrafo 1, vieta il trattamento di informazioni personali che rivelino l'origine razziale o etnica, l'orientamento sessuale, i sentimenti politici, le convinzioni religiose, l'appartenenza a sindacati, o dati genetici o biometrici che possono essere utilizzati per identificare una persona. L'articolo 9, paragrafo 2, elenca dieci distinte esclusioni all'articolo 9, paragrafo 1, tra cui il consenso esplicito e il caso in cui l'interessato abbia accettato di rendere pubbliche le informazioni personali.

L'articolo 30 richiede che i responsabili e gli incaricati del trattamento dei dati personali conservino un registro delle proprie attività di trattamento. Secondo il GDPR, un'organizzazione deve comprendere le basi legali per il controllo e il trattamento dei dati personali. L'articolo 4, paragrafo 11, del GDPR stabilisce che il consenso deve essere esplicito e che è vietato l'utilizzo del consenso opt-out, una forma di consenso presunto.

Ai sensi dell'articolo 33, quando si verifica una violazione dei dati, le autorità preposte alla protezione dei dati devono essere informate entro 72 ore dal momento in cui si viene a conoscenza della violazione.

[26] Schwartz, P. M., & Solove, D. J. (2011). Privacy, information, and technology. Aspen Publishers

La notifica della violazione dei dati personali deve specificare la natura della violazione, il nome del responsabile della protezione dei dati, le probabili conseguenze della violazione e le azioni da intraprendere per mitigarne gli effetti negativi. L'articolo 34 prevede che, in caso di rischio elevato di violazione dei diritti e delle libertà individuali, anche gli interessati debbano essere avvisati; l'articolo 34, paragrafo 3, elenca le eccezioni a questo requisito aggiuntivo.

L'articolo 37 del GDPR prevede che le organizzazioni mantengano un responsabile della protezione dei dati, il cui compito è garantire che i dati personali siano sufficientemente protetti. Il responsabile della protezione dei dati deve essere libero di informare e consigliare i responsabili del trattamento, gli incaricati del trattamento e i dipendenti in merito alle loro responsabilità ai sensi del GDPR.[27]

## 3. Approccio americano al diritto alla privacy

Secondo il Merriam-Webster's Dictionary, la privacy è la "qualità o lo stato di essere separati dalla compagnia o dall'osservazione" o la "libertà da intrusioni non autorizzate". Il Black's Law Dictionary definisce la privacy come: "il diritto che determina il non intervento della sorveglianza segreta e la protezione delle informazioni di un individuo". Nel Black, la definizione è suddivisa in quattro parti. In primo luogo, vi è la privacy fisica che è: "un'imposizione che limita l'esperienza di un individuo o di una situazione da parte di un altro individuo". In secondo luogo, c'è la privacy illusoria, che è "l'imposizione di una restrizione esclusiva di un'entità". In terzo luogo, c'è la privacy informativa, che è "la prevenzione della ricerca di informazioni". Infine, c'è la privacy dispositiva che è: "la prevenzione dei tentativi fatti per conoscere lo stato mentale di un individuo ".

Nel caso Griswold, la Corte Suprema ha riconosciuto per la prima volta il diritto alla privacy. Il caso riguardava la consulenza alle coppie sposate in materia di contraccettivi, e se una coppia sposata avesse un diritto costituzionale alla privacy quando veniva consigliata sull'uso di contraccettivi. Prima di Griswold, nel 1890, Louis D. Brandeis, che in seguito divenne giudice della Corte Suprema, fu coautore con Samuel D. Warren di un articolo della Harvard Law

[27] Solove, D. J. (2011). Understanding privacy. Harvard University Press.

Review intitolato: The Right to Privacy. Nell'articolo, Warren e Brandeis definirono la privacy come "il diritto di essere lasciati in pace".[28]

La ragionevole aspettativa di privacy è un test legale utilizzato per decidere la portata del Quarto Emendamento. Non è la stessa cosa del diritto alla privacy. Il diritto alla privacy è un concetto più ampio che esiste nel sistema giuridico europeo. I due tipi di aspettative di privacy sono un'aspettativa oggettiva di privacy che può essere protetta dalla legge e un'aspettativa soggettiva di privacy che è l'opinione di una persona riguardo a una particolare circostanza. Ad esempio, un individuo ha una ragionevole aspettativa di privacy nei luoghi pubblici in cui la privacy è presunta. Questi luoghi comprendono le camere d'albergo, i bagni pubblici, le parti delle carceri o le cabine telefoniche pubbliche. Una notevole eccezione alla ragionevole aspettativa di privacy si verifica quando le forze dell'ordine effettuano una sorveglianza aerea.

Nella causa Olmstead, la Corte Suprema ha stabilito che le conversazioni telefoniche private possono essere intercettate senza un mandato. La Corte ha ritenuto che non vi fosse alcuna violazione dei diritti del Quarto Emendamento di Olmstead. In Katz, la Corte ha annullato Olmstead e ha esteso la protezione del Quarto Emendamento quando l'aspettativa è ragionevole. Nella sua opinione concorde, il giudice Harlan ha creato un criterio di ragionevole aspettativa di privacy per decidere quando un'azione governativa costituisce una perquisizione. Nella causa Miller, la Corte ha ritenuto che Miller non avesse alcun interesse ai sensi del Quarto Emendamento per quanto riguarda i suoi registri bancari perché non aveva una legittima aspettativa di privacy per quanto riguarda i suoi assegni e le sue ricevute di deposito, in quanto non si trattava di informazioni riservate. La Corte ha ritenuto che il governo potesse legittimamente ottenere queste informazioni.

Nella causa Smith, la Corte ha applicato il test del giudice Harlan quando il governo ha utilizzato un registratore per ottenere un numero di telefono. Non si trattava di una perquisizione ai sensi del Quarto Emendamento perché Smith non aveva una ragionevole aspettativa di privacy. In Kyllo, la Corte ha nuovamente utilizzato il test della ragionevole aspettativa di privacy quando ha ritenuto che l'uso di un dispositivo di imaging termico FLIR (Forward Lookin Infra-Red) costituisse una perquisizione perché l'uso del dispositivo violava la ragionevole aspettativa di

[28] Greenleaf, G. W., & Waters, N. (Eds.). (2014). Privacy in the digital era: 21st-century challenges to the Fourth Amendment. Edward Elgar Publishing.

privacy di Kyllo. Nella sua arringa a favore della maggioranza, il giudice Scalia ha affermato che l'ispezione di una casa con un'apparecchiatura altamente tecnica violava la ragionevole aspettativa di privacy di Kyllo.

In Jones, la Corte ha deciso che il governo ha violato la ragionevole aspettativa di privacy di Jones quando ha collegato un dispositivo di localizzazione GPS (Global Positioning System) alla sua auto. Come nel caso di Kyllo, il giudice Scalia ha osservato che un test di violazione della privacy non dovrebbe escludere un'argomentazione relativa alla ragionevole aspettativa di privacy. [29]

Il giudice Scalia non ha discusso le più ampie implicazioni sulla privacy che si sarebbero potute avere quando si raccolgono dati GPS senza mandato. Il giudice Sotomayor ha osservato che il test della ragionevole aspettativa di privacy è indipendente dal test di violazione di domicilio di common law. Il giudice Sotomayer ha chiesto se la sorveglianza GPS a breve termine fosse costituzionale osservando che una terza parte non necessariamente divulga tali dati. Knotts rispetto a Jones, fa una distinzione quando un individuo viene sorvegliato sette giorni su sette, 24 ore al giorno. Il giudice Alito ha osservato che il monitoraggio GPS a lungo termine viola la ragionevole aspettativa di privacy di un individuo, argomentando contro il test di violazione della privacy. Il giudice Alito ritiene che la sorveglianza a lungo termine possa fornire informazioni a breve termine sulle convinzioni e sui valori di una persona.

Nella causa Riley, la Corte ha stabilito che la perquisizione e il sequestro del contenuto di un telefono cellulare sono incostituzionali.

Il proprietario di un telefono cellulare ha una ragionevole aspettativa di privacy anche se viene arrestato. Il problema è che la perquisizione del contenuto del telefono cellulare è simile a un agente di polizia che fruga tra i documenti privati di una persona nell'ufficio o nell'armadietto senza un mandato, violando così la sua ragionevole aspettativa di privacy.

In Carpenter, la Corte ha stabilito che il governo ha violato i diritti del Quarto Emendamento di Carpenter ottenendo i metadati del telefono cellulare senza un mandato. Prima di Carpenter, il governo poteva ottenere i metadati dei telefoni cellulari semplicemente richiedendoli al provider,

[29] Bygrave, L. A. (2002). Data Protection Law: Approaching Its Rationale, Logic, and Limits. Kluwer Law International.

dichiarando che i dati erano necessari per un'indagine. La sentenza Carpenter non ha stabilito chi fosse il proprietario dei metadati.

I diritti di proprietà dell'utente del telefono cellulare non sono stati discussi nell'opinione di maggioranza, anche se i diritti di proprietà erano alla base della sentenza del Sesto Circuito. Nel dissenso del giudice Gorsuch, egli ha affermato che i metadati dei telefoni cellulari sono di proprietà dei proprietari dei telefoni cellulari, laddove i fornitori di telefoni cellulari sono i depositari. La sua obiezione è stata significativa perché ha rappresentato un passo avanti verso la possibilità per gli individui di controllare i dati che li riguardano.[30]

Il 28 giugno 2018, il governatore della California Jerry Brown ha firmato la legge SB-375 o California Consumer Privacy Act. La legislatura californiana ha approvato i primi emendamenti al CCPA il 31 agosto 2018 e il CCPA entra in vigore il 1° gennaio 2020, mentre l'applicazione della legge inizia il 1° luglio 2020.

Lo scopo della legge è quello di proteggere le informazioni personali dei consumatori californiani in modo analogo alla protezione garantita dal GDPR nella tutela delle informazioni personali degli individui nell'UE. Il CCPA regola la raccolta e l'elaborazione di informazioni personali che possono essere utilizzate per identificare o descrivere una persona o un nucleo familiare particolare. Per il CCPA, un consumatore è un residente della California domiciliato nello Stato, ma che può avere la residenza in un altro Stato. Il CCPA non tutela le informazioni personali di persone che si trovano in California per motivi temporanei o transitori. La legge interessa le imprese e le società di persone a scopo di lucro che raccolgono e gestiscono informazioni personali relative ai residenti in California nei casi in cui:

- Il fatturato annuo è superiore a 25 milioni di dollari;

- vengono ricevute o divulgate informazioni personali su almeno 50.000 residenti in California; oppure

- il 50% o più delle entrate annuali derivano dalla vendita di queste informazioni personali.

I residenti in California hanno il diritto di conoscere le categorie di informazioni personali raccolte, la fonte delle informazioni personali e se e quali organizzazioni stanno acquistando le

[30] Hildebrandt, M., & Gaakeer, J. (Eds.). (2013). In Search of 'European' Judicial Methodologies: A Comparative Perspective. Bloomsbury Publishing

loro informazioni personali. Gli individui hanno il diritto di rivedere le informazioni personali che vengono raccolte per assicurarsi che le informazioni raccolte siano corrette. Infine, i residenti in California hanno il diritto di richiedere la cancellazione delle proprie informazioni personali o, nei termini espressi nella causa Google contro Costeja González, la California riconosce ai propri cittadini il diritto all'oblio, fatte salve diverse eccezioni.[31]

Il CCPA contiene diverse disposizioni chiave. In primo luogo, i consumatori californiani hanno il diritto di rinunciare alla vendita delle loro informazioni personali. Questa disposizione deriva dal fatto che il CCPA riconosce che le informazioni personali sono una proprietà e quindi i residenti possono salvaguardare la loro privacy. Si tratta di una disposizione importante perché è coerente con i dissensi dei giudici Alito, Kennedy e Thomas nella causa Carpenter, in cui sostenevano che senza diritti di proprietà un individuo non ha una ragionevole aspettativa di privacy. La disposizione è anche coerente con il dissenso del giudice Gorsuch, in cui si ipotizzava che i fornitori di telefoni cellulari fossero depositari dei metadati dei telefoni cellulari a favore degli utenti. Va ricordato che il giudice Gorsuch presumeva che i metadati generati dal telefono cellulare degli utenti fossero di proprietà di questi ultimi e non dei provider.

In secondo luogo, le aziende coperte non possono addebitare ai residenti della California un prezzo più alto perché stanno esercitando i loro diritti ai sensi del CCPA. Questa disposizione è simile alla nozione di neutralità della rete, in base alla quale agli individui non possono essere addebitati prezzi diversi per l'utilizzo di Internet in base ai siti web che visitano. Questo requisito del CCPA è essenziale perché non consente alle aziende di penalizzare le persone che esercitano i loro diritti legali. In terzo luogo, le società di raccolta dati sono tenute a fornire ai consumatori californiani una copia dei loro dati in un formato elettronico facilmente trasferibile. Esistono eccezioni a questa disposizione, ma non sono irragionevoli. In quarto luogo, per le informazioni personali relative a persone di età inferiore ai 16 anni, le società di raccolta dati devono ottenere dai genitori o dai tutori legali l'autorizzazione alla vendita delle informazioni personali.

In quinto luogo, la trasparenza è una disposizione fondamentale del CCPA. Le politiche sulla privacy delle aziende coperte che operano in California sono tenute a rivelare annualmente al pubblico le categorie, i destinatari e le fonti di tutti i dati che le organizzazioni raccolgono,

[31] Schwartz, P. M. (2011). Privacy and democracy in Europe and the United States: Converging on regulation. Berkeley Technology Law Journal, 26(4), 1523-1566.

divulgano o vendono. Questa disposizione ha diverse ragioni, tra cui la capacità dello Stato della California di determinare l'efficacia del CCPA. In sesto luogo, sui siti web aziendali deve essere presente un link intitolato "Non vendere le mie informazioni personali" che consenta ai residenti in California di esercitare il diritto di non vendere le proprie informazioni personali. Questa decisione può essere riconsiderata solo una volta all'anno. Infine, le aziende sono tenute a specificare due metodi con cui i consumatori possono richiedere che l'azienda fornisca loro le proprie informazioni personali. Proprio come Equifax, Experian e TransUnion, a cui il Fair Credit Reporting Act ("FCRA") assegna 30 giorni per rispondere a una richiesta di credito o a un contenuto, le società di raccolta dati hanno 45 giorni per rispondere alla richiesta di un residente della California in merito alle proprie informazioni personali. In molti casi, il consumatore non deve sostenere alcun costo.

Il CCPA elenca due tipi di sanzioni per la mancata conformità. In primo luogo, sono previste sanzioni per le violazioni della sicurezza. Si tratta di una sanzione ragionevole, viste le massicce violazioni della sicurezza che le aziende hanno subito negli ultimi dieci anni. Il CCPA ha creato un'azione legale privata a disposizione dei residenti in California contro le aziende coperte quando le loro informazioni personali sono compromesse, a condizione che i dati non siano né crittografati né redatti. Il risarcimento è di 750 dollari per violazione o il danno effettivo, a seconda di quale sia il maggiore, e il Procuratore generale della California può far rispettare le disposizioni sulla privacy del CCPA attraverso l'uso di sanzioni civili con un massimo di 7.500 dollari per violazione.  È evidente che il CCPA ha i denti e può mordere e le aziende fanno bene a prendere sul serio la legge. Le violazioni possono essere sostanziali, soprattutto quando i singoli individui si aggregano e citano in giudizio le aziende tramite azioni collettive. Ad esempio, supponiamo che un'azienda subisca una violazione dei dati personali che coinvolga solo un milione di persone. La sanzione massima prevista da un'azione civile privata può essere al massimo di 750 milioni di dollari, una somma di denaro che la maggior parte delle organizzazioni non può permettersi di pagare. In questo esempio, anche il Procuratore generale della California potrebbe citare in giudizio le organizzazioni colpevoli. In questo caso, la multa massima sarebbe di 7,5 miliardi di dollari. Naturalmente, il numero di persone coinvolte in molte violazioni di dati e privacy supera di gran lunga il milione di individui. Le sanzioni massime per una violazione di dati di questo tipo sono apparentemente al di là della portata finanziaria della

maggior parte delle aziende Fortune 100. Questo è di per sé un motivo per prendere molto, molto sul serio il CCPA.

Table 1. *Serious Data Breaches in the United States from 2008 to 2018*

| American Company | Year | Individuals Affected |
|---|---|---|
| Adobe Systems, Inc. | 2013 | 152 million |
| Anthem, Inc. | 2015 | 80 million |
| Apple, Inc. / Blue Toad | 2012 | 12.3 million |
| Ebay, Inc. | 2014 | 145 million |
| Equifax, Inc. | 2017 | 143 million |
| Target Corp. | 2014 | 70 million |
| Uber Technologies, Inc. | 2017 | 57 million |
| Yahoo! | 2013 | 3 billion |

## 4. Confronto tra il gdpr e il ccpa

Per quanto riguarda la privacy, cosa ha l'America? In primo luogo, c'è la definizione di privacy data da Warren e Brandeis nel loro articolo della Harvard Law Review, che definisce la privacy come "il diritto di essere lasciati in pace".

In secondo luogo, gli Stati Uniti dispongono di un test di ragionevole aspettativa di privacy, come prescritto dal giudice Harlan in Griswold. In terzo luogo, esiste una pletora di casi della Corte Suprema che illustrano le modalità di applicazione del test di ragionevole aspettativa di privacy.[32]

Infine, l'America ha il Quarto Emendamento che stabilisce che le perquisizioni e i sequestri devono essere ragionevoli, il che significa che deve esistere una causa probabile, che un

[32] De Hert, P., & Gutwirth, S. (Eds.). (2009). Privacy and the Criminal Law. Springer.

magistrato neutrale deve emettere un mandato e che gli oggetti o le persone da perquisire o sequestrare devono essere descritti con particolarità. Il problema di tutti questi strumenti è che si basano sulla proprietà.

La privacy è un diritto del proprietario della proprietà. Nell'articolo di Warren e Brandies del 1890, la privacy viene discussa in relazione alla proprietà. Prima di Katz, la privacy era associata ai luoghi e non necessariamente alle persone. Dopo Katz, la privacy divenne un attributo della persona, e quali erano le ragionevoli aspettative di quell'individuo riguardo al fatto che le sue attività fossero o meno azioni private, come prescritto dal famoso test sulla privacy del giudice Harlan. Ad esempio, nel caso Katz, l'imputato si trovava in una cabina telefonica per telefonare.

Katz aveva una ragionevole aspettativa di privacy perché il luogo in cui stava telefonando era completamente chiuso. Era separato dal mondo esterno da tre pareti e due piccole porte a soffietto in un contenitore grande quanto una scatola di sardine.

Poi c'è il Quarto Emendamento che afferma che "il diritto del popolo di essere sicuro nelle sue persone, case, documenti ed effetti, contro perquisizioni e sequestri irragionevoli....".

Solo grazie al 13° Emendamento una persona fisica non può essere considerata una proprietà, a meno che la schiavitù o la servitù non siano una punizione per un crimine, nel qual caso la legge può considerare una persona fisica come una proprietà.

I principi della privacy, così come sono stati enunciati dall'Organizzazione per la Cooperazione e lo Sviluppo Economico, di cui gli Stati Uniti sono firmatari, sono molto importanti quando si cerca di comprendere i problemi della legge sulla privacy negli Stati Uniti. L'OCSE ha descritto in modo approfondito i principi che costituiscono la base della privacy individuale per quanto riguarda le informazioni personali. Si noti che la parola "economico" è contenuta nei nomi di entrambe le organizzazioni.[33]

In altre parole, implicitamente, la privacy in generale, e la privacy delle informazioni personali, è strettamente legata agli interessi economici e commerciali. È interessante notare che i principi della privacy attribuiti dagli Stati Uniti, così come sposati da Serwin et al. non hanno di fatto nulla a che fare con il guadagno economico.

[33] Hildebrandt, M., & Gaakeer, J. (Eds.). (2013). In Search of 'European' Judicial Methodologies: A Comparative Perspective. Bloomsbury Publishing.

Tuttavia, il problema è che gli Stati Uniti d'America sono intrinsecamente un'organizzazione governativa il cui scopo primario è quello di promuovere il commercio. Pertanto, anche se i principi sulla privacy non parlano esplicitamente di transazioni commerciali, in realtà ne sono inclusi.

Il Regolamento generale sulla protezione dei dati e il California Consumer Privacy Act presentano molte analogie e alcune differenze. Ad esempio, sia il GDPR che il CCPA definiscono in modo ampio i dati comparabili. Le definizioni comprendono quasi tutti i dati sulle persone, comprese le informazioni che si riferiscono implicitamente alle persone. Per contro, il CCPA riguarda le informazioni personali relative a individui e famiglie, mentre il GDPR riguarda solo le persone fisiche.

Il CCPA esclude le informazioni personali disponibili al pubblico, mentre il GDPR non prevede tale esclusione. Infine, il CCPA ritiene che le cronologie di ricerca siano dati personali a condizione che siano utilizzate per accertare l'identità di un individuo o di un nucleo familiare; tuttavia, il GDPR non si occupa delle cronologie di ricerca.

Con il GDPR, gli interessati hanno il diritto di sapere quali dati un'organizzazione possiede su un soggetto, le ragioni per cui i dati sono stati raccolti, le modalità di utilizzo dei dati al momento della raccolta o prima, i tipi di terze parti che hanno accesso alle informazioni personali e il periodo previsto di conservazione dei dati. Il CCPA prevede un diritto di accesso simile, in base al quale i consumatori sono autorizzati a conoscere le categorie di informazioni personali raccolte, la fonte delle informazioni personali, i terzi che hanno accesso alle informazioni e se un'organizzazione di raccolta dati vende o condivide le informazioni personali.[34]

Nella causa Costeja González, la Corte di giustizia dell'UE ha discusso in dettaglio il diritto all'oblio. Secondo la CGUE, una persona interessata può chiedere che un motore di ricerca su Internet cancelli le informazioni, a condizione che la cancellazione includa situazioni in cui i risultati della ricerca sono di fatto inadeguati, non più pertinenti o eccessivi dato il tempo trascorso. Il GDPR prevede un equilibrio tra il diritto alla privacy dell'individuo, le leggi sulla protezione dei dati dell'Unione Europea e il diritto del pubblico di sapere. Tuttavia, se l'interessato è un personaggio pubblico, l'equilibrio è a sfavore dell'interessato. Ai sensi del

[34] De Hert, P., & Gutwirth, S. (Eds.). (2009). Privacy and the Criminal Law. Springer.

CCPA, un consumatore ha un diritto simile all'oblio, che dipende dalla capacità di un'organizzazione di memorizzare le informazioni personali esclusivamente per uso interno.

Esiste anche il diritto di un individuo di insistere affinché un'organizzazione interrompa il trattamento dei suoi dati personali. Con il GDPR, la persona interessata ha il diritto di ritirare il consenso, costringendo un'entità ad astenersi dal trattare le informazioni personali, mentre con il CCPA, un cliente può rinunciare o impedire a un'azienda di vendere i suoi dati, ma non può evitare che i dati vengano raccolti.

Il diritto di notifica o il diritto di essere informati è parte integrante delle leggi americane e dell'Unione Europea. Con il GDPR, gli interessati vengono informati prima della raccolta dei dati personali e del loro utilizzo. Se i dati non vengono raccolti direttamente dall'interessato, l'ente è tenuto a fornire una notifica un mese prima della raccolta dei dati. In base al CCPA, invece, i consumatori possono conoscere le categorie di dati raccolti, la fonte delle informazioni personali, l'esistenza di eventuali terze parti e se l'organizzazione vende o condivide le informazioni personali. Poiché il diritto di notifica implica un processo decisionale, gli interessati ai sensi del GDPR hanno il diritto di richiedere che un essere umano prenda decisioni in merito all'uso e alla vendita di informazioni personali, mentre non esiste un diritto simile ai sensi del CCPA.[35]

In base al GDPR, gli interessati hanno il diritto alla portabilità dei dati, mentre il CCPA prevede un requisito simile entro limiti tecnicamente fattibili. Con il primo l'interessato ha il diritto di correggere le informazioni personali, a differenza del secondo che non prevede tale diritto. Il GDPR conferisce all'interessato il diritto intrinseco alla parità di servizi e di prezzo, mentre con il CCPA questo diritto è parte esplicita della legge.

Il regolamento europeo concede agli interessati il diritto di intentare un'azione legale contro un raccoglitore di dati senza limitazioni di responsabilità, mentre secondo quello californiano, come detto nel precedente paragrafo, la responsabilità è limitata da 100 a 750 dollari per individuo e per incidente. Le sanzioni previste dal GDPR sono sostanziali: la sanzione massima è di 20 milioni di euro o del quattro per cento del fatturato annuo globale, a seconda di quale sia il valore più alto.

[35] Cate, F. H., & Dempsey, J. X. (2011). Privacy in the Modern Age: The Search for Solutions. Brookings Institution Press.

Va notato che la conformità al GDPR non assicura che un'organizzazione sia conforme al CCPA e viceversa. Le due leggi hanno definizioni diverse e requisiti diversi per l'acquisizione e l'utilizzo delle informazioni personali. Il GDPR è stato approvato dal Parlamento europeo il 14 aprile 2016 ed è entrato in vigore il 25 maggio 2018. Il CCPA è stato firmato il 28 giugno 2018, entrerà in vigore il 1° gennaio 2020 e inizierà a essere applicato il 1° luglio 2020.[36]

La buona notizia per le aziende che operano in California è che al momento in cui scriviamo c'è tempo più che sufficiente per prepararsi all'attuazione della legge. Anche se non c'è alcuna garanzia che la legge cambi nel frattempo, ci saranno sicuramente emendamenti proposti da rappresentanti del settore, elettori e legislatori. Il procuratore generale della California probabilmente emanerà norme e regolamenti nei prossimi mesi, e si prevede che i tribunali interpreteranno la legge man mano che le controversie attraverseranno il sistema legale. In altre parole, il GDPR è attualmente solido, mentre nel bene o nel male il CCPA è malleabile.

Confrontando l'approccio europeo e quello americano alla privacy, la domanda che viene in mente è come un individuo vuole che il suo Paese protegga le informazioni personali. La risposta alla domanda dipende dal tipo di governo in carica.

L'individuo vuole un governo in cui i diritti individuali alla privacy siano esplicitamente sanciti e protetti in modo rigoroso? Desidera un governo in cui i diritti individuali alla privacy siano esplicitamente sanciti e protetti in modo rigoroso? Molte persone possono scegliere la seconda opzione piuttosto che la prima perché ritengono di non avere nulla da nascondere. Tuttavia, le persone che non hanno nulla da nascondere potrebbero non essere degne di fiducia perché attribuiscono poco valore alle proprie informazioni personali e a quelle degli altri.

Nell'UE la privacy è di primaria importanza, mentre negli Stati Uniti, prima dell'approvazione del CCPA, i cittadini americani avevano solo una ragionevole aspettativa di privacy. Va notato che c'è un oceano di differenza tra un diritto alla privacy e una ragionevole aspettativa di privacy. Il primo è un diritto con pari dignità rispetto ai diritti specificati nella Carta dei diritti. Il secondo è solo un'aspettativa, una speranza o una convinzione che la privacy esista.

[36] Bartolucci F., A., "Metodi statistici per l'inferenza causale," Pearson Italia, 2014, p .34.

# CAPITOLO III: *Il caso Facebook*

1. Facebook

Fondato nel 2004 con la missione di "dare alle persone il potere di condividere e rendere il mondo più aperto e connesso", Facebook ha, al 30 settembre 2014, 1,35 miliardi di utenti attivi mensili, con oltre l'82% degli utenti al di fuori di Stati Uniti e Canada. Rimane il servizio di social networking più popolare al mondo.

In Europa, è in testa al mercato in 17 Paesi su 25,204 e secondo uno studio condotto nel 2012, Facebook avrebbe aggiunto 15,3 miliardi di euro al mercato europeo. Rispetto a Twitter, un altro popolare SNS, ha cinque volte il numero di utenti attivi mensili e ha goduto di un fatturato più che decuplicato nel secondo trimestre del 2014, accumulando 2,91 miliardi di dollari di entrate. Tsaoussi ha individuato tre caratteristiche che conferiscono a Facebook la sua popolarità, ossia:

a) Gli utenti possono scambiarsi messaggi, comprese le notifiche automatiche quando aggiornano il loro profilo,[37]

(b) possono entrare a far parte di gruppi di utenti con interessi comuni (organizzati per luogo di lavoro, scuola o università, o altre caratteristiche, e

(c) costruire "applicazioni" che consentano agli utenti di personalizzare il proprio profilo e di svolgere altre attività.[38]

Oltre a queste configurazioni organizzative, si ritiene che anche le scelte rilevanti per la privacy nelle fasi iniziali abbiano dato a Facebook un vantaggio rispetto ai concorrenti. Ellison e Boyd, ad esempio, hanno suggerito che Facebook ha dato la possibilità agli utenti di decidere chi, nella loro rete, può visualizzare diversi aspetti dei loro profili, a differenza di LinkedIn, che controlla ciò che un utente può vedere a seconda del tipo di account, o di MySpace, che fornisce solo un'opzione "pubblica" o "solo per gli amici".

[37] Edwards, Lilian, Privacy and Data Protection Online: The Laws Don't Work ? in Lilian Edwards and Walden (eds) in L Edwards, C Waelde (ed) "Law and the Internet" (Third Edition, Oxford, Hart Publishing, 2009) pp.443-288
[38] Lener S.M., Percorsi per la protezione delle persone fisiche dalle inferenze create dall'intelligenza artificiale, Piccin nuova libreria, 2023.

In particolare, a differenza di altri SNS dell'epoca, Facebook "inizialmente non consentiva agli utenti di rendere i propri contenuti ampiamente accessibili".

La possibilità di controllare maggiormente la privacy è stata quindi un vantaggio per Facebook fin dall'inizio. Questo modello rimane al centro di Facebook anche oggi, ma funziona in modo complicato.

Quando gli utenti aprono un account Facebook, sono tenuti a fornire dati demografici come il nome, l'età, lo studio, il sesso, lo stato di parentela e così via. Inoltre, vengono invitati a fornire indirizzo, numero di telefono, occupazione, fotografie, luoghi di lavoro, luoghi in cui vivono, eventi della vita, interessi e altri dettagli. Dopo aver fornito i dati, agli utenti viene chiesto di accettare le condizioni d'uso di Facebook, che descrivono in dettaglio i rapporti tra Facebook e gli utenti, compreso il modo in cui Facebook utilizza i dati degli utenti. In questo modo, l'accumulo di numerosi dati personali inizia fin dall'inizio. [39]

Con il passare del tempo, Facebook ha introdotto molte funzioni e con esse un maggior numero di dati. Tra le altre, l'aggiornamento dello stato e la condivisione di foto/video che viene immediatamente inviata agli "amici" (la funzione News Feed); la visualizzazione cronologica della storia dell'attività di Facebook di un utente nelle sue "Mura" (la Timeline), la messaggistica privata, i "Mi piace" e gli "interessi" sono stati tutti fonte di immensi dati per la piattaforma. Come si evince dall'elenco di voci alla voce "Accesso ai dati di Facebook ", almeno 69 serie di dati sono archiviate da Facebook. [40]

Facebook, come molti altri SNS, è stato fondamentale per servire il pubblico in molti modi, sia per quanto riguarda l'istruzione, le relazioni sociali, la promozione e la creazione di imprese e l'aiuto nell'organizzazione di movimenti politici. Tuttavia, poiché i principali introiti di Facebook dipendono dai dati personali degli utenti, le preoccupazioni sulla privacy e, di fatto, gli incidenti sono numerosi. Data la sua portata e la crescente sofisticazione, è ragionevole pensare che le sue pratiche in materia di privacy abbiano un'implicazione considerevole, non solo per gli oltre un miliardo di utenti, ma anche per il sistema di regolamentazione dei SNS in generale.

[39] Efron B. and Tibshirani R. J., "An Introduction to the Bootstrap," Chapman & Hall, 1993, p .34.
[40] Bygrave Lee A, Data Privacy Law: An International Perspective, Oxford (Oxford university press) 2014

2. L'applicazione della direttiva a Facebook

Il RGPD agisce principalmente imponendo determinati obblighi ai responsabili del trattamento e fornendo i corrispondenti diritti agli interessati per la gestione dei loro dati personali, laddove il consenso è predominante.

Ai sensi dell'articolo 2, lettera d), del RGPD, il titolare del trattamento è colui che decide le finalità e i mezzi del trattamento. I SNS sono per definizione responsabili del trattamento, semplicemente perché sono loro che, principalmente attraverso l'impostazione e l'organizzazione dei loro servizi, decidono la finalità del trattamento, che di solito è "consentire agli utenti di impegnarsi nel social networking in modo che gli inserzionisti possano utilizzare le informazioni pubblicate sui profili degli utenti per indirizzare meglio i loro annunci".[41]

Come discusso in precedenza, Facebook si qualifica come responsabile del trattamento. L'altra condizione importante per l'applicazione della direttiva a Facebook è che quest'ultimo tratti dati personali, come discusso nel terzo capitolo. Come evidenziato in precedenza, sia il "trattamento" che i "dati personali" sono definiti in modo ampio. Inoltre, è chiaro che molti dei dati forniti dagli utenti di Facebook al momento dell'apertura di un account o attraverso i loro post e tag sono semplici dati personali e alcuni di essi possono essere considerati sensibili. Poiché Facebook opera con i dati degli utenti, anche attraverso la registrazione, l'archiviazione e il trasferimento a terzi, il trattamento dei dati personali è facilmente soddisfatto.

Tuttavia, il fatto che Facebook renda anonimi i dati personali quando li fornisce agli inserzionisti non può essere una difesa, almeno per tre motivi. In primo luogo, affinché l'anonimizzazione avvenga, Facebook deve disporre di dati personali acquisiti in base alle leggi sulla privacy. In secondo luogo, il processo stesso di anonimizzazione può essere benissimo considerato come un "ulteriore trattamento" e quindi richiede un consenso specifico o un altro motivo, come abbiamo visto. In terzo luogo, dati tutti i mezzi a disposizione di Facebook, è facile collegare i dati a una persona identificabile.

[41] Purtova Nadezhda, Property in Personal Data: Second Life of an Old Idea in the Age of Cloud Computing, Chain Information, and Ambient Intelligence in Serge Gutwirth, Yves Poullet, Paul De Hert and Ronald Leenes (eds) Computers, Privacy and Data Protection: an Element of Choice London (Springer) 2011

L'ultimo punto importante da considerare per stabilire l'applicabilità della direttiva a Facebook riguarda il suo campo di applicazione ai sensi dell'articolo 4. Di conseguenza, la direttiva disciplina il trattamento dei dati personali "effettuato nell'ambito delle attività dello stabilimento del responsabile del trattamento" negli Stati membri e il trattamento dei dati personali per i quali il responsabile del trattamento "si avvale di un dispositivo, automatizzato o meno, situato sul territorio". Probabilmente, le operazioni di Facebook, almeno per quanto riguarda gli utenti europei, rientrano nella direttiva per entrambi i criteri.

In relazione al primo criterio di cui all'art. 4 (a), la questione rilevante è se gli uffici di Facebook in Europa si qualifichino come "stabilimento" e se il trattamento dei dati personali provenienti dall'Europa avvenga, ovunque esso sia, nel contesto delle attività degli uffici. A questo proposito, Facebook non è stato aperto in relazione alle sue operazioni in Europa. Ad esempio, è stato riferito che "le informazioni sulla natura esatta delle attività degli uffici di Facebook situati in Europa e, soprattutto, se sono coinvolti nel trattamento dei dati sono molto difficili da ottenere". Facebook non risponde nemmeno alle domande individuali sulle sue operazioni. [42]

Tuttavia, per sua stessa ammissione, sembra che abbia delle sedi in Europa. Facebook ha aperto un ufficio a Londra nel 2007. Un anno dopo ha annunciato l'apertura di una sede internazionale a Dublino, in Irlanda. L'ufficio è descritto da Facebook come il centro delle operazioni internazionali e fornisce "una gamma di supporto tecnico, commerciale e operativo online agli utenti e ai clienti di Facebook in Europa, Medio Oriente e Africa".

Inoltre, la Dichiarazione è trattata come un accordo tra Facebook Ireland Limited e gli utenti di Facebook che risiedono al di fuori degli Stati Uniti e del Canada, il che indica che l'ufficio di Dublino opera come un'entità indipendente. Data l'ampia interpretazione di "stabilimento", questo è un chiaro caso in cui Facebook Ireland rientra nel suo ambito. Di conseguenza, il trattamento dei dati personali provenienti dall'Europa, effettuato in relazione alle attività dell'ufficio di Dublino, tra gli altri, sarebbe soggetto alla Direttiva.

Detto questo, nella sua recente modifica dell'Informativa sull'utilizzo dei dati, Facebook ha chiarito che Facebook Ireland Limited è stata costituita e registrata in Irlanda come società a responsabilità limitata ed è il responsabile del trattamento dei dati personali di persone al di fuori

[42] Custers and et al, *Informed Consent in Social Media Use – The Gaps between User Expectations and EU Personal Data Protection Law*, Scripted Vol. 10, Issue 4 (2013)

degli Stati Uniti e del Canada. Pertanto, l'articolo 4, paragrafo 1, lettera c), della Direttiva non sarebbe appropriato per il nostro caso, poiché riguarda uno scenario in cui il responsabile del trattamento non è stabilito nell'UE.[43]

3. Facebook Basics e alcuni problemi di privacy

Lilian Edwards ci consiglia che un modo per comprendere i problemi di protezione dei dati nei SNS è quello di vedere le loro fonti di guadagno e i loro modelli di business.Gli scrittori Enders et al. hanno classificato i modelli di guadagno dei SNS in tre categorie principali, ovvero pubblicità, abbonamento e transazione. La pubblicità, a sua volta, può assumere due forme: i modelli di affiliazione e i banner pubblicitari. Nel primo modello, un SNS indirizza il traffico verso un sito web affiliato e si fa pagare per il rinvio, mentre nel secondo la pubblicità viene visualizzata sul SNS. Facebook si affida principalmente alla pubblicità come principale fonte di guadagno. Ad esempio, nella sua dichiarazione del 18 giugno 2013, Facebook ha dichiarato di avere oltre 1 milione di inserzionisti attivi. I marketer e gli inserzionisti selezionano il pubblico target e Facebook, utilizzando la sua sofisticata tecnologia di mining e gli immensi dati personali degli utenti, fornisce il gruppo mirato.

È proprio qui che l'estensione e la qualità/accuratezza dei dati personali diventano cruciali per Facebook, poiché il pagamento da parte degli inserzionisti dipende, di solito, dal numero di clic, che a sua volta dipende dall'accuratezza della selezione. Come ha affermato nel 2009 l'allora commissario europeo Meglena Kuneva, i dati personali sono, come per Facebook, il "nuovo petrolio di Internet e la nuova moneta del mondo digitale". Per questo motivo, i problemi di privacy legati alle operazioni di Facebook riguardano principalmente il modo in cui Facebook acquisisce i numerosi dati personali che tratta e il modo in cui li tratta in seguito.

Molti incidenti hanno portato i problemi di privacy di Facebook sotto i riflettori e hanno assunto dimensioni diverse. Anche le conseguenze delle violazioni della privacy variano dal semplice disagio e dalle sorprese all'imbarazzo e alla frustrazione; dai danni alla reputazione al furto di

[43] Kokott Juliane and Christoph Sobotta, The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR, International Data Privacy Law, Vol. 3, No.4, 2013.

identità; dalla perdita del lavoro e dai provvedimenti disciplinari a scuola ai suicidi. Ovviamente, alcune funzioni del servizio violano i principi di protezione dei dati più di altre. Di seguito sono riportati alcuni dei servizi di Facebook che hanno suscitato controversie in materia di privacy.

4. Dichiarazione dei diritti e delle responsabilità e Informativa sull'utilizzo dei dati di Facebook

Come si legge nell'incipit dell'Informativa, "utilizzando o accedendo a Facebook" gli utenti accettano l'Informativa, come aggiornata di volta in volta in conformità alla Sezione 14". A completamento di ciò, l'art. 14(3) recita: "l'uso continuato di Facebook a seguito di modifiche alle nostre condizioni costituisce l'accettazione delle nostre condizioni modificate", conferendo così a Facebook un'importante leva. Le modifiche possono essere pubblicate sulla "Pagina di governance del sito di Facebook", che conta solo circa tre milioni di follower. In molti casi, Facebook invia un avviso agli utenti, come nella schermata riportata di seguito. [44]

La Dichiarazione regola il rapporto tra Facebook e gli utenti, gli sviluppatori di applicazioni, gli amministratori di pagine, gli inserzionisti e i siti che utilizzano i plug-in di Facebook. Essendo la maggior parte della Dichiarazione di responsabilità delle altre parti, le questioni relative alla privacy degli utenti sono disciplinate all'inizio, anche se non completamente. Così, la sezione 1 invita gli utenti a leggere la "politica di utilizzo dei dati" relativa alle modalità di raccolta e utilizzo dei dati personali da parte di Facebook, mentre la sezione 2(4) informa o avverte gli utenti sugli effetti della pubblicazione di contenuti come "pubblici".

Secondo l'informativa sull'uso dei dati, le fonti di informazioni che Facebook raccoglie includono le informazioni richieste per la registrazione, le informazioni condivise dagli utenti come pubbliche e tramite le aggiunte degli amici, i "mi piace" alle pagine o ai siti web, e alcuni dati che sono considerati pubblici per definizione, ossia nome, immagini del profilo, foto di copertina, sesso, reti, nome utente e ID utente.

[44] Moerel (2011a) Lokke. The Long arm of EU data protection Law: Does the Data protection directive apply to processing of personal data of EU citizens by websites worldwide? In: International Data Privacy Law. Vol. 1. No. 1 (2011)

Vengono fornite alcune ragioni per cui questi dati vengono trattati come tali, ma solo alla fine. Le altre fonti di dati sono gli amici degli utenti, l'ultima fonte, presentata in un paragrafo condensato e mal strutturato, include informazioni provenienti da: gestione di Facebook (messaggi, sguardo alla timeline degli altri), "dati sull'ora e sulla posizione dei post; visite a giochi e siti con piattaforma Facebook e plug in, e da siti pubblicitari e affiliati". È inoltre previsto in modo vago che possano essere raccolti anche da "click su, visualizzazione o altra interazione con cose (enfasi aggiunta)".

Per quanto riguarda gli scopi per cui Facebook utilizza i dati degli utenti, fornisce sia una descrizione generale che alcuni casi di utilizzo dei dati degli utenti. I dati possono essere utilizzati "in relazione ai servizi e alle funzionalità che forniamo a voi e ad altri utenti come i vostri amici, ai nostri partner, agli inserzionisti che acquistano annunci sul sito e agli sviluppatori che creano i giochi, le applicazioni e i siti web che utilizzate".

Tra gli scopi particolari menzionati, vi sono: aiutare le persone a vedere e trovare le cose che fate e condividete, mantenere Facebook sicuro e protetto; proteggere i diritti di Facebook e di altri, misurare o comprendere l'efficacia degli annunci pubblicitari e distribuirli; per operazioni interne, tra cui risoluzione dei problemi, analisi dei dati, test, ricerca e miglioramento del servizio.[45]

La condivisione con altri è prevista anche indirettamente con alcune condizioni, ad esempio "informando l'utente in questa informativa". Inoltre, verso la fine, è previsto che Facebook possa "consentire ai fornitori di servizi di accedere alle informazioni in modo che possano aiutarci a fornire servizi". È molto importante notare che le "informazioni" sono definite in modo molto ampio e circolare dalla Dichiarazione come fatti o altre informazioni sull'utente, comprese le azioni intraprese dagli utenti e dai non utenti che interagiscono con Facebook (art. 18(3)).

Per quanto riguarda la durata, Facebook conserva i dati "per tutto il tempo necessario a fornire prodotti e servizi a voi e ad altri". La presentazione della dichiarazione e dell'informativa sull'uso dei dati è corretta, tranne che per alcune parti. Tuttavia, trovare i termini e l'informativa sull'uso dei dati è un po' complicato. Ad esempio, non si può semplicemente dare un'occhiata alla pagina della timeline.

---

[45] Romano Fabio Balducci, *The Right to the Protection of Personal Data: a New Fundamental Right of the European Union*, (2013) Electronic copy available at: http://ssrn.com/abstract=2330307

La legge sulla protezione dei dati è un'area emergente del diritto che mira a salvaguardare i dati personali degli individui dall'accesso e dall'uso eccessivo e ingiustificato. Originariamente introdotta come mezzo per limitare la sorveglianza governativa, ha trovato una maggiore rilevanza con l'aumento della capacità di calcolo dei moderni strumenti tecnologici, tra cui i principali sono il computer e Internet. Più recentemente, l'emergere dei servizi di social network ha reso la protezione dei dati molto importante e al tempo stesso complicata. [46]

In Europa sono state adottate diverse leggi in materia. Le leggi in materia rivelano che i dati personali sono protetti sia per una questione di diritti umani che per finalità economiche. In relazione al secondo scopo, la crescente importanza dei dati personali nei servizi basati su Internet coincide con la creazione di un mercato unico in Europa. La direttiva del 1995, quindi, ha lo scopo di garantire la protezione dei dati personali dei cittadini europei e si preoccupa di assicurare un flusso di dati senza ostacoli all'interno dell'Unione. [47]

L'ampio campo di applicazione materiale della direttiva significa che si applica ai responsabili del trattamento stabiliti in Europa, a quelli extraeuropei, ma che hanno uno stabilimento in Europa in relazione al quale avviene il trattamento, e a quelli che non hanno uno stabilimento nell'UE, ma che utilizzano alcune apparecchiature in Europa per acquisire i dati.

La direttiva funziona principalmente imponendo determinati requisiti, sotto forma di principi di protezione dei dati, ai responsabili del trattamento e pone gli interessati all'altro capo dell'equazione con determinati diritti in relazione al trattamento dei dati che li identificano, anche indirettamente. Pertanto, affinché un responsabile del trattamento possa giustificare un'elaborazione di dati personali, è necessario che vi sia una o più basi solide stabilite dalla legge; il consenso degli interessati è una delle giustificazioni ed è spesso utilizzato. Esistono anche altri principi relativi ai dati per mitigare il trattamento eccessivo.

Per quanto sia importante che le persone possano avere un'opinione decisiva sui dati che le identificano attraverso il consenso, questo sistema ha dimostrato di soffrire di alcuni limiti. Tra l'altro, è difficile capire se c'è davvero un consenso con tutte le sue caratteristiche e questo può essere manipolato dai responsabili del trattamento. Questo vale in particolare per i popolari siti di

---

[46] Romano Fabio Balducci, *The Right to the Protection of Personal Data: a New Fundamental Right of the European Union*, (2013) Electronic copy available at: http://ssrn.com/abstract=2330307

[47] Lener S.M., Percorsi per la protezione delle persone fisiche dalle inferenze create dall'intelligenza artificiale, Piccin nuova libreria, 2023.

social network che raccolgono immensi dati dai loro utenti. Al fine di mitigare tali problemi, la Direttiva richiede che il consenso sia specifico per un determinato scopo, informato e dato liberamente. Inoltre, richiede che l'indicazione del consenso sia data in modo chiaro, senza lasciare dubbi, come requisito di validità.

Facebook, uno dei principali servizi di social network, si basa principalmente sui dati personali degli utenti. Gli utenti danno il loro consenso durante la registrazione e i termini a cui acconsentono dettano anche le modifiche future. Alcune funzioni di Facebook non soddisfano manifestamente i requisiti della direttiva. Il fatto che non consenta agli utenti di esprimere separatamente il proprio consenso per scopi diversi; il trattamento dell'"uso continuato" come consenso; il trattamento simile dei dati a prescindere dalla loro sensibilità. Il fatto che non consenta agli utenti di dare il consenso separatamente per scopi diversi, il trattamento dell'"uso continuato" come consenso, il trattamento simile dei dati indipendentemente dalla sensibilità, i termini facilmente inaccessibili e la modifica delle impostazioni predefinite che lasciano "pubblici" dati personali importanti e il rapporto complicato con i partner di terze parti sono alcuni degli aspetti che suscitano disagio quando vengono valutati rispetto ai requisiti di consenso della direttiva. Per questo motivo, è necessario che Facebook e le autorità di regolamentazione tengano in debita considerazione questi aspetti, oltre a una maggiore assertività e consapevolezza da parte degli utenti.

Con un nuovo regime legale con un campo di applicazione più ampio, regole dettagliate, una soglia di consenso più alta e meccanismi di applicazione più efficaci, si prevede che il consenso degli utenti sarà utilizzato in modo da proteggerli meglio.

## *BIBLIOGRAFIA*


Alibrandi S., Il diritto alla privacy nell'era digitale, Aracne Editrice, 2021.

Balducci R. F., The Right to the Protection of Personal Data: a New Fundamental Right of the European Union, 2013.

Bartolucci F., A., "Metodi statistici per l'inferenza causale," Pearson Italia, 2014.

Bergkamp L., EU Data Protection Policy: The Privacy Fallacy: Adverse Effects of Europe's Data Protection Policy in an Information-Driven Economy, Computer Law and Security Report, Vol.18, No.1, 2002.

Bygrave, L. The Place of Privacy in Data Protection, Computer Law & Security Report, Vol.17, 2001.

Bygrave L., Privacy and Data Protection in an International Perspective. In: Scandinavian Studies in Law Vol. 56, 2010.

Bygrave Lee A, Data Privacy Law: An International Perspective, Oxford (Oxford university press) 2014

Capobianco A.- Mignani S., "Metodi Statistici per le Decisioni," McGraw-Hill Education, 2017.

Cassano G., I diritti dell'era digitale, Giuffrè, 2020.

Cate, F. H., & Dempsey, J. X., Privacy in the Modern Age: The Search for Solutions. Brookings Institution Press, 2011.

Clarke, R. Internet privacy concerns confirm the case for intervention. Communications of the ACM, 42(2), 1999.

Clayton, R., Gellman, R., & Jochai, C., Model Privacy Notice Project: Building a user-centric privacy notice. In 26th USENIX Security Symposium, 2017.

Colussi I., Synthetic biology and the freedom of scientific research: a fundamental freedom in front of a new emerging technology, in Law and the Human Genome Review, Special Issue, 2014.

Cuffaro V., I dati personali del Diritto europeo, Giappichelli, 2019.

Culnan M.J., 'Protecting Privacy online: Is self-regulation working?' Journal of Public Policy Market, Vol. 19, 2000.

Daniel B. and et al, Data Protection: The Challenges Facing Social Networking, 6 Internet Law & Management review Vol. 6, 2010.

De Hert, P., & Gutwirth, S., Privacy and the Criminal Law. Springer, 2009.

Ellison D. N., Social Network Sites: Definition, History, and Scholarship' Journal of Computer-Mediated Communication, Vol. 13, 2007.

De Minico G., Tecnica e diritti sociali nella regulation della banda larga, in G. De Minico (a cura di), Dalla tecnologia ai diritti, Napoli, Jovene, 2010.

Efron B. and Tibshirani R. J., "An Introduction to the Bootstrap," Chapman & Hall, 1993.

Freedman D., "Statistics," Fourth Edition, W.W. Norton & Company, 2007.

Fuster G. G., The Emergence of Personal Data Protection as a Fundamental Right of the EU, New York, 2014.

Ferrari G. F., La tutela della privacy, Giappichelli Editore, 2021.

Gelman A., Carlin J. B., Stern H. S., Dunson D. B., Vehtari A., and D. Rubin B., "Bayesian Data Analysis," Third Edition, CRC Press, 2013.

Greenleaf, G. W., Privacy in the digital era: 21st-century challenges to the Fourth Amendment. Edward Elgar Publishing, 2014.

Hildebrandt, M., & Gaakeer, J., In Search of 'European' Judicial Methodologies: A Comparative Perspective. Bloomsbury Publishing, 2013.

Jaynes E. T., "Probability Theory: The Logic of Science," Cambridge University Press, 2003.

Kokott J. And Sobotta C., The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR, International Data Privacy Law, Vol. 3, No.4, 2013.

Lilian E., Privacy and Data Protection Online: The Laws Don't Work? in Lilian Edwards and Walden (eds) in L Edwards, C Waelde (ed) "Law and the Internet", Third Edition, Oxford, Hart Publishing, 2009.

Lener S.M., Percorsi per la protezione delle persone fisiche dalle inferenze create dall'intelligenza artificiale, Piccin nuova libreria, 2023.

Mantelero A., Diritto alla privacy e protezione dei dati personali nell'era digitale, Giappichelli Editore, 2017.

Marozzi M., "Inferenza statistica," Esculapio, 2013.

Moerel L., The Long arm of EU data protection Law: Does the Data protection directive apply to processing of personal data of EU citizens by websites worldwide? In: International Data Privacy Law. Vol. 1. No. 1, 2011.

Negri D., Diritto alla privacy e protezione dei dati personali, Giuffrè Editore, 2020.

Perri P., Il diritto alla riservatezza, Giuffrè Editore, 2019, p. 367.

Nissenbaum, H., Privacy in context: Technology, policy, and the integrity of social life. Stanford University Press, 2010.

Pizzetti F., La tutela della privacy nella società dell'informazione, Laterza, 2018.

Pizzetti F., Privacy e Diritto europeo alla protezione dei dati personali, Giappichelli, 2016.
Priora G., Privacy e diritto all'oblio: profili civilistici, Maggioli Editore, 2019.

Purtova N., Property in Personal Data: Second Life of an Old Idea in the Age of Cloud Computing, Chain Information, and Ambient Intelligence in Serge Gutwirth, Yves Poullet, Paul De Hert and Ronald Leenes (eds) Computers, Privacy and Data Protection: an Element of Choice London (Springer) 2011.

Reidenberg, J. R.  American and European privacy: The past, present, and future of the debate. Journal of Comparative Law, 2013.

Schwartz, P. M., Privacy and democracy in Europe and the United States: Converging on regulation. Berkeley Technology Law Journal, 26(4), 2013.

Schwartz, P. M., & Solove, D. J., Privacy, information, and technology. Aspen Publishers, 2011.

Sivia D. S., "Data Analysis: A Bayesian Tutorial," Second Edition, Oxford University Press, 2006.

Solove, D. J., Understanding privacy. Harvard University Press, 2011.

Timiani M., Come la privacy può rimodellare le prerogative dei consiglieri regionali, in Quaderni Costituzionali, 2, 2014.

Ziccardi G., Cybercrime, identità digitale e diritto alla privacy, Giappichelli, 2020.

Ziccardi G., Privacy, big data e internet delle cose, Giappichelli Editore, 2018.