UNIVERSITÀ DEGLI STUDI DI PADOVA

Dipartimento di
Diritto Pubblico, Internazionale e Comunitario

Corso di laurea in Diritto e Tecnologia

L'importanza della trasparenza nella disciplina privacy dei siti web: i casi Facebook e ChatGPT

Relatore
Prof. Filippo Viglione

Laureanda: MILENA BORTOLI
Matricola:2043268

Anno Accademico: 2023/2024

Sommario

INTRODUZIONE

La protezione dei dati personali è ormai uno dei principali argomenti, e preoccupazioni, dell'era digitale, che tra le caratteristiche principali ha le continue interazioni online che comportano la raccolta e l'elaborazione dei dati personali e delle informazioni degli utenti del web. La crescente digitalizzazione ha fatto diventare questi dati personali una risorsa fondamentale per le aziende, sia a livello economico che a livello competitivo, ma ha anche aumentato i rischi legati alla loro gestione illegittima.

In questo contesto di rischi online e attacchi informatici sempre più diffusi, la trasparenza nelle informazioni riguardanti il trattamento e la diffusione dei propri dati personali, assume un'importanza fondamentale, poiché consente agli utenti dei servizi nel web di comprendere come e perché le loro informazioni personali vengono raccolte, utilizzate e conservate.
Le informative sulla privacy, chiamate anche “privacy policy”, che i siti web sono obbligati a fornire secondo il Regolamento (UE) 2016/679, al giorno d’oggi dovrebbero rappresentare uno degli strumenti principali di garanzia per ottenere questo livello di consapevolezza. Tuttavia, spesso queste informative sono scritte in modo complesso, poco comprensibile o addirittura lacunoso o errato, rendendo difficile per gli utenti prendere decisioni informate per il consenso sulla gestione dei propri dati, come previsto dal Regolamento sulla protezione dei dati. In questo scenario, la trasparenza non è solo un principio etico sancito dal GDPR, ma una necessità legale che le aziende devono gestire con particolare diligenza, per evitare il rischio di sanzioni pecuniarie e amministrative o altre misure punitive.

In merito a quanto appena esposto, in questo testo, verrà analizzato come la mancanza di completezza e chiarezza nelle privacy policy può comportare conseguenze legali gravose per le aziende, con sanzioni significative da parte degli Istituti di controllo competenti, come il Garante per la protezione dei dati

personali o l'Autorità Garante della Concorrenza e del Mercato (AGCM). Più precisamente queste conseguenze verranno analizzate nei capitoli 2 e 3 del seguente elaborato, attraverso il commento dei casi Facebook VS AGCM e il “caso” ChatGPT VS il Garante per la Protezione dei dati Italiano.

Per garantire un’analisi della materia completa, verrà inoltre commentata la normativa statunitense in materia privacy, sia quella attuale dei vari stati degli USA, che il nuovissimo “American Privacy Rights Act”. In particolare si approfondiranno i possibili cambiamenti che porterà nel quadro normativo statunitense e verrà eseguita una sua comparazione con il Regolamento per la Protezione dei dati personali europeo.

CAPITOLO I

Introduzione ai concetti e riferimenti normativi in materia privacy UE e USA.

1.1 Introduzione al GDPR:

Il protagonista principale a livello europeo sulla normativa privacy è sicuramente il Regolamento n. 2016/679[1], cioè il Regolamento generale sulla protezione dei dati (General Data Protection Regulation) del Parlamento Europeo del 27 aprile 2016, la cui applicazione decorre dal 25 maggio 2018.

Il legislatore europeo ha voluto, e dovuto, adottare questo regolamento per unificare il quadro normativo in materia di tutela e libera circolazione dei dati personali all'interno dell'Unione Europea.

Prima della venuta del GDPR, la Direttiva 95/46/CE[2] era il principale strumento normativo a tutela delle persone fisiche in materia di trattamento dei dati; una normativa che garantiva un livello elevato e uniforme di tutela dei diritti e delle libertà fondamentali del cittadino europeo. Questa direttiva ha inoltre avuto un ruolo fondamentale per gli scambi commerciali, perché ha consentito l'abbattimento delle frontiere interne europee e ha contribuito alla realizzazione del “free flow of data”, parte della strategia per la creazione del Digital Single Market.[3]

Intorno al 2016, però, è sorta la necessità di emanare un nuovo regolamento in materia di data protection. Le motivazioni erano diverse, ma principalmente la tutela fornita dalla direttiva del 1995 non era aggiornata rispetto alle nuove tecnologie, in quanto nei successivi vent'anni dalla sua pubblicazione, ci sono stati degli sviluppi fondamentali in ambito tecnologico.

---

[1] Di seguito chiamato “GDPR” o “Regolamento”.

[2] Direttiva 95/46/CE “tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati”

[3] Nicola Fabiano (2019) GDPR & privacy: consapevolezza e opportunità. Analisi ragionata della protezione dei dati personali tra etica e cybersecurity; Editore: goWare. (Prefazione di Giovanni Buttarelli)

Il GDPR riprenderà poi gran parte dei principi previsti dalla vecchia direttiva, rafforzando e rendendo più efficace tutto ciò che riguarda il trattamento dei dati personali, nonché le norme relative alla circolazione di tali dati[4].

In questa introduzione alla normativa del GDPR, tratteremo i primi due capi del regolamento, che trattano rispettivamente le disposizioni generali e i principi.

1.2 Disposizioni generali:

L'articolo 2 del regolamento riguarda il suo ambito di applicazione materiale, specificando, quindi, quando e come deve essere applicato. In particolare, stabilisce che il GDPR si applica al trattamento di dati personali[5] effettuato, totalmente o parzialmente, con mezzi automatizzati e a trattamenti non automatizzati di dati personali che fanno parte, o sono destinati ad essere contenuti in un archivio. Questo articolo è molto importante, perché, introducendo l'obiettivo di includere il più ampio spettro possibile di trattamenti dei dati personali, rimarca la volontà del legislatore di garantire che la protezione di quest'ultimi sia applicata indipendentemente dal formato o dal metodo del loro trattamento. È altresì doveroso specificare le eccezioni sull'applicazione del regolamento indicato dall'articolo 2, comma 2: le principali riguardano il trattamento di dati da parte di singoli individui per attività esclusivamente personali o domestiche[6], oppure da parte di autorità competenti per attività legate alla sicurezza nazionale.

Per quanto riguarda l'ambito di applicazione territoriale del regolamento, all'articolo 3 si definisce che esso non si applica solamente alle organizzazioni con sede nell'Unione Europea, ma anche a quelle situate al di fuori, che trattano

[4] Articolo 1 GDPR - oggetto e finalità

[5] Art 4 GDPR: "«dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;"

[6] Chiamato anche "household exemption".

dati personali delle persone appartenenti alla comunità europea, rendendolo un regolamento con portata extraterritoriale.

L'articolo 4 del GDPR ci fornisce una serie di definizioni fondamentali per poter effettuare una corretta interpretazione e applicazione del regolamento. Tra i termini principali definiti da questo articolo abbiamo il "*Titolare del trattamento*" (data processor) che viene inteso come una persona fisica o giuridica, una pubblica autorità o un diverso organismo, che, in autonomia oppure cooperando con altri, individua le finalità e i mezzi del trattamento dei dati personali e ne è responsabile[7]. Il titolare può delegare a un "*responsabile del trattamento*"[8] la possibilità di trattare i dati personali per proprio conto. Altra definizione importante data dall'articolo 4 è quella del termine "*consenso*"[9], descritto come qualsiasi manifestazione di volontà libera, specifica e informata, con la quale l'interessato accetta che i propri dati personali siano oggetto di trattamento.

1.2.1 I principi del gdpr:

Nei primi articoli del regolamento, più precisamente all'articolo 5, sono esposti i principi fondamentali che costituiscono la base di tutte le normative proposte e che perseguono l'obiettivo centrale del GDPR: la protezione delle persone fisiche nel trattamento dei loro dati. Di seguito analizzeremo nel dettaglio questi principi.

Il primo comma dell'articolo 5 asserisce che "i dati devono essere trattati in modo lecito, corretto e trasparente". Per quanto riguarda il concetto di liceità del trattamento, quest'ultimo deve essere legittimo[10] e espressione di una delle condizioni previste dall'articolo 6 del GDPR[11]. Con il termine correttezza si intende invece il divieto di acquisizione e utilizzo dei dati in modo scorretto e ingannevole, vietando inoltre l'abuso di potere della posizione del titolare e del responsabile del trattamento. Il principio della trasparenza è una delle grandi

[7] Regolamento (UE) 2016/679, Art. 4, comma 7.
[8] Regolamento (UE) 2016/679, Art. 4, comma 8.
[9] Regolamento (UE) 2016/679, Art. 4, comma 11.
[10] Legittimo: "che è secondo la legge, che ha le condizioni richieste dalla legge, e perciò valido, regolare [...]". Treccani.it/vocabolario
[11] Articolo 6 GDPR: Liceità del trattamento.

novità rispetto alla Direttiva del ‘95. Con questo principio è rivoluzionato il modo con cui le organizzazioni procedono con la raccolta, la gestione, e, in generale, tutto il processo di trattamento dei dati, in quanto ora sono obbligate a dare un'informativa precisa sui loro metodi, portando alla creazione di “privacy policy” che devono essere “funzionali alla formazione ed espressione di un consenso al trattamento autenticamente libero e consapevole, nonché all’eventuale esercizio di tutti i diritti dell’interessato” [12].

In questa informativa, divenuta fondamentale per un trattamento legittimo dei dati, deve essere inserita anche la rappresentazione di ciò che viene espresso negli altri principi del GDPR, tra cui, di fondamentale importanza, è la “limitazione della finalità del trattamento” che impone una restrizione sulla raccolta e sull’utilizzo dei dati personali che deve avvenire solamente per le finalità previste. Ad esempio, i dati raccolti per scopi contabili non possono essere utilizzati per finalità di marketing, a meno che non sia stato dato il consenso specifico per quella tipologia di trattamento[13]. A questo principio è strettamente collegato quello sulla “minimizzazione dei dati”: sempre secondo l’articolo 5 del regolamento, i dati raccolti devono essere “adeguati, pertinenti e limitati” al raggiungimento delle finalità per cui vengono trattati. Questo stabilisce il divieto di raccogliere più dati di quanto sia effettivamente necessario per il trattamento, una regola che purtroppo viene spesso ignorata. È diventata abitudine di varie organizzazioni e siti web di chiedere dati, come ad esempio il sesso o l’età, che spesso vengono utilizzati per fini statistici e di marketing, ma che non sono espressamente necessari per la pura finalità dell’utilizzo del

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

[13] Considerando 32, GDPR: “Il consenso dovrebbe essere espresso mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano, ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale. Ciò potrebbe comprendere la selezione di un'apposita casella in un sito web, la scelta di impostazioni tecniche per servizi della società dell'informazione [...] Il consenso dovrebbe applicarsi a tutte le attività di trattamento svolte per la stessa o le stesse finalità. Qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per tutte queste. Se il consenso dell'interessato è richiesto attraverso mezzi elettronici, la richiesta deve essere chiara, concisa e non interferire immotivatamente con il servizio per il quale il consenso è espresso.”

prodotto o servizio offerto, senza richiedere il consenso specifico o inserendolo in modi ingannevoli.
Altri fondamenti del Regolamento sono: l'esattezza dei dati trattati (che prevede anche un loro aggiornamento se necessario), la loro “integrità” e la loro riservatezza, per cui deve essere garantita una adeguata sicurezza, inclusa la protezione contro il trattamento non autorizzato o illecito, la perdita, la distruzione o il danno accidentale, tramite l'uso di misure tecniche e organizzative appropriate.[14]

L'Unione Europea prevede molti metodi per una conservazione adeguata e in sicurezza dei dati personali, tra questi sono presenti varie certificazioni Standard ISO: riconoscimenti ufficiali che attestano che un'azienda o un ente rispetta determinati standard internazionali stabiliti dall’International Organization for Standardization (ISO). Sulla sicurezza delle informazioni abbiamo lo standard ISO/IEC 27001 che definisce i requisiti per la gestione della sicurezza delle informazioni e dei dati sensibili, assicurando che l'organizzazione sia in grado di proteggere le informazioni da accessi non autorizzati o perdite accidentali.
Ma non è necessario ricorrere a istituti internazionali per avere delle definizioni su misure di sicurezza per la gestione dei dati: il GDPR negli articoli 32 e seguenti, prevede una serie di obblighi che il titolare del trattamento deve rispettare per garantire l'integrità e la riservatezza dei dati.

1.2.2 Trasparenza del trattamento: analisi art 12 GDPR e Considerando 58 e 59

L’articolo 12 del Regolamento Generale sulla Protezione dei Dati è fondamentale per garantire la trasparenza e la responsabilizzazione del titolare del trattamento dei dati personali. Esso stabilisce i diritti degli interessati e i doveri dei titolari del trattamento riguardo alle informazioni da fornire

[14] Regolamento (UE) 2016/679, Art. 5.

articolandosi attorno agli altri principi fondamentali del regolamento, già analizzati nel paragrafo precedente, e focalizzandosi su quello della trasparenza.

Il primo comma, nello specifico, sottolinea l'importanza del fatto che i titolari del trattamento devono fornire le informazioni riguardo le modalità di quest'ultimo in modo conciso, trasparente, facilmente accessibile e con un linguaggio semplice e chiaro.

Questo articolo, inoltre, si concentra su una serie di comunicazioni che il titolare del trattamento deve riferire all'interessato per poter essere completamente trasparente nell' intero processo di gestione del dato personale: dalla raccolta, all'utilizzo e infine alla conservazione.[15]

A supporto di questo articolo abbiamo due Considerando: il considerando 58 e il considerando 59.

Il considerando 58 implementa questo articolo enfatizzando l'importanza di informare gli interessati in modo chiaro e comprensibile. Sottolinea la necessità di un'informazione che non sia solo formalmente corretta, ma che si adatti alle esigenze degli utenti: ad esempio cita il dato che riguarda i minori che, data la necessità di una protezione specifica del trattamento, deve essere di un linguaggio semplice che un minore possa facilmente comprendere. Questo è un aspetto fondamentale, poiché il Regolamento riconosce nuovamente la vulnerabilità di alcune categorie di soggetti e invita i titolari del trattamento a considerare il contesto in cui le informazioni vengono fornite in modo da garantire che tutti i soggetti siano in grado di esercitare i loro diritti.

Il considerando 59, invece, si concentra sulle modalità di comunicazione e sulle risposte alle richieste dell'interessato, che devono essere fatte al più tardi entro un mese.

[15] Da implementare poi con l'articolo 13 (Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato) e l'articolo 14 (Informazioni da fornire qualora i dati personali non siano stati ottenuti presso l'interessato) che elencano nello specifico le informazioni da fornire in caso di raccolta di dati.

1.3 Privacy Policy:

In un sito web tutte le informazioni descritte nell'articolo 12 del Regolamento devono essere riportate nella Privacy Policy.

Ma cosa si intende per Privacy Policy? L'informativa privacy di un sito web è il documento con il quale si comunica agli utenti che accedono al sito, chi è incluso e come viene effettuato il trattamento dei dati personali.

Innanzitutto vorrei ricordare che un dato personale è solamente ciò che viene definito dall'articolo 4 del Regolamento, per cui una qualsiasi informazione riguardante una persona fisica.[16]

La suddetta policy è, secondo il Regolamento e il Codice Privacy, obbligatoria ogni qualvolta che si verifica un trattamento di dati, questo comprende gran parte dei siti web, ma soprattutto i siti di e-commerce o tipologie ibride, come i social media, che offrono più servizi.

1.3.1 Differenza con le Cookie Policy

Tendenzialmente si tende a confondere questo documento con la Cookie Policy di un sito web, ma sono due cose che si differenziano parzialmente. Infatti la policy dei cookie spesso è solo una parte dell'informativa privacy o un documento a parte, che definisce all'utente quali cookie vengono rilasciati dal sito web e per quali finalità. I cookie sono una tipologia di file che viene installato sul terminale dell'utente quando visita un sito web; possono avere diverse finalità (cookie tecnici o di profilazione) e possono essere rilasciati direttamente dal sito oppure da soggetti terzi (cookie di terza parte), ad esempio Google o Facebook.

1.3.2. Caratteristiche privacy policy:

Innanzitutto, l'informativa sulla privacy deve rispettare i principi stabiliti dall'articolo 5 del GDPR. Pertanto, deve essere chiara, utilizzando un linguaggio comprensibile a tutti, non eccessivamente lunga e contenere

[16]Regolamento (UE) 2016/679, Art. 1, comma 1: «dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»);

informazioni veritiere e non ambigue. Inoltre, deve essere trasparente, come indicato dall'articolo 12 e dal considerando 39[17]; con questo si intende che deve contenere tutte le informazioni necessarie per il trattamento dei dati, e deve esporle in modo chiaro e dettagliato.

Innanzitutto, deve essere specificato il titolare del trattamento, con le generalità e le modalità di contatto, e il responsabile del trattamento, che svolge un ruolo cruciale nella gestione dei dati[18]. Se l'azienda rientra nella categoria che prevede l'obbligo di nomina, devono essere forniti i dati del Data Protection Officer (DPO), con le relative informazioni di contatto.

Le finalità del trattamento, come customer care, profilazione o marketing, devono essere chiaramente delineate per informare gli utenti sull'uso dei loro dati. La base giuridica del trattamento è stabilita dall'articolo 6 del GDPR, che definisce le condizioni necessarie per la legalità del trattamento stesso. È essenziale specificare i dati trattati e il loro periodo di conservazione, affinché gli interessati siano consapevoli di come e per quanto tempo le loro informazioni vengono gestite. Infine, è importante garantire che gli interessati siano a conoscenza dei propri diritti, come il diritto di accesso, rettifica e cancellazione dei dati, per assicurare una gestione responsabile e rispettosa delle informazioni personali.

1.4 Normativa privacy negli Stati Uniti

Dopo aver analizzato i principi e le norme fondamentali della normativa europea sulla protezione dei dati, vorrei ora concentrarmi su come questo argomento sia legiferato in un'altra grande potenza mondiale, gli Stati Uniti d'America.

Il concetto del diritto alla privacy nasce effettivamente alla fine del XIX secolo, proprio negli Stati Uniti, dagli autori dell'articolo “The right to privacy”: Samuel

[17] Regolamento (UE) 2016/679, Considerando 39: “Qualsiasi trattamento di dati personali dovrebbe essere lecito e corretto. Dovrebbero essere trasparenti per le persone fisiche le modalità con cui sono raccolti, utilizzati, consultati o altrimenti trattati dati personali che li riguardano nonché la misura in cui i dati personali sono o saranno trattati. [...] le informazioni e le comunicazioni relative al trattamento di tali dati personali siano facilmente accessibili e comprensibili e che sia utilizzato un linguaggio semplice e chiaro.”

[18] Definizione nel Regolamento (UE) 2016/679, Art 4, comma 8(«Definizioni»).

Warren e Louis D. Brandeis. Nel suddetto articolo questo diritto veniva definito come “the right to be let alone”, cioè il diritto di essere lasciati da soli.
La necessità di questo nuovo diritto nasce dal fatto che le nuove fotocamere, sviluppate appunto alla fine dell’800, permettevano di scattare fotografie senza più che la persona interessata ne fosse consapevole e questo era in grado di creare una vera e propria violazione della sfera privata.
Il riconoscimento del diritto alla privacy nel sistema giuridico statunitense ha richiesto del tempo, ma l'articolo di Warren e Brandeis ha rappresentato un passo cruciale per avviare il cambiamento. Un altro ruolo chiave è stato quello dei giudici, essenziali in un ordinamento di Common Law: interpretando attentamente gli Emendamenti della Carta dei Diritti, tramite varie decisioni, hanno individuato il fondamento costituzionale della privacy.

1.4.1 Attuale legislazione in materia privacy negli USA

Attualmente negli Stati Uniti la regolamentazione in materia privacy è molto frammentata.
Il sistema normativo statunitense è organizzato su base federale, per cui il potere è suddiviso tra il governo federale e i singoli stati. La Federazione nasce con la Costituzione del 1787, con l’obiettivo di unificare gli stati non dal punto di vista normativo, ma più dal punto di vista militare e fiscale, garantendo quindi l'autonomia statale. La Costituzione includerà poi nel 1789 il "Bill of Rights", composto da 10 emendamenti, con l’obiettivo di proteggere le libertà fondamentali degli individui, come la libertà di parola, di religione e il diritto a un giusto processo. Questi emendamenti sono stati introdotti per limitare i poteri del governo federale e sono fondamentali per la democrazia americana, ma questo documento non è da considerare come una Costituzione tipica di un ordinamento di “civil law”, ad esempio come quella Italiana del 1948: all’interno non vi è un testo di legge con una normativa dettagliata, ma più dei principi chiave che gli Stati della federazione devono seguire nella legiferazione delle loro leggi.

Oltre alle norme federali, ogni Stato ha la propria Costituzione e un insieme di leggi e regolamenti. Sono queste norme statali a regolamentare effettivamente la vita dei cittadini, in quanto coprono vari aspetti come l'istruzione, la salute, la criminalità e i diritti civili. La capacità degli stati di legiferare autonomamente è un principio chiave del federalismo, che è centrale nel sistema giuridico americano.
Inoltre, il Congresso degli Stati Uniti, composto da Camera dei Rappresentanti e Senato, può emanare leggi federali che si applicano a tutti gli stati. Quest'ultime trattano in genere questioni di interesse nazionale, come l'immigrazione e la politica estera. In caso di conflitto tra una legge statale e una legge federale, prevale quest'ultima secondo un principio di gerarchia delle fonti, sancito dalla Costituzione.

La disciplina sulla protezione dei dati negli Stati Uniti è molto legata a quella sulle tecnologie, in quanto entrambe vengono regolate dai singoli stati, con gli stessi criteri: le agevolazioni finanziarie su questi settori e la giurisprudenza su queste materie.
Da ciò è possibile dedurre che possono esserci stati, come la California, lo Stato di New York o il Delaware, con leggi orientate sullo sviluppo delle tecnologie e che quindi offrono anche molti incentivi per questo settore, e stati più conservatori che invece hanno un'ottica completamente opposta.
Negli ultimi anni, sono nati vari Regolamenti in materia privacy come il "Colorado Privacy Act" (ColoPA), il "California Privacy Rights Act" del 2020 (CPRA), il "Connecticut Act Concerning Personal Data Privacy and Online Monitoring" (CTDPA), il "Delaware Personal Data Privacy Act" (DPDPA) o il "Florida Digital Bill of Rights" (FDBR)[19].
Tutti questi regolamenti, essendo statali, possono presentare alcune similitudini, ma anche grandi differenze, in base ai principi politici ed economici dello stato da cui sono stati emanati.

[19] Lewis Rice. Lewisrice.com. https://www.lewisrice.com/u-s-state-privacy-laws/

1.4.2 Il nuovo American Privacy Rights Act:

Considerando quanto detto, tuttavia, nell'immediato futuro la normativa della privacy negli Stati Uniti potrebbe cambiare drasticamente. Difatti il 7 Aprile 2024 è stata presentata, in una seduta del Congresso "bipartisan"[20] una nuova bozza per una legge federale in materia privacy: l'American Privacy Rights Act (APRA). Questa proposta ha l'obiettivo di definire, finalmente a livello federale, i livelli minimi di protezione dei dati personali per vari settori economici, nonché di stabilire norme di sicurezza informatica. Al momento, come è stato analizzato nel precedente paragrafo, il quadro normativo è estremamente frammentato, con differenze tra Stato a Stato, con diversi livelli di protezione dei dati personali e, soprattutto, con grandi differenze settoriali.

Questa proposta di legge verrà applicata alle *"covered entities"*[21], cioè le organizzazioni che determinano le finalità e i mezzi della raccolta, elaborazione, conservazione o trasferimento dei dati. Sono previsti inoltre, dei soggetti per i quali ci saranno norme specifiche e più serrate, ad esempio i *"large data holder*[22]*"* e soggetti a cui non verranno applicate le norme previste dall'APRA, come alcuni soggetti pubblici, organizzazioni no profit e le piccole imprese.

Inoltre nella bozza della normativa viene data una definizione di quelli che sono i "Covered data", cioè i dati personali presi in oggetto dall'APRA e, vengono già definite le tipologie di dati personali che necessitano un livello più alto di

---

[20] Bipartisan: agg. ingl. Nel linguaggio politico [...], che è accettato da entrambe le parti politiche in contrasto o che è disposto ad assumere le difese dell'una e dell'altra. Treccani.it/vocabolario

[21] Definiti dall'American Privacy Rights Act come: "any entity that, alone or jointly with others, determines the purposes and means of collecting, processing, retaining, or transferring covered data and (i) is subject to the Federal Trade Commission Act (15 U.S.C. 41 et seq.); (ii) is a common carrier subject to title II of the Communications Act of 1934 (47 U.S.C. 201 et seq.); or (iii) is an organization not organized to carry on business for its own profit or that of its members."
American Privacy Rights Act, H. R. 8818, 118th Cong., 25 June 2024, Section 101, https://www.congress.gov/bill/118th-congress/house-bill/8818/text#H6C8FDD4A9BE34CF78198D4D0673D9DF6

[22] Definiti dall'American Privacy Rights Act come: "a covered entity or service provider that, in the most recent calendar year, had an annual gross revenue of not less than $250,000,000 and, subject to subparagraph (B), collected, processed, retained, or transferred"— definendo poi al paragrafo B le quantità di dati personali, comuni e sensibili, che devono possedere per rientrare nella categoria.
American Privacy Rights Act, H. R. 8818, 118th Cong., 25 June 2024, Section 101, https://www.congress.gov/bill/118th-congress/house-bill/8818/text#H6C8FDD4A9BE34CF78198D4D0673D9DF6

protezione, come i dati relativi alla salute o all'orientamento politico, religioso o sessuale.

Le normative americane, sia che siano statali o del Congresso, in genere danno molta importanza all'ottica economica dell'argomento oggetto di discussione, per cui anche in questa nuova normativa l'aspetto economico del dato personale sarà fondamentale, infatti essa considera valutabili come dati personali anche i dati che possono essere oggetto di compravendita.

Per quanto riguarda i principi di questa proposta di legge, si avvicinano molto a quelli del Regolamento europeo, già analizzati nei paragrafi precedenti. In particolare i due principi fondamentali alla base della nuova normativa americana sono proprio il principio di minimizzazione dei dati e il principio di trasparenza.

1.4.3 Analisi similitudini e prime differenze tra Amercan Privacy Rights Act e Regolamento (UE) 2016/679.

A seguito dell'analisi del paragrafo precedente, è già possibile intuire che tra il Regolamento della Commissione Europea e la bozza della nuova normativa sulla privacy americana ci sono diverse similitudini, ma anche alcune differenze sostanziali.

Le prime analogie le troviamo nella Section 101, la prima sezione riguardante le definizioni, che comprende la descrizione di varie parole chiave, presenti o di stesso significato di quelle descritte nell'articolo 4 del GDPR.

Innanzitutto i soggetti definiti dalla normativa come "*Covered entities*" ricordano i "titolari del trattamento" definiti dall'articolo 4 del GDPR[23]. Nella definizione generica di "*Covered data*" data dall'APRA[24] *"[...] information that identifies or*

[23] Regolamento (UE) 2016/679, Art 4, comma 7: «titolare del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri; Cfr con nota [16]

[24] [...] information that identifies or is linked or reasonably linkable, alone or in combination with other information, to an individual or a device that identifies or is linked or reasonably linkable to 1 or more individuals" American Privacy Rights Act, H. R. 8818, 118th Cong., 25 June 2024, Section 101,

is linked or reasonably linkable, alone or in combination with other information, to an individual or a device that identifies or is linked or reasonably linkable to 1 or more individuals", il concetto di base è lo stesso di quella di *"dato personale"* [25] del GDPR, cioè nell'informazione che identifica o che può identificare un individuo. La definizione statunitense aggiunge, rispetto a quella europea, il concetto del "*device*", cioè del dispositivo che può portare all'identificazione del soggetto.

Vengono definiti poi i "*sensitive data*", che ricordano sotto vari punti di vista, la loro definizione nell'articolo 9 del GDPR e varie altre parole chiave come "Large Data Holder"[26], "Third party", "Small business", etc.

Nella Section 102 viene ripreso un principio fondamentale che accomuna la normativa europea e quella statunitense: la minimizzazione dei dati. La limitazione della raccolta di quest'ultimi a scopi specifici e il divieto di trasferire dati sensibili a terzi senza il consenso esplicito dell'utente, è un punto fondamentale per la normativa americana e un diritto del consumatore. Infatti, richiedendo alle organizzazioni di raccogliere solo le informazioni necessarie, viene sottolineata l'importanza di un altro argomento chiave, cioè diritti dei consumatori. Questi diritti comprendono l'accesso ai dati, la correzione, la cancellazione, l'esportazione e la possibilità di rinunciare alla pubblicità mirata; tutti diritti fondamentali per il trattamento dei dati anche secondo la Commissione europea.

La minimizzazione dei dati personali è uno dei principi fondamentali dell'APRA insieme quello esposto nella Section 104, la trasparenza.

Con questo principio i membri del Congresso vogliono garantire non solo la trasparenza del trattamento dei dati personali, ma anche la possibilità di rinunciare alla pubblicità mirata e al trasferimento dei propri dati. Nella sezione

---

https://www.congress.gov/bill/118th-congress/house-bill/8818/text#H6C8FDD4A9BE34CF78198D4D0673D9DF6

[25] Art 4 GDPR - «dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

[26] Vedi nota [17]

sulla trasparenza vengono elencate una serie di informazioni fondamentali che devono essere comunicate alle *"covered entities"* , come viene fatto negli articoli 12 e seguenti del Regolamento europeo.
Altro punto in comune tra le normative, è la creazione di una autorità di controllo, la Federal Trade Commission, con la differenza che, come si può comprendere dal nome, sarà federale, cioè una unica per tutti gli Stati della federazione. Non vi saranno quindi delle autorità di controllo per i singoli stati come è previsto dall'articolo 51 del Regolamento europeo (ad esempio il Garante Italiano, l'ICO per la Gran Bretagna, l'AEPD spagnola, ect…).

Ultimo punto in comune tra le due normative di necessaria analisi per comprendere l'oggetto di questa tesi, è il concetto di Privacy By Design.
Il principio di "privacy by design", coniato da Ann Cavoukian[27] già nel 2010, si basa su vari aspetti, tra cui l'implementazione di misure tecniche e organizzative adeguate, l'analisi dei rischi fin dalla fase progettuale, l'integrazione della privacy come impostazione predefinita e la trasparenza del trattamento in tutto il suo iter. Il GDPR enfatizza per questo principio un approccio basato sulla valutazione del rischio da predisporre prima dell'inizio del trattamento, con obblighi più rigorosi per i dati sensibili, come quelli di minori.
L'American Privacy Rights Act, alla Section 103, intitolata di fatto "Privacy By Design", asserisce che ogni "Covered Entity" deve implementare delle politiche per la gestione del trattamento dei dati e creare un piano per la "Mitigation of privacy risks", questo comporta una valutazione dei rischi e un progetto di formazione interna per i soggetti responsabili del trattamento. Inoltre viene prevista, entro un anno dall'entrata in vigore della normativa, la presentazione di alcune linee guida sull'argomento da parte della Commissione, che avranno

[27] Ann Cavoukian è un'esperta canadese di privacy, conosciuta per essere la pioniera del concetto di "privacy by design", un approccio che integra la protezione dei dati sin dalle fasi iniziali di progettazione dei sistemi. E' stata un membro della Commissione per la privacy dell'Ontario dal 1997 al 2014, dove ha promosso politiche innovative per la tutela dei dati personali. Cavoukian ha scritto numerosi articoli e rapporti su temi legati alla privacy e alla sicurezza dei dati, collaborando anche con organizzazioni internazionali, tra cui "The 7 Foundational Principles Information and Privacy Commissioner of Ontario (2011)"

particolare attenzione per le “nonprofit organizations, service provider, and data brokers.”[28]

1.5 Conclusioni

In questo capitolo è stato analizzato come il concetto di trasparenza nel trattamento dei dati personali in Europa è già consolidato, in quanto aspetto fondamentale del Regolamento Generale sulla Protezione dei Dati. Negli ultimi anni la maggior parte delle aziende e istituzioni hanno dovuto implementare processi e policy proprio per garantire questo principio.

È stata poi analizzata, sia la situazione attuale riguardante la normativa statunitense sulla privacy, sia i cambiamenti dovuti alla nuova proposta di legge su questa materia: l’American Privacy Rights Act.

Entrambe queste potenze mettono, di fatto, al centro della loro normativa il diritto alla trasparenza delle informazioni.

Nei prossimi due capitoli verranno commentate due sentenze che sono un esempio fondamentale su come i siti web devono obbligatoriamente garantire questo principio per non ricorrere a sanzioni.

[28] American Privacy Rights Act, H. R. 8818, 118th Cong., 25 June 2024, Section 103, https://www.congress.gov/bill/118th-congress/housebill/8818/text#H6C8FDD4A9BE34CF78198D4D0673D9DF6

CAPITOLO II

Commento del caso Facebook vs AGCOM

2.1 Introduzione sulle autorità di controllo.

Con il Regolamento generale sulla protezione dei dati 2016/679, nello specifico all'articolo 51, la Commissione europea impose ad ogni Stato membro l'istituzione di una o più autorità indipendenti. Questi istituti di controllo sono stati ideati col fine di esercitare un potere di esecutivo di supervisione nell'applicazione del suddetto regolamento e, di conseguenza, tutelare i diritti e le libertà fondamentali delle persone fisiche in relazione al trattamento dei loro dati.

L'autorità italiana è il Garante per la protezione dei dati personali.

Tra gli obblighi definiti dal GDPR e dal Codice in materia di protezione dei dati personali (D. lgs. 196/2003)[29] abbiamo: controllare che i trattamenti dei dati personali avvengano in modo conforme al regolamento, collaborare con le altre autorità di controllo, esaminare i reclami e, di conseguenza, adottare i provvedimenti previsti dalla normativa, prima con ammonimenti ai titolari del trattamento o ai responsabili, poi ordinando la rettifica, la cancellazione dei dati o la limitazione del trattamento.

Oltre a questi compiti di mero carattere esecutivo, ruolo fondamentale del Garante è la formulazione di pareri su proposte di atti amministrativi e normativi e la creazione di linee guida che colmano alcuni vuoti amministrativi.

Quest'ultimo ruolo del Garante per la protezione dei dati personali, in questo specifico ambito, riveste una funzione di fondamentale importanza non solo per le aziende, che devono affrontare il delicato, e a volte complesso, processo di adeguamento alle normative previste dal GDPR, ma anche per la fase di interpretazione della normativa stessa. Effettivamente, attraverso la produzione

[29] Adeguato alle disposizioni del GDPR tramite il d.lgs 10 agosto 2018, n. 101, e altri atti normativi italiani e internazionali.

di linee guida che approfondiscono e chiariscono aspetti specifici del regolamento, il Garante contribuisce a rendere l'applicazione delle disposizioni più chiara e accessibile, semplificando così il processo di conformità per le imprese e assicurando una corretta applicazione delle normative sulla protezione dei dati personali.

Un'altra autorità italiana indipendente che riveste un ruolo significativo in materia di privacy, sebbene non sia la sua funzione principale, è l'Autorità Garante della Concorrenza e del Mercato (AGCM). Istituita nel 1990 con la legge n. 287, l'AGCM ha come missione principale quella di vigilare sulla concorrenza e sul corretto funzionamento del mercato, contrastando le pratiche commerciali scorrette e vigilando sui conflitti di interesse. Tuttavia, in virtù della sua attività di tutela dei diritti dei consumatori e delle imprese, essa svolge anche un ruolo di crescente importanza nell'ambito della protezione dei dati personali, sebbene questo compito derivi indirettamente dalle sue funzioni principali. Questo aspetto, seppur secondario rispetto al suo mandato originario, risulta comunque cruciale per il caso di studio specifico che esamineremo in questo capitolo, in quanto l'AGCM interviene, insieme ad altre autorità, per garantire che le pratiche di mercato rispettino anche la privacy dei consumatori.

L'importanza di queste autorità indipendenti, non può essere in alcun modo sottovalutata, in quanto il Regolamento Generale sulla Protezione dei Dati, pur appartenendo a una tradizione giuridica di tipo civilistico, tipica dei sistemi di civil law con le sue disposizioni dettagliate e codificate, si distingue per l'integrazione di elementi distintivi del sistema giuridico anglosassone della common law. Un esempio evidente di questa influenza è l'introduzione del principio di accountability, che implica una responsabilizzazione attiva dei soggetti che trattano i dati personali e l'adozione di una certa flessibilità nell'applicazione delle norme. Questa combinazione tra tradizioni giuridiche conferisce al GDPR un livello di adattabilità e interpretazione che permette un

adattamento più agile alle realtà concrete e alle evoluzioni tecnologiche e che rende necessaria l'azione di intermediari ed interpreti, come le autorità garanti sopra descritte. Il processo di interpretazione e adeguamento è particolarmente importante, poiché il GDPR, pur essendo un regolamento europeo, è applicabile in contesti molto diversi tra loro, che vanno dalle piccole imprese locali alle multinazionali, e influisce settori che vanno dalla salute all'e-commerce, dalla pubblica amministrazione al settore finanziario. È quindi corretto ribadire che le linee guida e le decisioni delle autorità garanti non solo garantiscono una corretta applicazione delle leggi, ma contribuiscono anche a definire un quadro normativo più preciso e coerente, che permette di affrontare le nuove tecnologie e le dinamiche sociali in continua evoluzione.

2.2. La delibera dell'AGCM

Il caso che andremo a esaminare in questo capitolo inizia con la delibera n. 27432 dell'Autorità garante della Concorrenza e del Mercato (AGCM) emessa il 29 novembre 2018 con il fine di sanzionare Facebook Inc. e Facebook Ireland Ltd., che irrogava due sanzioni amministrative pecuniarie di 5 milioni di euro ciascuna e l'obbligo di una comunicazione di rettifica. La sanzione è stata imposta in relazione a due presunte pratiche commerciali scorrette[30] riguardanti il trattamento dei dati degli utenti di Facebook, sia durante la registrazione degli account sia durante l'utilizzo di alcuni servizi offerti dalla piattaforma. In particolare le suddette pratiche riguardavano la raccolta, l'uso e la condivisione con terze parti dei dati personali degli utenti per fini commerciali.

La prima pratica di Facebook contestata nella delibera dell'AGCM, riguardava l'informativa privacy fornita durante la registrazione alla piattaforma degli utenti. Più precisamente, l'Autorità ha affermato che Facebook non informava l'utente in fase di registrazione in merito alla raccolta e all'utilizzo dei dati di quest'ultimo

[30] Art 20, comma 2, Codice del Consumo: Una pratica commerciale è scorretta se è contraria alla diligenza professionale, ed è falsa o idonea a falsare in misura apprezzabile il comportamento economico, in relazione al prodotto, del consumatore medio che essa raggiunge [...].
La nozione generale di pratica scorretta si declina in due ulteriori categorie: le pratiche ingannevoli (art. 21 e 22 Codice del Consumo) e le pratiche aggressive (art. 24 e 25 Codice del Consumo).

a fini remunerativi. In questo modo non venivano applicati alcuni dei principi fondamentali del GDPR, come l'immediatezza, la chiarezza e la completezza delle informazioni. Difatti, l'informativa nella pagina di registrazione, faceva intendere all'utente che l'uso del servizio fosse gratuito, anzi l'attenzione veniva proprio posta sul fatto che l'iscrizione fosse "gratuita per sempre". Tuttavia, nell'istruttoria di AGCM si sottolinea che: *"i ricavi provenienti dalla pubblicità online, basata sulla profilazione degli utenti a partire dai loro dati, costituiscono l'intero fatturato di Facebook Ireland Ltd e il 98% del fatturato di Facebook Inc."*.
Da questa affermazione è possibile chiaramente dedurre che la prestazione, pur essendo presentata come gratuita per gli utenti, non era in realtà priva di un corrispettivo: il trattamento dei dati personali degli utenti andava a configurarsi come una vera e propria contro-prestazione per il servizio offerto, a fini conseguentemente remunerativi.
In merito a questa condotta ingannevole, l'Autorità ha imposto due azioni obbligatorie per Facebook: in primo luogo il divieto di proseguire con tale pratica e, in secondo luogo, la pubblicazione di una dichiarazione correttiva dell'informativa[31] entro quarantacinque giorni dalla notifica del provvedimento. Questa dichiarazione doveva essere visibile e rimanere attiva per venti giorni sia sulla homepage del sito web italiano sia sull'applicazione di Facebook. Inoltre, doveva apparire al primo accesso di ogni utente italiano registrato, a partire dalla mezzanotte del quarantacinquesimo giorno successivo alla notifica del provvedimento.
La seconda pratica analizzata dall'AGCM, consisteva nel fatto che Facebook avesse implementato un meccanismo di trasferimento dei dati dei propri utenti a siti web e applicazioni di terzi, estranei al rapporto tra Facebook e l'utente, sempre con fini commerciali e remunerativi. Questa condotta è stata definita

[31] Come previsto dall'articolo 27, comma 8 del Codice del Consumo: "*L'Autorità, se ritiene la pratica commerciale scorretta, vieta la diffusione, [...] . Con il medesimo provvedimento può essere disposta, a cura e spese del professionista, la pubblicazione della delibera, anche per estratto, ovvero di un'apposita dichiarazione rettificativa, in modo da impedire che le pratiche commerciali scorrette continuino a produrre effetti".*

“aggressiva” in quanto la trasmissione dei dati personali è avvenuta senza il preventivo ed esplicito consenso delle persone interessate.

Tramite questa analisi, è inoltre emerso un importante problema riguardante la protezione dei dati personali sia nell'ambito delle interazioni tra le diverse piattaforme digitali gestite da Facebook (come ad esempio WhatsApp, Instagram e Messenger), ma anche tra quelle gestite da terzi. Utilizzando questo approccio, gli esperti hanno evidenziato come questo scambio di informazioni, riconducibili al medesimo titolare del trattamento, tra piattaforme diverse può provocare conseguenze preoccupanti nell'ambito della tutela dei dati personali. Infatti, soprattutto durante il processo di esternalizzazione dei dati, informazioni e preferenze dell'utente, si è riscontrato che quest’ultimi possono essere analizzati da sistemi di intelligenza artificiale per ottenere informazioni utilizzabili a fini di marketing e profilazione.

2.3. La sentenza del TAR Lazio

Facebook, in seguito alla delibera dell’AGCM, ha presentato ricorso presso il TAR Lazio (Tribunale Amministrativo Regionale del Lazio) per ottenere una pronuncia di annullamento. Quest'ultimo, con le sentenze n. 260 e 261[32] del 10 gennaio 2020, ha accolto parzialmente il ricorso riconoscendo la fondatezza solamente della prima delle due pratiche contestate, dimezzando di conseguenza la sanzione pecuniaria irrogata nel 2018 da dieci milioni a cinque milioni di euro e rigettando invece la seconda pratica indagata in quanto ritenuta infondata.

2.3.1 Decisioni del TAR sulla prima pratica ingannevole

Nello studio della prima condotta indicata è stato di fondamentale importanza il “claim”, cioè il messaggio promozionale di Facebook, visibile sulla pagina di registrazione iniziale, che incoraggiava gli utenti a iscriversi promettendo: *"Iscriviti, è gratis e lo sarà per sempre".* Con questa affermazione, come già

[32] TAR Lazio, Prima Sezione, Sent. n. 260/2020 https://canestrinilex.com/risorse/facebook-viola-i-dati-personali-tar-lazio/

approfondito nel paragrafo precedente, la piattaforma suggeriva agli utenti che non fosse necessaria alcuna controprestazione "contrattuale" per utilizzare il social network, dando quindi l'impressione che l'accesso e l'utilizzo del servizio fosse completamente libero e gratuito.

Sotto questo punto di vista, il TAR ha sostenuto la decisione dell'AGCM in quanto, considerando gli obiettivi commerciali e remunerativi di Facebook nel trattamento di dati personali dei suoi utenti, non è corretto definire tale servizio come "gratuito". Il TAR ha inoltre evidenziato l'assenza di chiarezza, completezza e trasparenza nelle informative privacy fornite agli utenti, il che ha impedito agli utenti di comprendere appieno le finalità del trattamento dei loro dati.

Il tribunale ha affermato che tale pratica era ingannevole secondo la definizione dell'articolo 20, comma 2 del Codice del Consumo[33], e impediva *"la formazione di una scelta consapevole, omettendo di informarlo* (il titolare del trattamento) *del valore economico di cui la società beneficia in conseguenza della sua registrazione al social network".*[34]

L'argomentazione principale del ricorso di Facebook, che sosteneva la gratuità della fruizione del servizio in virtù dell'assenza di un effettivo pagamento monetario, non è stata, pertanto, accettata. È stato ordinato a Facebook di proseguire con la pubblicazione della dichiarazione correttiva riguardante l'informativa presente sul suo sito web, già richiesta dall'AGCM, secondo quanto previsto dall'articolo 27, comma 8 del Codice del Consumo[35].

2.3.2 Decisioni sulla seconda pratica ingannevole

Per quanto riguarda la seconda condotta ingannevole contestata dall'AGCM, relativa al meccanismo di integrazione dei dati degli utenti, tra diverse app e social network, i Giudici Amministrativi l'hanno valutata in modo differente rispetto all'Autorità di controllo. Hanno infatti ritenuto che questa pratica non

[33] Vedi nota a piè pagina n. 30
[34] TAR Lazio, Prima Sezione, Sent. n. 260/2020
[35] vedi nota a piè pagina n. 31

violasse i diritti degli utenti e hanno annullato la sanzione pecuniaria ad essa associata (5 milioni di euro).
Il TAR ha motivato questa decisione sottolineando che, al momento della registrazione su Facebook, gli utenti avevano l'opzione di esprimere il proprio consenso riguardo all'uso dei loro dati personali per integrazioni con altre piattaforme. Pertanto, mentre l'Autorità di controllo aveva ritenuto che gli utenti di Facebook avessero subito un *"indebito condizionamento"* nel fornire il proprio consenso per la trasmissione dei dati a diverse app, il TAR ha fatto notare che è sempre stato possibile scegliere se e quali dati personali condividere in caso di eventuali integrazioni tra Facebook e enti terzi.

2.3.3. I risvolti della sentenza

Queste sentenze del TAR hanno avuto un riscontro alquanto importante riguardo al riconoscimento del valore economico e commerciale dei dati personali, soprattutto nel mercato digitale.
Difatti, i giudici amministrativi, nonostante abbiano riconosciuto solamente la fondatezza della prima delle due condotte contestate dall'AGCM, hanno enfatizzato sia l'importanza generica di un trattamento lecito dei dati personali nelle piattaforme digitali e soprattutto nei social network, ma anche l'importanza di come deve essere informato il titolare del trattamento.
La sentenza del Tar Lazio è di grande rilevanza anche perché conferma il potere dell'AGCM di infliggere sanzioni a tutela degli interessi economici dei consumatori. Come approfondito all'inizio di questo capitolo, il GDPR ha dato il potere di sanzionare gli illeciti commessi durante il trattamento dei dati personali agli istituti di controllo di cui l'articolo 51, che in Italia si concretizza nel Garante per la protezione dei dati personali; ma l'esistenza di altre autorità di controllo, come l'Autorità garante della Concorrenza e del Mercato, sono fondamentali per la protezione dei diritti e delle garanzie dei consumatori online.

Nelle sentenze viene inoltre evidenziato il fatto che i dati personali non sono solamente delle informazioni in grado di identificare un individuo, ma possono

essere anche oggetto di compravendita e, di conseguenza, essere soggetti ad ulteriori tutele sia da parte del nostro ordinamento che da fonti internazionali, anche commerciali. Questo può portare a ulteriori controlli da parte delle autorità e possibili sanzioni in caso di inadeguato livello di tutela.
Analizzando in modo approfondito la struttura del commercio virtuale, emerge che le potenzialità derivanti dallo sfruttamento dei dati personali possono costituire un vero e proprio asset negoziabile, in grado di generare valore economico e, di conseguenza, di assumere la funzione di controprestazione in un contratto. In questo contesto il Tar, affermando che i dati personali possiedono quindi una doppia natura (da un lato sono un diritto legato alla sfera della persona, dall'altro rappresentano una controprestazione a un servizio o prodotto), ha introdotto un concetto innovativo, ma che è stato la base per rimarcare l'importanza del principio della trasparenza nelle informative sui trattamenti dei dati personali dei consumatori nei contratti conclusi online.

Alla luce della gravità rilevante della sanzione pecuniaria inflitta alla società proprietaria del social network, sorge spontanea la domanda su quali misure avrebbero potuto essere adottate per evitarla.
Questa sanzione si sarebbe potuta evitare attraverso un semplice aggiornamento della Privacy Policy della pagina di registrazione. Questo è solo uno di moltissimi casi in cui sono state comminate sanzioni pecuniarie di altissimo livello, per una informativa non adeguata. Pertanto, per le aziende in generale, non solo per i grandi colossi del mercato mondiale, investire in un progetto di adeguamento alle norme del GDPR può essere una grande protezione legale nei confronti di pene pecuniarie di alto livello.

Un ulteriore esempio di errore riguardante le informative privacy presenti in alcuni siti web, ancora oggi molto ricorrente, è il riferimento all'articolo 13 su cui si pone la base del trattamento. Infatti una coincidenza non voluta ha portato che l'informativa per il trattamento dei dati personali del D. Lgs. 196/2003 fosse

stata disciplinata dall'articolo 13, come nel GDPR[36]. Non sono rari infatti, i casi di informative privacy in cui, a scanso di equivoci, vengono inseriti entrambi gli articoli o viene erroneamente nominano solamente quello del Codice Privacy. Questo all'apparenza non comporta un problema di grave importanza, salvo che l'articolo 13 del d.lgs. 196/2003 sia stato abrogato dal successivo D. lgs. 101/2018 e, di conseguenza, non più applicabile. Questo piccolo errore nella compilazione delle informative di un sito web di un'azienda, può comportare anche delle ripercussioni di carattere reputazionale: difatti, la categoria di utenti, purtroppo non ha ancora molto ampia, che sono aggiornati sulla materia, può subito rendersi conto di una mancanza di attenzione e di aggiornamento nella tutela dei loro dati.

È stato ampiamente sottolineato che, anche per le aziende di dimensioni relativamente ridotte, l'adozione e l'applicazione del Regolamento Generale sulla Protezione dei Dati, comporta una serie complessa di adempimenti che vanno ben oltre la mera implementazione di misure di sicurezza informatica o il rispetto delle normative legali. Questi obblighi includono, infatti, una vasta gamma di attività, come la produzione di informative sulla privacy, la redazione di lettere di incarico per i responsabili del trattamento dei dati e gli altri soggetti che trattano dati personali, l'adozione di politiche interne per la formazione del personale in materia e la definizione di processi per la gestione dei dati particolari. Tali attività non sono opzionali e devono essere considerate parte integrante del processo di conformità al GDPR. Il mancato adeguamento a queste disposizioni espone l'azienda a sanzioni di entità estremamente grave, che possono raggiungere importi pari a milioni di euro o, in alcuni casi, a percentuali significative del fatturato annuo dell'azienda stessa. Oltre a ciò, come evidenziato in precedenza, le conseguenze non si limitano solo alle sanzioni pecuniarie, ma possono comportare anche danni reputazionali

[36] Articolo 13 GDPR: Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato; da tener da conto simultaneamente con l'articolo 14 dello stesso Regolamento - Informazioni da fornire qualora i dati personali non siano stati ottenuti presso l'interessato.

significativi, che possono compromettere la fiducia dei clienti e dei partner commerciali, riducendo la competitività dell'azienda sul mercato.
Per concludere, un'azienda che non rispetta adeguatamente le normative sulla protezione dei dati potrebbe diventare vulnerabile a rischi informatici gravi, come attacchi ransomware o incidenti di data breach, che, oltre a comportare danni economici immediati, possono danneggiare in modo permanente l'integrità e la sicurezza delle informazioni trattate.

CAPITOLO III

Caso ChatGPT vs Garante

3.1 Introduzione a ChatGPT e all'Intelligenza Artificiale in EU

ChatGPT è un modello di intelligenza artificiale sviluppato dalla società OpenAI che negli ultimi anni è diventato uno degli strumenti basati sull'intelligenza cognitiva più famosi e utilizzati.

L'espressione "intelligenza artificiale" (spesso abbreviata in "AI" o "IA") è stata coniata nel 1956 da John McCarthy, un informatico statunitense, durante un'importante conferenza al Dartmouth College nel New Hampshire. Questa conferenza è considerata di grande importanza in quanto è diventata il simbolo dell'inizio ufficiale della ricerca sull'IA. Argomento principale di questo convegno era la possibilità di creare delle cosiddette "macchine intelligenti" in grado di emulare i processi cognitivi umani: questo significa saper dare delle risposte ragionate a delle domande come le darebbe un individuo. Già nel XIX secolo, matematici e ingegneri come Charles Babbage e Ada Lovelace avevano immaginato la possibilità di costruire dispositivi capaci di eseguire operazioni complesse in modo automatico. Tuttavia fu solo grazie ai primi computer elettronici negli anni '40 e '50 che queste idee poterono effettivamente iniziare a concretizzarsi.

Nel 1950, Alan Turing, uno dei fondatori della scienza informatica, ideò il famosissimo "Test di Turing"[37], un esperimento mentale con l'obiettivo di valutare se una macchina riuscire a ingannare un umano facendogli credere di essere a sua volta un essere umano durante una conversazione: una macchina di questo tipo verrà considerata "intelligente".

Oggi, l'IA diventato un settore effettivo che è in continua evoluzione e si applica a una vasta gamma di altri settori, non solo alla robotica come si potrebbe

[37] Pubblicato nel suo celebre articolo sulla rivista accademica di filosofia "MIND". Turing, A. M. (1950). Computing machinery and intelligence. Mind, 59(236), 433-460. https://doi.org/10.1093/mind/LIX.236.433

pensare, ma anche alla medicina, ai sistemi di assistenza e molti altri, diventando una delle aree tecnologiche più promettenti e influenti del nostro tempo.

Il parlamento europeo, invece, presso il portale "Società", definisce l'intelligenza artificiale come *"l'abilità di una macchina di mostrare capacità umane quali il ragionamento, l'apprendimento, la pianificazione e la creatività".*[38]
L'IA è quindi capace di apprendere informazioni autonomamente dai dati che processa mediante il cosiddetto *"machine learning"*[39], processo che permette all'intelligenza artificiale di costruire dei modelli basati sulle informazioni ottenute durante il suo "training", da utilizzare poi per prendere decisioni o rispondere alle domande che le vengono poste.

ChatGPT è un software di intelligenza artificiale definito come "chatbot". Con questo termine si intende un "programma informatico capace di interagire vocalmente con l'utente"[40], cioè un modello di linguaggio progettato per comprendere e successivamente creare un testo o un'immagine come se lo farebbe un umano. La piattaforma si basa quindi su un algoritmo "intelligente" chiamato GPT, "Generative Pre-trained Transformer", che "apprende" come le parole e le frasi si connettono tra di loro attraverso un insieme di dati presenti nella rete.
Il problema dal punto di vista della protezione dei dati, che sta alla base del motivo di analisi di questo caso di studio, consiste proprio nel cosiddetto "insieme di dati presenti nella rete". La possibilità di accedere a questo elevatissimo numero di informazioni, da parte di ChatGPT, e di conseguenza

[38] SAS, *"Perché l'intelligenza artificiale è importante? In IA Che cos'è l'intelligenza Artificiale"*, https://www.sas.com/it_it/insights/analytics/what-isartificial-intelligence.html
[39] Treccani, vocabolario: machine learning = "branca dell'Intelligenza Artificiale che si occupa dello sviluppo di algoritmi e tecniche finalizzate all'apprendimento automatico mediante la statistica computazionale e l'ottimizzazione matematica". https://www.treccani.it/vocabolario/machine-learning_%28Neologismi%29/.
[40] Treccani, vocabolario. https://www.treccani.it/vocabolario/chatbot_(Neologismi)/

da parte della società che l'ha prodotta, OpenAI, può portare a trattamenti di dati personali degli individui, che possono risultare illeciti.
Il Garante per la protezione dei dati personali, nel caso di analisi del seguente capitolo, proprio in relazione a questa affermazione, ha reso esecutivo il suo potere e ha preso provvedimenti contro la Società.

3.2 I comunicati del Garante

Il 31 marzo 2023, il Garante per la protezione dei dati, attraverso un comunicato stampa, ha annunciato l'adozione di un provvedimento d'urgenza nei confronti della piattaforma ChatGPT, con la conseguente limitazione del trattamento dei dati personali degli utenti italiani. Questo comunicato è avvenuto a seguito la segnalazione di un reclamo avente oggetto il "data breach"[41] subito dalla società Open AI del 20 marzo del medesimo anno, riguardante le *"conversazioni degli utenti e le informazioni relative al pagamento degli abbonati al servizio a pagamento"* [42].
Questo provvedimento suscitò notevole attenzione, poiché il Garante lo ha emanato senza consultare le autorità di protezione dei dati degli altri Stati membri dell'Unione Europea né il Comitato europeo. L'articolo 60, comma 11, del Regolamento (UE) 2016/679 tuttavia, prevede comunque questa possibilità in caso di circostanze eccezionali[43] e il Garante ha giustificato la richiesta dell'urgenza con il problema del data breach subito dalla piattaforma.

Le varie valutazioni determinate nella fase istruttoria riguardano principalmente l'informativa privacy presente nel sito web. Difatti, secondo il Garante, ChatGPT

[41] Garante per la protezione dei dati personali, https://www.garanteprivacy.it/data-breach: "Una violazione di sicurezza che comporta - accidentalmente o in modo illecito - la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati."
[42] Dal comunicato Stampa del Garante per la protezione dei dati personali, 31 marzo 2023: *Intelligenza artificiale: il Garante blocca ChatGPT. Raccolta illecita di dati personali. Assenza di sistemi per la verifica dell'età dei minori.* https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9870847
[43] Articolo 60, comma 11, GDPR: "Qualora, in circostanze eccezionali, un'autorità di controllo interessata abbia motivo di ritenere che urga intervenire per tutelare gli interessi degli interessati, si applica la procedura d'urgenza di cui all'articolo 66"

non *“forniva alcuna informativa agli utenti, né agli interessati i cui dati sono stati raccolti da OpenAI e trattati tramite il servizio di ChatGPT.”* Oltre a questo problema, è stata rilevata l'assenza di una base giuridica adeguata per la raccolta e il trattamento dei dati degli individui per la finalità specifica dell’addestramento degli algoritmi necessari per il funzionamento del servizio. Un’ulteriore violazione del Regolamento europeo individuata nella fase istruttoria dal Garante è stata un’inesattezza nel trattamento dei dati personali degli interessati. Quest’ultimo problema è dovuto al fatto che le informazioni fornite dalla e all'intelligenza artificiale non corrispondono sempre al dato reale. Infatti ChatGPT viene addestrato con le informazioni pubbliche che trova in vari siti Internet e sulla base di ciò che gli utenti scrivono nella piattaforma stessa. Queste informazioni, tuttavia, non sono sempre corrette, anche semplicemente per una questione di traduzione dall'italiano all'inglese, lingua originale dell'algoritmo.
Infine, ultima importante violazione rilevata dal Garante è l'assenza di una qualsiasi verifica dell'età degli utenti iscritti o di quelli che utilizzano il servizio senza iscrizione, che, secondo le condizioni di utilizzo pubblicate dalla società OpenAI, dovrebbe però essere riservato ai soggetti che abbiano compiuto almeno 13 anni.
Tramite questa analisi, L'autorità italiana per la protezione dei dati, ha ritenuto che *“il trattamento dei dati personali degli utenti, compresi i minori, e degli interessati i cui dati sono utilizzati dal servizio, è in violazione degli artt. 5, 6, 8, 13 e 25 del Regolamento”*. Di conseguenza, esercitando i suoi poteri d'urgenza pervisti dal già citato articolo 60, comma 11 del GDPR, il Garante ha limitato con effetto immediato il trattamento dei dati di utenti italiani per la piattaforma di intelligenza artificiale.

A partire dal 30 marzo 2023, la società proprietaria della piattaforma ha avuto un termine di 20 giorni per informare il Garante riguardo alle misure adottate per sanare le violazioni indicate nel comunicato, con l'avvertimento che, in caso

di mancata comunicazione, sarebbe stata applicata nei confronti della società un'ulteriore sanzione amministrativa.
OpenAI ha subito provveduto ad adeguarsi alle misure richieste dal Garante, migliorando la sua informativa rendendola conforme e principi del Regolamento Europeo, soprattutto per quanto riguarda l'argomento della trasparenza. Ha inoltre specificato che la raccolta dei dati nel servizio di ChatGPT non è effettuata in tempo reale, questo perché il suo "addestramento" si basa su dati raccolti fino al 2022. Chiarendo questo punto, la società si è accertata di non violare il principio sulla correttezza delle informazioni dell'articolo 5 del GDPR. La società, ha inoltre dimostrato il suo impegno nell'applicazione delle correzioni alle violazioni riscontrate dal Garante inserendo il link è l'informativa privacy nel flusso di registrazione e modificando le finalità del trattamento dei dati personali aggiungendo quella di addestramento degli algoritmi. Quanto riguarda la questione del controllo dell'età, la società ha dovuto presentare al Garante, entro il 31 maggio 2023, un programma per l'implementazione di misure sicure ed adeguate, ed entro il 30 settembre 2023 completare l'adeguamento attivando un sistema di "age verification".

Dopo aver ricevuto le informazioni sulle azioni di adeguamento da parte della società OpenAI, l'11 Aprile 2023, attraverso il provvedimento numero 9874702, il Garante ha sospeso il provvedimento adottato con la delibera d'urgenza del 31 marzo e la relativa limitazione provvisoria dell'utilizzo del servizio.

Chiedendo oggi alla piattaforma di intelligenza artificiale di visionare l'informativa privacy, si riceve come risposta che è possibile consultare l'informativa sulla privacy della piattaforma direttamente nel sito ufficiale di OpenAI, e viene inoltre generato un link ipertestuale che rimanda alla pagina dell'informativa.[44].È inoltre descritto, come frase conclusiva del discorso, che

[44] link alla pagina dell'informativa: https://openai.com/it-IT/policies/privacy-policy/

nella pagina si troveranno tutte le informazioni riguardo a come i dati vengono trattati, raccolti e conservati.

Per quanto riguarda, invece, il sistema di age verification richiesto dal Garante, OpenAI ha inserito nella schermata del proprio sito internet di benvenuto riservata agli utenti italiani già registrati al servizio, un ulteriore comando cliccabile tramite un collegamento ipertestuale, attraverso il quale è possibile accedere nuovamente al servizio (effettuare il login con i propri dati di registrazione), solamente dopo aver dichiarato di essere maggiorenni o ultra tredicenni e, in questo caso, viene richiesto di accertare di avere il consenso preliminare dei genitori.[45] Inoltre, nella schermata di registrazione alla piattaforma è richiesta la data di nascita, con un blocco che impedisce la continuazione del processo di login nel caso in cui venga inserita un'età inferiore ai 13 anni. Per i minorenni di età superiore ai 13 anni, viene richiesta anche in questo caso la conferma del consenso parentale.[46]

Con l'utilizzo gratuito e senza registrazione non compare però alcuna modalità di certificazione dell'età. In questo caso però il servizio non è di tipo continuativo, ma è possibile effettuare solo un determinato numero di domande all'intelligenza artificiale. Superate questa quantità viene bloccata la possibilità di inserire ulteriori affermazioni nella barra di richiesta e appare il pop-up per il login o la registrazione alla piattaforma.

Oltre a ciò, la vicenda si è conclusa con la creazione da parte del Garante di una task force sulla piattaforma insieme agli altri istituti di controllo europei, con lo scopo di promuovere la cooperazione nell'applicazione delle normative del Regolamento europeo sulla protezione dei dati all'interno del servizio in tutti gli stati membri.[47]

---

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

[46] vedi ultima citazione

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

3.3. Conclusioni

Questo provvedimento e le successive interazioni tra il Garante per la protezione dei dati personali e la società OpenAI, è stato di fondamentale importanza, in quanto è stato uno dei primi passi per la gestione di queste nuove tecnologie di intelligenza artificiale, che rappresentano ancora oggi un grande vuoto normativo[48]. È da citare, inoltre, una vicenda simile avvenuta tra l'Autorità Garante irlandese[49] e Google Bard, un chatbot simile a ChatGPT sviluppato da Google, che è stato bloccato in quanto non ritenuto conforme alla normativa europea sulla privacy.

Questo nuovo approccio adottato dagli istituti di controllo degli Stati membri, è basato su una valutazione fatta preventivamente delle nuove tecnologie per evitare che quest'ultime possano poi rivelarsi non conformi o addirittura illegittime. Questo approccio si basa sul principio di "privacy by design e privacy by default" previsto dal Regolamento come corollario del principio di accountability su cui è basato.

Tramite il commento di questo provvedimento da parte del garante e le relative ripercussioni e azioni correttive da parte della società OpenAI, è stata nuovamente rimarcata l'importanza di una corretta e trasparente stesura dell'informativa privacy. In questo caso, a differenza da quello analizzato nel capitolo precedente, non vi sono state delle sanzioni pecuniarie o di reputazione, grazie alle azioni repentine della società proprietaria della piattaforma.

[48] La Commissione europea, con la promulgazione dell'AI Act prevista per il 2025 ha effettuato però un grande passo in avanti rispetto a questo problema.
[49] The Data Protection Commission, link al sito ufficiale: https://www.dataprotection.ie/en

SITOGRAFIA E BIBLIOGRAFIA:

- American Privacy Rights Act, H. R. 8818, 118th Cong., 25 June 2024, Section 103, https://www.congress.gov/bill/118th-congress/housebill/8818/text#H6C8FDD4A9BE34CF78198D4D0673D9DF6
- Anastasio, “ChatGPT torna online in Italia, nuovo sistema di age verification entro il 30 settembre”,
- CALIFANO, Privacy: affermazione e pratica di un diritto fondamentale, Napoli, 2016, p.63.
- Codice del consumo, link al sito di Normattiva: https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2005-09-06;206!vig=
- Comunicato Stampa del Garante per la protezione dei dati personali, 31 marzo 2023: *Intelligenza artificiale: il Garante blocca ChatGPT. Raccolta illecita di dati personali. Assenza di sistemi per la verifica dell’età dei minori. https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9870847*
- Direttiva 95/46/CE “tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati”
- Informativa Privacy ChatGPT: https://openai.com/it-IT/policies/privacy-policy/
- Key4biz, 2023. https://www.key4biz.it/chatgpt-torna-online-in-italia-nuovo-sistema-di-age-verificationentro-il-30-settembre/444595/
- Lewis Rice. Lewisrice.com. https://www.lewisrice.com/u-s-state-privacy-laws/
- Nicola Fabiano (2019) GDPR & privacy: consapevolezza e opportunità. Analisi ragionata della protezione dei dati personali tra etica e cybersecurity; Editore: goWare. (Prefazione di Giovanni Buttarelli)
- Palumbo, “*ChatGPT e Garante italiano: alcune riflessioni a distanza di tempo”*, DebertiJacchia, 2023.

https://www.dejalex.com/2023/06/chatgpt-gdpr-riflessioni-tutela-dati/?lang=it

- Regolamento (UE) 2016/679
- Rivista accademica di filosofia “MIND”. Turing, A. M. (1950). Computing machinery and intelligence. Mind, 59(236), 433-460. https://doi.org/10.1093/mind/LIX.236.433
- SAS, *“Perché l’intelligenza artificiale è importante? In IA Che cos’è l’intelligenza Artificiale”*, https://www.sas.com/it_it/insights/analytics/what-isartificial-intelligence.html
- Sito ufficiale del Garante per la protezione dei dati personali, https://www.garanteprivacy.it/
- TAR Lazio, Prima Sezione, Sent. n. 260/2020 https://canestrinilex.com/risorse/facebook-viola-i-dati-personali-tar-lazio/
- The Data Protection Commission, link al sito ufficiale: https://www.dataprotection.ie/en
- Treccani, vocabolario. https://www.treccani.it/vocabolario/