



UNIVERSITA' DEGLI STUDI DI PADOVA

**DIPARTIMENTO DI SCIENZE ECONOMICHE ED AZIENDALI
"M. FANNO"**

CORSO DI LAUREA IN ECONOMIA

PROVA FINALE

**TRA PRIVACY E POTERE DI MERCATO: IL CASO APPLE E L'APP
TRACKING TRANSPARENCY**

RELATORE:

CH.MO PROF. MADIO LEONARDO

LAUREANDO/A: FANTINATO RAFFAELLO

MATRICOLA N. 2034905

ANNO ACCADEMICO 2024 – 2025

Dichiaro di aver preso visione del “Regolamento antiplagio” approvato dal Consiglio del Dipartimento di Scienze Economiche e Aziendali e, consapevole delle conseguenze derivanti da dichiarazioni mendaci, dichiaro che il presente lavoro non è già stato sottoposto, in tutto o in parte, per il conseguimento di un titolo accademico in altre Università italiane o straniere. Dichiaro inoltre che tutte le fonti utilizzate per la realizzazione del presente lavoro, inclusi i materiali digitali, sono state correttamente citate nel corpo del testo e nella sezione ‘Riferimenti bibliografici’.

I hereby declare that I have read and understood the “Anti-plagiarism rules and regulations” approved by the Council of the Department of Economics and Management and I am aware of the consequences of making false statements. I declare that this piece of work has not been previously submitted – either fully or partially – for fulfilling the requirements of an academic degree, whether in Italy or abroad. Furthermore, I declare that the references used for this work – including the digital materials – have been appropriately cited and acknowledged in the text and in the section ‘References’.

Firma (signature)

INDICE

INTRODUZIONE

CAPITOLO 1: La privacy, il dato personale e la loro tutela

- 1.1 La privacy, il dato personale e il paradosso della privacy
 - 1.1.2 Distinzione tra privacy e dato personale
- 1.2 Evoluzione della legislazione sulla privacy
- 1.3 Il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio (GDPR)
- 1.4 Regolamento (UE) 2022/868: Data Governance Act (DGA)
 - 1.4.2 GDPR e DGA, differenze e controversie

CAPITOLO 2: Il vantaggio competitivo dei dati e la loro regolamentazione

- 2.1 Il mercato unico digitale (DSM)
- 2.2 Proposte regolatrici: Digital Markets Act (DMA)
 - 2.2.2 Definizioni importanti
 - 2.2.3 Le norme del DMA
- 2.3 Economics of digital privacy
- 2.4 Antitrust e l'AGCM
 - 2.4.2 Art. 102 TFUE e concetto di abuso di posizione dominante
 - 2.4.3 Concetto di "self-preferencing"

CAPITOLO 3: Case study - A561 - APP TRACKING TRANSPARENCY DI APPLE

- 3.1 Le parti
- 3.2 Analisi del caso
- 3.3 I mercati di riferimento
- 3.4 Effetti e conseguenze economiche del caso
- 3.5 Le conclusioni del caso

CONCLUSIONI

BIBLIOGRAFIA

INTRODUZIONE

L'evoluzione digitale ha portato con sé innovazione e tecnologia, fattori in grado di semplificare la vita di ogni essere umano. Nonostante ciò, anche quello che può sembrare gratuito ad un primo impatto ha un prezzo.

L'evoluzione digitale, infatti, ha semplificato l'accesso ai dati personali, a vantaggio delle imprese e a discapito del consumatore. Le aziende puntano a raccogliere una quantità sempre maggiore di dati al fine di vendere di più i propri beni e servizi. Tale fenomeno accade in quanto l'accesso alle informazioni personali di un utente permette alle imprese di proporre la soluzione ideale ad ogni possibile consumatore.

Questo elaborato si propone di comprendere in che modo il dato personale è in questo contesto protetto e se esso possa diventare un fattore di vantaggio competitivo per le aziende.

A tal fine, nel primo capitolo si indagherà il concetto di privacy e di dato personale per capire in che modo lo Stato e la Comunità Europea stiano operando per garantire una maggiore tutela al cittadino. A tal fine, si scoprirà anche il cosiddetto "paradosso della privacy", una contraddizione tra l'apparente interesse alla privacy e la facilità con la quale il consumatore se la nega. Inoltre, le principali tutele analizzate saranno il Regolamento Generale sulla Protezione dei Dati (GDPR) e il Data Governance Act (DGA).

Nel secondo capitolo, invece, si esplorerà la nozione di dato personale da un punto di vista maggiormente economico. In questa sezione il dato verrà visualizzato come vantaggio competitivo per le aziende e si cercherà di comprendere in che modo la Regolamentazione stia agendo. Le proposte analizzate saranno il Digital Markets Act (DMA) e l'articolo 102 del TFUE. Fondamentale in tale contesto sarà la figura dell'Autorità Garante della Concorrenza e del Mercato.

Infine, nel terzo capitolo si analizzerà un caso studio, al fine di concretizzare i concetti analizzati nelle pagine precedenti. Il caso in esame riguarda una Regolamentazione implementata dalla società Apple Inc., la cosiddetta App Tracking Transparency. Inoltre, in quest'ultima parte si evidenzierà come l'accesso ai dati personali influenzi l'andamento economico di un'azienda.

CAPITOLO 1: LA PRIVACY, IL DATO PERSONALE E LA LORO TUTELA

1.1 La privacy, il dato personale e il paradosso della privacy

La prima definizione di privacy è rintracciabile tra i pensieri di Warren e Brandeis (si veda Lukács 2016, p. 257), definita come “The right to be let alone”. Gli autori richiedevano una tutela contro la divulgazione senza consenso di vicende private, emozioni e pensieri.

Privacy però è un concetto ampio, in continuo mutamento ed evoluzione. Solove (2010) (si veda Lukács 2016, p. 258), individua quattro principali dimensioni ai fini di dare una spiegazione alla disciplina indagata: metodo, generalità, variabilità e focus.

Iniziando dal concetto di metodo, l'autore afferma che la privacy è la risultante di diverse nozioni tra loro correlate. La generalità, invece, si riferisce al fatto che la privacy si forma a partire da contesti specifici, ma deve avere una portabilità generale, applicabile dunque a svariati contesti. La terza dimensione, riguarda la variabilità, ovvero la flessibilità e l'adattamento del concetto trattato a differenti culture e al tempo. Nonostante ciò, non può essere troppo adeguabile al contesto, in quanto perderebbe stabilità e provocherebbe confusione. Infine, la privacy non può essere guardata da troppe angolazioni ma deve partire da un punto focale, come risposta a problemi concreti della vita reale.

Sulla base di queste dimensioni, Solove, afferma che la privacy è:

1. Il diritto ad essere lasciati in pace,
2. L'accesso limitato al sé,
3. Il segreto,
4. Il controllo delle informazioni personali,
5. La personalità,
6. L'intimità

Nonostante questa possibile definizione, Lukács (2016) sostiene che una definizione esauriente del concetto di privacy è impossibile da illustrare.

Secondo quanto riporta il GDPR all'art. 4, paragrafo 1, il dato personale è *“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”.

Come affermato da Bassini (2023), non è possibile trattare la materia della privacy, senza considerare le dinamiche tecnologiche. Con l'avvento dell'era digitale, i dati non sono più trasmissibili solamente fisicamente, ma anche attraverso canali online: il dato assume così anche una dimensione digitale.

In questo modo, la nozione di privacy si arricchisce, aumentando ancora di più la sua ampiezza.

Secondo gli studi di Goldfarb & Tucker (2012b), Nissenbaum (2004) e Acquisti et al. (2015) (si vedano Goldfarb e Que 2023, p. 270), le preoccupazioni legate alla privacy tendono ad aumentare nel tempo e man mano che i consumatori riscontrano pratiche di condivisione dei dati più sofisticate. Nonostante questa crescita, il flusso di informazioni personali fornite dai consumatori sembra non fermarsi. Questo fenomeno è nominato come “il paradosso della privacy”. Con questo termine si vuole rappresentare la dicotomia tra il desiderio alla privacy e la facile e volontaria divulgazione dei propri dati personali.

Athey et al. (2017) affermano che il paradosso della privacy è la conseguenza di tre fattori principali: “small money”, “small costs” e “small talk”.

Per quanto riguarda il concetto di small money; lo studio sostiene che in cambio di una piccola remunerazione, le persone sono più propense a condividere i propri dati anche se dichiarano di tenere alla propria privacy. Per sostenere questa tesi, essi sottopongono ad un campione di studenti un questionario in cui si richiedono i dati dei loro amici. Il 50% degli aderenti riceverà un piccolo incentivo (una pizza da condividere), mentre l'altro 50% non avrà alcuna remunerazione. Il risultato è quello previsto; un piccolo incentivo, come una pizza, influisce in maniera positiva nel fornire dati personali.

Small cost, invece si riferisce a come fretta e distrazione possano influenzare la condivisione dei propri dati. A tal proposito, lo studio di Athey et al. (2017), esegue un ulteriore esperimento. In questo caso, ai partecipanti è chiesto di scegliere tra quattro portafogli digitali. Il risultato dimostra che a seconda della posizione in cui vengono presentate le scelte, le persone condividono più facilmente i propri dati personali.

Infine, small talk, si riferisce al fenomeno secondo cui nonostante l'introduzione di politiche o opzioni che aumentino la privacy, spesso il cittadino non se ne avvale. Tale evento è la risultante di due principali fattori: difficoltà nel comprendere la procedura e ignoranza delle nuove politiche.

A questi studi riguardanti il cosiddetto paradosso della privacy, si aggiunge quello di Barnes (2006), la quale afferma che tale fenomeno è facilmente osservabile nel contesto dei social media, dove soprattutto adolescenti, condividono le proprie informazioni e dati sensibili.

1.1.2 La distinzione tra privacy e il dato personale

È importante sottolineare la fondamentale differenza tra la nozione di privacy e quella di dato personale. Nonostante spesso possano essere confusi ed interscambiati, vanno a identificare concetti diversi.

Chang (2011) chiarisce che il dato personale è un fatto oggettivo, come ad esempio il nome o l'indirizzo di domicilio, mentre la privacy è un concetto normativo. In altri termini, il dato personale descrive un fatto concreto e se il contesto lo richiede, la privacy lo tutela.

1.2 Evoluzione della legislazione sulla privacy

L'evoluzione della legislazione sulla privacy è molto articolata; per questo motivo nel paragrafo che segue si cercherà di ripercorrere le tappe normative più significative.

I primi a trattare il concetto di privacy sono Warren e Brandeis (si veda Bratman 2001, p. 629-630). Essi sostenevano che doveva essere protetto il diritto dell'individuo di decidere quale suo pensiero e fatto potesse essere pubblicato. Ricorre alla già esistente azione legale per diffamazione non era sufficiente, in quanto non veniva considerata la lesione a sentimenti ed emozioni. Per questo motivo, una legislazione che potesse comprendere un'aggravante anche per la sofferenza interiore era necessaria.

Le prime protezioni date dalla legislazione italiana, invece, arrivano nel 1947 con la formulazione della Costituzione Italiana, dove nell'Articolo 2 si afferma che “La Repubblica riconosce e garantisce i diritti inviolabili dell'uomo”.

Secondo quanto affermato da Pace (2010), tra i diritti inviolabili citati nell'articolo vi è compreso “il diritto al proprio decoro, rispettabilità, riservatezza, intimità e reputazione”. In questi termini si fa riferimento ad una maggiore tutela, che comprende anche la dimensione morale e relazionale dell'uomo che dunque oltrepassa quella fisica, proprio come affermato anche da Warren e Brandeis.

L'articolo 8 della Convenzione Europea dei Diritti dell'Uomo (CEDU, 1950) riconosce il diritto al rispetto della vita privata e familiare, includendo in questa tutela anche il domicilio e la corrispondenza.

L'articolo rappresenta, un riconoscimento formale del diritto alla privacy. Inoltre, al comma secondo dell'articolo 8 CEDU, si sottolinea che tale diritto non è assoluto, in quanto le autorità pubbliche possono interferire se: previsto dalla legge, necessario e in misura proporzionata.

La Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale numero 108 (1981), offre un'ulteriore disciplina al diritto della privacy.

Tale Convenzione è stata redatta al fine di garantire ad ogni persona (con residenza o nazionalità in un paese che aveva aderito), il rispetto del diritto alla vita privata, in relazione al trattamento automatizzato dei dati personali.

Inoltre, all'articolo 5, si enuncia che i dati personali devono: essere raccolti lealmente e legalmente (comma a), registrati per scopi determinati (comma b), esatti (comma d), rilevanti e conservati non più a lungo del necessario (comma e).

Nel 2018, a fronte dell'evoluzione della dimensione digitale, è stata adottato un aggiornamento della Convenzione, la Convenzione 108+. In quest'ultima, all'articolo 8 comma 2 si afferma che i titolari devono fornire informazioni chiare e accessibili agli interessati prima o durante il trattamento.

Infine, l'antecedente dell'attuale GDPR è la Direttiva del Parlamento Europeo e del Consiglio 95/46/CE. Tale disciplina, come esposto all'articolo 1, aveva il fine di "tutelare le libertà e i diritti fondamentali delle persone fisiche, in particolare il diritto alla vita privata, con riguardo al trattamento dei dati personali". Essa si applicava al trattamento dei dati personali totalmente o parzialmente automatizzato.

Come riportato all'articolo 94, paragrafo 1 del GDPR, la direttiva 95/46/CE è stata abrogata il 25 maggio 2018, in concomitanza con l'entrata in applicazione del Regolamento stesso.

1.3 Il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio (GDPR)

Il General Data Protection Regulation (GDPR) è la normativa più rilevante in materia di protezione dei dati e della privacy. Si applica su qualunque organizzazione che colleziona e elabora informazioni dei cittadini dell'Unione Europea sia all'interno che all'esterno del territorio dell'Unione Europea. I principi applicabili al trattamento dei dati sono (Zaeem e Barber, 2020):

- “Liceità, correttezza e trasparenza.
- Limitazione della finalità.
- Minimizzazione dei dati.
- Esattezza.
- Limitazione della conservazione.
- Integrità e riservatezza.
- Responsabilizzazione”.

L'articolo 6 del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio stabilisce che il trattamento dei dati personali è lecito solo se sussiste almeno una delle condizioni previste dalla norma, come il consenso esplicito dell'interessato o la necessità del trattamento per il perseguimento di specifiche finalità. Inoltre, il titolare del trattamento è tenuto a fornire all'interessato tutte le informazioni relative al trattamento, tramite comunicazione scritta o altri mezzi, nel pieno rispetto del principio di trasparenza.

L'articolo 13 del Regolamento (UE) 2016/679 stabilisce che nel caso in cui i dati personali siano stati raccolti direttamente presso l'interessato, il titolare del trattamento debba fornire l'identità e i dati di contatto propri, del suo rappresentante e del responsabile della protezione dei dati. Inoltre, deve indicare le finalità del trattamento, i possibili destinatari dei dati personali e la sua intenzione di trasferire i dati a un paese terzo o a un'organizzazione internazionale. In aggiunta fornisce ulteriori informazioni per garantire un trattamento corretto e trasparente, tra cui, il periodo di conservazione dei dati, il diritto di proporre reclamo e se la comunicazione dei dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto. Qualora i dati non siano stati ottenuti presso l'interessato, in aggiunta a quanto detto finora, il titolare dovrà anche dichiarare la fonte da cui hanno origine i dati personali e l'eventualità che i dati provengano da fonti accessibili al pubblico.

Nell'articolo 18 del Regolamento 2016/679 si afferma che, per tutelare l'interessato, il diritto di limitazione del trattamento può essere esercitato quando si verifica una delle seguenti dinamiche: contestazione da parte dell'interessato dell'esattezza dei dati personali, il trattamento è illecito ma si preferisce limitarne l'uso, oppure i dati non sono più necessari al trattamento ma servono per accertare, esercitare o difendere un diritto in sede giudiziaria.

Inoltre, come riportato all'articolo 21 del Regolamento 2016/679, l'interessato ha il diritto di opporsi nei casi in cui i dati personali siano trattati ulteriormente per finalità diverse da quelle

originariamente dichiarate, ad esempio di marketing diretto o ricerca scientifica. Questo diritto rispetta il principio di limitazione della conservazione.

Per il principio di minimizzazione dei dati, questi devono essere pertinenti e limitati a quanto necessario rispetto alle finalità per cui sono trattati.

L'articolo 17 del Regolamento 2016/679 riconosce il diritto all'oblio, ovvero il diritto dell'interessato di chiedere la cancellazione dei dati personali. Questo può avvenire quando i dati non sono più necessari rispetto alle finalità per le quali sono stati raccolti o sono stati trattati in modo illecito.

In seguito, l'articolo 32 tratta la sicurezza del trattamento. Rispetto alla protezione dei dati, il titolare del trattamento ha l'obbligo di mettere in atto misure tecniche adeguate, ad esempio la pseudonimizzazione e la cifratura dei dati personali. L'obiettivo è garantire che siano trattati solo i dati personali necessari per la specifica finalità, al fine di soddisfare i requisiti di integrità e riservatezza. Altre misure richieste per garantire sicurezza sono la capacità di: assicurare la riservatezza, l'integrità dei sistemi e servizi che trattano dati personali; di ripristinare i dati e l'accesso in caso di incidenti (come guasti tecnici o attacchi informatici); procedure di verifica per controllare periodicamente l'efficacia di tutte le misure adottate. Tali misure servono per fare in modo che i dati personali non siano resi accessibili a un numero indefinito di persone fisiche. In altre parole, si cerca di minimizzare i rischi per i diritti e le libertà delle persone coinvolte.

Quanto invece al titolare del trattamento, esso deve dimostrare che il trattamento è legittimo e conforme al presente regolamento. Quindi oltre all'obbligo di rispettare i principi del GDPR, deve anche essere in grado di dimostrare di averlo fatto.

1.4 Regolamento (UE) 2022/868: Data Governance Act (DGA)

Il Data Governance Act punta, tramite il riutilizzo e la condivisione di dati in determinati settori, a beneficiare i cittadini e le imprese dell'Unione Europea, aumentando l'offerta di lavoro e l'innovazione.

Nell'articolo 1 del Regolamento 2022/868 si stabilisce:

- “le condizioni per il riutilizzo, all'interno dell'Unione, di determinate categorie di dati detenuti da enti pubblici;
- un quadro di notifica e controllo per la fornitura di servizi di intermediazione dei dati;

- un quadro per la registrazione volontaria delle entità che raccolgono e trattano i dati messi a disposizione a fini altruistici; e
- un quadro per l'istituzione di un comitato europeo per l'innovazione in materia di dati.”

Questa norma è valida su dati detenuti da enti pubblici, soggetti a protezione per motivi di riservatezza commerciale, riservatezza statistica, protezione dei diritti di proprietà intellettuale di terzi e protezione dei dati personali. Sono invece escluse altre tipologie di dati detenuti da enti pubblici, per esempio quelli di proprietà di imprese pubbliche ed enti culturali e di istruzione.

Un ente pubblico, con il potere di concedere o negare l'accesso per il riutilizzo di determinati dati, deve pubblicare le regole, condizioni e la procedura di richiesta che rendono tale riutilizzo lecito. Le condizioni per il riutilizzo devono dunque essere pubbliche. Inoltre, devono essere trasparenti, proporzionate e giustificate ma non possono essere discriminatorie.

Infine, quando un ente pubblico consente il riutilizzo, può imporre delle tariffe, le quali devono avere le stesse caratteristiche delle condizioni.

L'articolo 11 del Regolamento 2022/868 dice che la notifica per i servizi di intermediazione deve contenere:

- “il nome del fornitore di servizi di intermediazione dei dati;
- lo status giuridico, la forma giuridica, l'assetto proprietario, le pertinenti società controllate e, qualora il fornitore di servizi di intermediazione dei dati sia registrato nel registro delle imprese o in un altro registro pubblico nazionale analogo, il numero di registrazione del fornitore di servizi di intermediazione dei dati;
- l'indirizzo dell'eventuale stabilimento principale del fornitore di servizi di intermediazione dei dati nell'Unione e, se opportuno, di eventuali sedi secondarie in un altro Stato membro o l'indirizzo del rappresentante legale;
- un sito web pubblico in cui sono reperibili informazioni complete e aggiornate sul fornitore di servizi di intermediazione dei dati e sulle sue attività, comprese almeno le informazioni di cui alle lettere a), b), c) e f);
- le persone di contatto e i recapiti del fornitore di servizi di intermediazione dei dati;
- una descrizione del servizio di intermediazione dei dati che il fornitore di servizi di intermediazione dei dati intende fornire e un'indicazione delle categorie elencate all'articolo 10 in cui rientra tale servizio di intermediazione dei dati;
- la data prevista di inizio dell'attività, se diversa dalla data della notifica.”

Per avviare i servizi di intermediazione dei dati, i fornitori di servizi devono inviare una notifica all'autorità competente. Quest'ultima non necessita di autorizzazione ma è obbligatoria per iniziare l'attività.

Inoltre, il rappresentante legale collabora con le autorità per dimostrare che il servizio rispetta le regole dettate dal GDPR. Sempre a tal fine, all'articolo 12 del Regolamento si afferma che le autorità verificano che il servizio sia non discriminatorio, equo e che non falsi la concorrenza. Solo dopo che la notifica è stata presentata il fornitore può avviare l'attività, a condizione che non utilizzi i dati intermediati per scopi propri e che si comporti con correttezza, trasparenza e conforme alle condizioni comunicate alle parti coinvolte.

Gli articoli 16 e 17 del Regolamento 2022/868 trattano il fenomeno dell'altruismo dei dati, quest'ultimo si rileva quando, su base volontaria e gratuita, gli interessati rendono disponibili i loro dati personali detenuti da enti pubblici a fini di altruismo. Gli Stati membri possono aiutare questo fenomeno, predisponendo politiche nazionali e stabilendo le informazioni necessarie che chiariscono il metodo con cui i dati vengono riutilizzati. Le organizzazioni che decidono di partecipare all'altruismo dei dati vengono registrate in un registro pubblico nazionale.

Secondo l'articolo 18 del Regolamento 2022/868, un'entità, per essere registrata nel registro, deve:

- “svolgere attività di altruismo dei dati;
- essere una persona giuridica costituita a norma del diritto nazionale per conseguire obiettivi di interesse generale, stabiliti nel diritto nazionale, ove applicabile;
- operare senza scopo di lucro ed essere giuridicamente indipendente da qualsiasi entità che operi a scopo di lucro;
- svolgere le proprie attività di altruismo dei dati mediante una struttura funzionalmente separata dalle sue altre attività;
- rispettare il codice di cui all'articolo 22, paragrafo 1, al più tardi entro 18 mesi dopo la data di entrata in vigore degli atti delegati di cui a tale paragrafo.”

Al momento della domanda di registrazione, l'articolo 19 del Regolamento 2022/868 stabilisce che devono essere presentati le informazioni dell'entità necessarie per essere idonei alla registrazione nel registro, tra cui il nome, lo status giuridico e l'indirizzo dello stabilimento principale dell'entità. Inoltre, l'entità deve soddisfare i requisiti di cui all'articolo 18 per presentare la domanda.

Il Comitato per l'innovazione in materia di dati, introdotto con il Regolamento 2022/868 è un organismo consultivo, creato per favorire la cooperazione tra stati membri.

L'articolo 29 del Regolamento 2022/868, stabilisce che il Comitato è composto dai rappresentanti delle autorità competenti di ogni stato membro (le quali si occupano di gestione dei dati), del comitato europeo per la protezione dei dati e da altri organismi dell'UE.

Infine, all'articolo 30 del Regolamento 2022/868, sono elencati i compiti del Comitato, tra cui:

- alla lettera a) e b) si stabilisce che il Comitato per l'innovazione in materia di dati consiglia e assiste la Commissione Europea, al fine di fornire l'applicazione delle norme del DGA,
- alla lettera c), d) e f) si spiega che il Comitato deve rendere più semplice l'interscambio dei dati tra i paesi aderenti,
- alla lettera e) e h) si afferma che il Comitato si impegna a condividere specifiche tecniche in grado di assicurare sicurezza e protezione dei dati,
- ad ogni lettera si sottolinea il ruolo di assistenza e consulenza da parte del Comitato nei confronti della Commissione Europea

1.4.2 GDPR e DGA, differenze e controversie

Vardanyan e Kocharyan (2022) analizzano i più recenti regolamenti sul trattamento del dato, GDPR e DGA, andando a sottolinearne equivalenze, differenze e controversie.

Essi affermano innanzitutto, che i due Regolamenti hanno scopi differenti: il GDPR, infatti, ha come obiettivo la protezione della privacy, mentre il DGA mira a promuovere la condivisione di dati.

Nonostante ciò, in entrambi i casi, la condivisione di dati è realizzata al fine di apportare un beneficio alla società e per il bene comune.

Nella loro analisi, Vardanyan e Kocharyan (2022), cercano di capire se il livello di protezione dei dati può rimanere costante anche con l'introduzione del nuovo Regolamento (UE) 2022/868.

A tal proposito, essi affermano che il DGA rischia di indebolire la tutela raggiunta con il GDPR, in quanto consente il riutilizzo dei dati senza il consenso dell'interessato. Tale possibilità diventa ancora più grave se il riutilizzo dei dati avviene per finalità commerciali. La conseguenza di quanto affermato è una diminuzione del controllo da parte dell'individuo sull'uso delle proprie informazioni personali, controllo che risiede alla base ed è l'idea fondante

del GDPR, considerato come lo strumento normativo che garantisce il diritto all'autodeterminazione informativa.

Inoltre, il Regolamento (UE) 2022/868 è in generale meno dettagliato rispetto al GDPR. Questa caratteristica aumenta la facilità con cui le aziende possano utilizzare un modello di consenso poco dettagliato e per finalità diverse da quelle affermate, come quelle commerciali sopra citate.

In conclusione, Vardanyan e Kocharyan (2022) sostengono la tesi secondo cui il DGA non solo non riesca a garantire un adeguato livello di protezione dei dati personali, ma in aggiunta, sia preoccupante dal punto di vista della tutela dei diritti fondamentali.

CAPITOLO 2:

IL VANTAGGIO COMPETITIVO DEI DATI E LA LORO REGOLAMENTAZIONE

2.1 Mercato unico digitale

Il mercato unico digitale (Digital single market - DSM), è la risultante di un processo in grado di trasformare le informazioni da contenuti valoriali a dati numerici, attraverso l'utilizzo di dispositivi tecnologici (Alpa, 2021).

Tale evento è a sua volta conseguenza di un ulteriore fenomeno, la Rivoluzione digitale, spesso indicata con il termine digitalizzazione. Alpa (2021), afferma che l'ampiezza di questo processo è ravvisabile anche da un punto di vista linguistico, attraverso l'utilizzo del suffisso "e", come ad esempio e-commerce ed e-learning.

Inoltre, l'autore sostiene che in queste dinamiche di mercato, il prezzo è una variabile secondaria, in quanto i beni e i servizi sono facilmente trasferibili. Questo fenomeno rende la legge della domanda e dell'offerta futile. La variabile che fa veramente la differenza in questo contesto è l'innovazione.

2.2 Proposte regolatrici: Digital Markets Act (DMA)

Il Regolamento (UE) 2022/1925 del Parlamento europeo e del Consiglio del 14 settembre 2022 ha principalmente due obiettivi: il primo è rendere il mercato digitale concorrenziale, equo e tale da essere un terreno fertile per le nuove imprese; il secondo è garantire la sicurezza degli utenti online.

2.2.2 Definizioni importanti

All'articolo 2 sono riportate una serie di spiegazioni chiave per la comprensione del Digital Markets Act, tra queste vi è la definizione di gatekeeper. Secondo il Regolamento (UE) 2022/1925, il gatekeeper è "un'impresa che fornisce servizi di piattaforma di base".

Sempre l'articolo 2 specifica che i servizi di piattaforme di base, sono tutti i servizi che erogano un servizio di intermediazione tra utente commerciale e utente finale.

Nello specifico, questi comprendono "a) servizi di intermediazione online; b) motori di ricerca online; c) servizi di social network online; d) servizi di piattaforma per la condivisione di video;

e) servizi di comunicazione interpersonale indipendenti dal numero; f) sistemi operativi; g) browser web; h) assistenti virtuali; i) j) servizi di cloud computing; servizi pubblicitari online”

Nonostante ciò, non tutte le imprese che offrono servizi di piattaforme di base possono essere definite gatekeeper. Per un’adeguata distinzione tra questi e gli altri operatori, l’articolo 3 stabilisce che possono essere definiti tali solo se soddisfano cumulativamente i seguenti fattori:

- “ha un impatto significativo sul mercato interno;
- fornisce un servizio di piattaforma di base che costituisce un punto di accesso (gateway) importante affinché gli utenti commerciali raggiungano gli utenti finali; e
- detiene una posizione consolidata e duratura, nell'ambito delle proprie attività, o è prevedibile che acquisisca siffatta posizione nel prossimo futuro.”

In aggiunta, sempre all’articolo 3, vengono elencati alcuni criteri economici.

Un’impresa ha un impatto importante nel mercato del paese quando raggiunge almeno 7,5 miliardi di euro di fatturato nei paesi dell’Unione Europea negli ultimi tre anni o se ha un fair value di 75 miliardi. In entrambi i casi, l’azienda deve operare con il proprio servizio di base al minimo in tre paesi membri dell’Unione Europea.

Inoltre, in riferimento al punto b) del primo comma, l’impresa deve avere perlomeno 45 milioni di utenti attivi mensilmente e 10000 utenti commerciali. Questi ultimi però devono essere annuali e non mensili.

Infine, un’azienda può affermare di detenere o di potere acquisire una posizione stabile nel mercato europeo, se il numero di utenti attivi precedentemente indicato, sia stato raggiunto per almeno tre anni.

Un’ulteriore definizione importante al fine di comprendere il contenuto del Regolamento è quella che riguarda la figura dell’utente commerciale. Esso è descritto all’articolo 2 del DMA, come la persona fisica o giuridica che al fine di esercitare la propria attività utilizza i servizi di piattaforme di base. L’utente finale, invece, è colui che utilizza il servizio offerto dal gatekeeper non a fini commerciali ma personali.

2.2.3 Le norme del DMA: obblighi e divieti del gatekeeper

In relazione ai compiti dei gatekeepers, essi possiedono obblighi e divieti.

Gli articoli 5 e 6 del Regolamento (UE) 2022/1925 indicano le pratiche che devono essere seguite per evitare di incorrere in comportamenti sleali e non concorrenziali e quelle che non devono essere perseguite.

In primo luogo, i gatekeepers possiedono l'obbligo di consentire agli utenti commerciali la libertà di utilizzare ulteriori piattaforme per la promozione del proprio servizio. Le aziende, infatti non sono limitate all'utilizzo di un unico gatekeeper.

In secondo luogo, gli utenti commerciali hanno il diritto di visionare e accedere ai propri dati generati nelle piattaforme definite gatekeeper. Quest'ultimo deve dunque permettere l'analisi agli usufruttori dei servizi che erogano. A questo proposito, il gatekeeper deve garantire anche gli strumenti per svolgere tutte le verifiche delle campagne di promozione erogate nelle proprie piattaforme. È dunque obbligatoria la trasparenza.

Infine, il gatekeeper consente a soggetti terzi la possibilità di collaborare con i propri servizi, se vi è questa necessità.

Come anticipato, i gatekeepers hanno anche diversi divieti.

Innanzitutto, non devono favorire i propri prodotti o servizi rispetto a quelli degli altri utenti commerciali che utilizzano la piattaforma. La non ottemperanza di questo divieto causerebbe comportamenti preferenziali non leciti.

Inoltre, è vietato tenere traccia delle attività degli utenti finali del gatekeeper, oltre la propria piattaforma. In aggiunta, non possono utilizzare i dati personali degli utenti a fini commerciali, senza il loro consenso. L'utilizzatore della piattaforma, infatti, ha il diritto alla proprietà dei propri dati, i quali possono essere usati solo con il suo consenso esplicito.

Ad arricchire la lista dei divieti, vi è il fatto che il gatekeeper deve lasciare la libertà nella scelta del sistema di pagamento nella propria piattaforma. L'utente, per comprare un bene o servizio, deve avere la libertà di scegliere tra differenti metodi di pagamento e non essere vincolato a quello di proprietà del gatekeeper.

Infine, deve rendere le proprie app preinstallate nei dispositivi, disinstallabili con facilità.

2.3 Economia della privacy digitale

I dati nel tempo hanno incrementato la loro utilità anche in campo economico. Grazie al processo di trasformazione dei dati in formato digitale, i vari costi di collezione e gestione di essi sono diminuiti (Goldfarb e Tucker 2019). Secondo gli studi di Goldfarb e Tucker (2019), il prezzo online di un prodotto è più basso rispetto allo stesso bene venduto offline. Inoltre, la riduzione dei costi online ha a sua volta ridotto la dispersione dei prezzi (ovvero una variazione di prezzo per lo stesso prodotto venduto da diversi venditori), anche se non l'ha eliminata.

Questo evento ha aiutato la diffusione di prodotti e servizi personalizzati ad un costo minore. L'accesso a questi servizi ad un prezzo migliore, non solo aumenta significativamente il benessere dei consumatori, ma anche le imprese ne possono beneficiare. Queste, infatti, possono aumentare i loro profitti utilizzando i dati raccolti. In questo modo, migliorano a sua volta i prodotti e servizi offerti ai clienti, in modo che possano rispecchiare ancora di più le loro necessità.

I dati sono considerabili come informazioni, le quali riducono l'incertezza su risultati sconosciuti. Possono essere copiate quasi a costo zero e senza perdere qualità, per questo motivo, quando non ci sono limiti nell'accesso dei dati, le informazioni non concorrono tra di loro. Il flusso di questi dati non ha solo effetti positivi, ma talvolta può causarne anche di negativi.

I benefici che una grande quantità di dati può dare ai consumatori sono diversi. Tra questi si identificano la pubblicità personalizzata, i prodotti e i servizi mirati. Inoltre, quando le aziende hanno accesso ai dati, i prezzi possono abbassarsi. Lo studio di Kummer e Schulte (2019) svolto sui dati di 300.000 applicazioni di Google Play Store, stabilisce che le applicazioni a pagamento chiedono meno dati ai consumatori rispetto alle applicazioni gratuite.

Come accennato, grazie all'accesso di dati da parte delle aziende, queste ultime possono personalizzare i loro prodotti e servizi per il cliente. In questo modo, le imprese, riducono il carico di informazioni, e forniscono ciò di cui il consumatore potrebbe aver bisogno in quell'esatto momento, agevolando il processo decisionale dell'utente finale.

A dimostrazione dell'importanza della personalizzazione di beni e servizi per i consumatori vi è un esperimento condotto da Sun et al. (2024). Lo studio viene condotto su 555.800 clienti della piattaforma "Alibaba". La ricerca dimostra che vietando l'uso di dati personali nell'algoritmo di raccomandazione della homepage, si registra una diminuzione del 75% nel tasso di click sui prodotti raccomandati e una diminuzione del 33% sul comportamento di navigazione sulla homepage, comportando a sua volta una riduzione degli acquisti dell'81%. Questo risultato dimostra l'importante ruolo della personalizzazione sia per le aziende, che per i clienti, soprattutto per determinate categorie.

Solitamente, i consumatori tengono alla propria privacy per evitare la discriminazione dei prezzi, ovvero la strategia con la quale le aziende impongono prezzi diversi a seconda del consumatore. Nonostante ciò, questa strategia può, sotto determinate circostanze, portare anche

benefici a loro vantaggio. Infatti, secondo lo studio di Conitzer et al. (2012), quando mantenere la propria privacy è costoso e un monopolista ha la possibilità di applicare prezzi discriminatori per i vecchi clienti, i consumatori eviteranno di fare il loro primo acquisto. Di conseguenza, il monopolista si ritroverà ad abbassare i prezzi iniziali per incentivare l'acquisto ai consumatori. Quando invece mantenere l'anonimato è poco costoso, tutti i consumatori sceglieranno questa opzione, così facendo il profitto per le aziende sarà massimizzato.

In questa circostanza, la prima opzione va a vantaggio dei consumatori in quanto aumenta il loro surplus, la seconda al contrario è meno favorevole in quanto diminuisce il loro surplus. Invece, quando il prezzo è regolato (quindi imposto da una politica), una riduzione della privacy beneficerà sempre i consumatori in quanto comporta prezzi più bassi e una migliore personalizzazione.

Dal punto di vista aziendale, anche le imprese possono trarre vantaggio dal flusso di dati. Ad esempio, come affermato da Goldfarb e Que (2023), avendo informazioni riguardo i propri clienti, possono imporre prezzi personalizzati, ma come spiegato precedentemente, non sempre è la strategia migliore per massimizzare il proprio profitto.

Le aziende, inoltre, attraverso la raccolta di dati possono proporre pubblicità mirate, aiutando ad evitare costi in pubblicità inutili. In questo modo si incrementa l'efficacia, si aumenta il tasso di click sulle proprie campagne e si migliora la gestione della relazione con i clienti, capendo i loro bisogni e implementando strategie di fidelizzazione proattive.

Il flusso di dati ha fatto nascere i cosiddetti intermediari dei dati, i quali hanno un importante ruolo. A fornire le aziende di dati, non sono dunque solamente i consumatori, ma anche questi intermediari.

Quando un individuo decide di condividere i suoi dati, questi dati a volte possono procurare informazioni anche riguardo altri individui. Questo fenomeno viene chiamato esternalità e può essere sia negativo che positivo. Tale esternalità può accadere in tre modi: in primo luogo, quando una lista di contatti di una persona, condivide informazioni su di essa ma anche sui suoi rispettivi contatti; in secondo luogo, quando le informazioni su una persona, forniscono informazioni probabilistiche su altre e infine anche quando un individuo sceglie di non fornire informazioni, questo potrebbe rivelare comunque i suoi dati sulle attività di mercato.

Acemoglu et al. (2022) analizzano l'ipotesi di un monopolio in un mercato dei dati. In questa circostanza, a causa delle esternalità negative dei dati, esiste un equilibrio dove le aziende utilizzano in maniera eccessiva i dati. In questo modo il loro prezzo si riduce praticamente a

zero e non vi è più nessun incentivo a tenerli privati. Di conseguenza, il costo dei dati, non rispecchia più il valore della privacy che gli attribuisce il consumatore. Le esternalità spostano, dunque, il vantaggio economico dal consumatore alle aziende.

Quando, invece, un flusso di dati più ampio genera benessere per le aziende e i consumatori, queste vengono chiamate esternalità positive. Un esempio è il servizio di ricerca di Google che deriva dallo sfruttamento dei dati generati dalle attività di ricerca degli utenti. Jones e Tonetti (2020) dimostrano che i diritti di proprietà dei dati, hanno un ruolo importante nell'usare in modo efficiente la quantità di dati disponibile. Quando le aziende hanno la proprietà dei dati, questi vengono accumulati, perdendo così tutta la varietà di usi in cui potrebbero essere utilizzati se ad avere il diritto di proprietà fossero i consumatori. In questa circostanza, la privacy dei consumatori sarebbe maggiormente tutelata e le aziende beneficerebbero delle esternalità positive derivanti dai dati. Inoltre, le esternalità possono in alcuni casi ridurre la distorsione delle informazioni e incentivare il comportamento prosociale.

2.4 Antitrust e l'AGCM

In Italia, le leggi riguardanti la libera concorrenza del mercato sono tutelate dall'Autorità Garante della concorrenza e del mercato (AGCM). La legge del 10 ottobre 1990 n. 287, stabilisce che l'AGCM è responsabile della giusta applicazione dell'articolo 101 e 102 del Trattato sul Funzionamento dell'Unione Europea. L'autorità in questione, tutela quindi consumatori e imprese.

In aggiunta l'AGCM ha anche ruolo di competition advocacy. All' articolo 21 della legge 287/1990, si stabilisce che l'Autorità della concorrenza e del mercato ha il potere di segnalare anche atti promulgati dal Governo o dal Parlamento.

2.4.2 L'Art. 102 TFUE e il concetto di abuso di posizione dominante

L'articolo 102 del Trattato sul Funzionamento dell'Unione Europea (TFUE) afferma che è vietato "lo sfruttamento abusivo da parte di una o più imprese di una posizione dominante sul mercato interno o su una parte sostanziale di questo".

Ad essere illecito, dunque non è essere leader nel proprio mercato di riferimento, bensì l'abuso di questa posizione di potere. Proprio per questo motivo, alcune condotte possono essere messe in atto da tutte le imprese, ma non da quelle in posizione dominante.

In particolare, le pratiche ritenute illecite se attuate da aziende leader nel proprio mercato, come stabilito dall'articolo 102 del TFUE, consistono:

- “a) nell'imporre direttamente od indirettamente prezzi d'acquisto, di vendita od altre condizioni di transazione non eque;
- b) nel limitare la produzione, gli sbocchi o lo sviluppo tecnico, a danno dei consumatori;
- c) nell'applicare nei rapporti commerciali con gli altri contraenti condizioni dissimili per prestazioni equivalenti, determinando così per questi ultimi uno svantaggio per la concorrenza;
- d) nel subordinare la conclusione di contratti all'accettazione da parte degli altri contraenti di prestazioni supplementari, che, per loro natura o secondo gli usi commerciali, non abbiano alcun nesso con l'oggetto dei contratti stessi.”

Davanti a tale definizione, è necessario indagare anche il concetto di posizione dominante.

Azzopardi (2015) afferma che questo termine è strettamente collegato con quello di potere commerciale di mercato, in quanto un'azienda in posizione dominante permette di alterare e danneggiare il mercato in cui l'impresa opera assumendo comportamenti indipendenti a quelli dei concorrenti. In particolare, Azzopardi (2015), fa riferimento al potere di mercato sostanziale, il quale si dirama in due tipologie principali: il potere sui prezzi e il potere di escludere i concorrenti. Nonostante tale terminologia non tenga in considerazione il concetto di redditività, l'autore spiega che la giurisprudenza non la ritiene una variabile determinante per definire una posizione dominante.

Nelle linee guida indicate dalla Commissione della Gazzetta Ufficiale, C 45 del 24/02/2009, la posizione dominante è una situazione di potere economico in grado di modificare la giusta concorrenza di mercato in quanto immune alle decisioni strategiche di prezzo delle altre imprese. Questa dinamica avviene in una circostanza in cui l'impresa può “mantenere i prezzi al di sopra del livello concorrenziale” “per un periodo di tempo significativo”.

Inoltre, si aggiunge che per valutare la posizione di dominanza di un'impresa, bisogna considerare anche: il potere di mercato dei concorrenti effettivi, l'ingresso di concorrenti potenziali e il potere contrattuale dei consumatori.

Infine, per determinare una posizione dominante, bisogna considerare il mercato in cui l'azienda opera. Questo, è definito mercato rilevante.

Secondo quanto determinato nella Comunicazione della Commissione C 372 del 09/12/1997, il mercato rilevante può essere analizzato da una prospettiva di prodotto e da una prospettiva geografica.

Il mercato rilevante di prodotto “comprende tutti i prodotti e/o servizi che sono considerati intercambiabili o sostituibili dal consumatore, in ragione delle caratteristiche dei prodotti, dei loro prezzi e dell'uso al quale sono destinati”.

Mentre, quello geografico “comprende l'area nella quale le imprese in causa forniscono o acquistano prodotti o servizi, nella quale le condizioni di concorrenza sono sufficientemente omogenee e che può essere tenuta distinta dalle zone geografiche contigue perché in queste ultime le condizioni di concorrenza sono sensibilmente diverse”.

In conclusione, i comportamenti considerati illeciti all’art. 102 del Trattato sul Funzionamento dell’Unione Europea sono imputabili solo alle aziende che godono di una posizione dominante. Questa è intesa come il potere di mercato che permette ad un’azienda di agire indipendentemente dai propri concorrenti. Tale potere deve essere considerato o da un punto di vista di prodotto o geografico.

2.4.3 Concetto di “self-preferencing”

Bougette et al. (2022) affermano che un comportamento denominato “self-preferencing”, avviene quando un’impresa in posizione dominante altera la concorrenza in un mercato collegato, avvantaggiando sé stessa.

Un’ ulteriore specifica è che queste aziende solitamente possiedono piattaforme nella quale operano anche terze parti. Un esempio chiarificatore è la piattaforma App store, la quale è proprietà di Apple, ma nella quale oltre alle applicazioni della casa madre ve ne sono anche di aziende esterne.

L'impresa in posizione di dominanza può, in questo senso, operare solo nel mercato a valle (dunque a contatto con l’utente finale) oppure essere verticalmente integrata.

CAPITOLO 3:

Case study - A561 - APP TRACKING TRANSPARENCY DI APPLE

3.1 Le parti

Considerando quanto riportato nel documento ufficiale del caso, l'impresa segnalata è Apple Inc. (Apple). L'azienda in questione vede la propria sede principale situata in Cupertino, California, dunque è una società di diritto statunitense. Essa è "a capo dell'omonimo gruppo attivo nella progettazione, produzione e commercializzazione di dispositivi per la comunicazione mobile e multimediale, personal computer e dispositivi audio-video con i marchi Apple e Beats, nonché nella vendita di un'ampia gamma di software, servizi, periferiche e soluzioni di networking correlate e, ancora, di applicazioni e contenuti digitali di soggetti terzi."

Inoltre, l'azienda è quotata in Borsa a New York e il suo fatturato netto nel 2022 (anno rilevante per l'accusa), ammontava a circa 394,33 miliardi di dollari, pari a circa 358 miliardi di euro.

La multinazionale controlla anche Apple Italia S.r.l, responsabile di servizi di supporto vendite e marketing in Italia, e Apple Distribution International Ltd. Quest'ultima ha sede a Cork, Irlanda e si occupa dell'Apple Online Store e l'app mobile App Store.

L'impresa segnalante, dunque l'attore del caso, è invece omessa per garantire la sua privacy.

Infine, l'attività che indaga il caso, è l'Autorità Garante della Concorrenza e del Mercato (AGCM), già analizzata nel paragrafo 2.4 del presente elaborato.

3.2 Analisi del caso

Con l'introduzione della politica ATT, Apple è stata accusata di imporre regole più restrittive ai concorrenti rispetto a sé stessa. In particolare, l'Autorità Italiana Antitrust, nel caso A561, menziona la "finestra a comparsa" e l'interfaccia di programmazione SkadNetwork.

La "finestra a comparsa", che appare agli utenti, ha il fine di ottenere il consenso di tracciare i dati di navigazione in internet da parte di app terze. La finestra in questione pone in maggior evidenza l'opzione di negazione del consenso al tracciamento dei dati rispetto all'ipotesi di concederlo. Inoltre, cerca di diffondere preoccupazione aggiungendo il termine "tenere traccia",

senza dare nessuna spiegazione sul suo effettivo significato e non menziona i vantaggi per gli utenti alla pubblicità personalizzata.

Per le app sviluppate direttamente da Apple, invece, si utilizza un'impostazione contraria a quanto detto finora. Si pone in primo piano l'opzione di accettazione del consenso e, come oggetto del consenso, vengono inseriti i "servizi personalizzati" al posto del "tenere traccia dell'attività di navigazione degli utenti".

Un'altra grande differenza è nel cosiddetto "doppio consenso esplicito". Con tale terminologia si vuole indicare il fatto che anche qualora diverse app siano dello stesso sviluppatore e l'utente dia il consenso ad una di queste app, il consenso al tracciamento non potrà essere considerato anche per le altre applicazioni. Dunque, ogni app ha la sua richiesta di tracciamento alle attività. Questo, appunto, non è previsto per le app sviluppate da Apple, la quale, con il consenso da parte dell'utente, potrà utilizzare i dati su tutte le attività nelle app di terzi indipendentemente da l'autorizzazione al tracciamento ottenuta dagli sviluppatori. Quanto detto finora ha portato un calo significativo dei consensi nelle app dei concorrenti disponibili su App Store.

Anche per quanto riguarda l'attività di misurazione degli effetti delle campagne, la differenza è evidente. SkadNetwork, l'interfaccia di programmazione messa a disposizione di Apple per i terzi al fine di misurare l'efficacia delle loro campagne pubblicitarie, presenta delle problematiche tecniche che rendono lo strumento praticamente inutile rispetto a quello di Apple (Apple Ads Attribution). La piattaforma consente l'accesso ai dati di conversione dopo 24-48 ore rispetto ad Apple che ce l'ha immediato, per lo più, questi dati risultano confusionari e non riescono a rilevare gli effettivi gusti degli utenti, contrariamente ad Apple Ads Attribution.

3.3 I mercati di riferimento

Al fine di capire e analizzare il caso è necessario definire il mercato rilevante per l'impresa. Stando a quanto rilevato dall'Autorità Garante della Concorrenza e del Mercato, i mercati di prodotto principali in cui opera Apple Inc. sono principalmente quattro.

Il primo è "il mercato delle piattaforme per la distribuzione on-line di app per utenti del sistema operativo iOS". In questo contesto si fa riferimento ad App store, il quale è una piattaforma "two-sided", in quanto intermedia tra gli sviluppatori di app e i consumatori di applicazioni. I due operatori della piattaforma, dunque sviluppatori e consumatori, dipendono l'uno dall'altro e per questo motivo i due lati sono definiti mercati distinti.

Bisogna considerare che App store distribuisce anche applicazioni non create da iOS, ma non permette la condivisione delle proprie app con Google Play, piattaforma Android.

Apple, dunque, controlla rigidamente il suo sistema, imponendo regole agli sviluppatori di app e non offrendo applicazioni di sostituzione all'App store a nessun dispositivo iOS.

Dunque, "il mercato delle piattaforme per la distribuzione on-line di app per utenti del sistema operativo iOS" è di portata globale e si trova in una posizione dominante.

Il secondo è "Il mercato dello sviluppo e distribuzione di app". Apple, infatti, oltre a possedere App Store, sviluppa e distribuisce applicazioni. In questo modo, essa è in concorrenza anche con altri sviluppatori. Nonostante ciò, è in una posizione di vantaggio competitivo rispetto agli altri sviluppatori, in quanto possiede una posizione dominante e può impartire politiche come la ATT.

Tra i vari modelli di monetizzazioni delle applicazioni, (a pagamento, ad-supported che guadagna dalla pubblicità e freemium con un programma gratuito e uno a pagamento), le regole di Apple impattano principalmente il modello ad-supported e freemium. Tale fenomeno è dovuto al fatto che la politica ATT limita il tracciamento degli utenti e di conseguenza anche l'efficacia delle pubblicità in app.

Da un punto di vista geografico, questo mercato ha una portata europea.

Il terzo riguarda "i mercati della pubblicità online". In questo caso è importante considerare che con l'entrata in vigore della politica ATT, i guadagni derivanti dalla pubblicità online degli sviluppatori concorrenti di Apple sono diminuiti di molto. Spiegazione di tale evento è che la nuova regolamentazione Apple restringe la possibilità di raccolta dei dati, ma questi sono il mezzo chiave per offrire targeting pubblicitario e misurare l'efficacia delle proprie pubblicità. Infine, Apple Search Ads (ASA), risente meno dell'influenza dell'ATT policy, in quanto Apple controlla sia i dati sia la piattaforma.

Questo terzo mercato ha dimensione nazionale, con portata linguistica massima dentro lo Spazio Economico Europeo (SEE). Anche in questo caso, Apple non possiede una posizione dominante.

Infine, l'ultimo mercato rilevante è "Il mercato della produzione e vendita di dispositivi mobili di alta gamma". In questo caso, la nuova regolamentazione Apple, porta un incremento nella fidelizzazione degli utenti iOS, fattore che spinge i consumatori a non comprare dispositivi concorrenti, aumentando quindi le sue vendite.

Quest'ultimo mercato rilevante ha dimensioni SEE.

3.4 Effetti e conseguenze economiche del caso

L'implementazione di questa politica da parte di Apple ha avuto effetti sui ricavi e i costi relativi ai servizi di cui abbiamo parlato sopra. Questo perchè la raccolta di dati personali da parte dell'azienda permette di implementare una strategia di targeting dettagliata e un'efficace misurazione delle performance (Aridor et al., 2025).

La politica ATT dava la possibilità ai consumatori di negare il consenso di lasciarsi tracciare le attività di navigazione su internet dalle applicazioni, questo ha causato sia l'impossibilità di utilizzare questi dati per campagne mirate sia l'incapacità di capire se un annuncio ha portato ad un acquisto.

Aridor et al. (2025) hanno indagato l'impatto della politica ATT sull'efficacia pubblicitaria di Meta e Google. Secondo lo studio, le aziende che dipendevano maggiormente da Meta hanno visto una riduzione del 37,1% dei propri ricavi, mentre quelle più dipendenti da iOS del 40,1%.

In generale, Meta è stata molto più colpita di Google dalla politica ATT. La motivazione di tale differenza risiede nel fatto che Meta utilizza principalmente dati off-platform (ovvero raccolti su altri siti e app), mentre Google basa le sue pubblicità su dati raccolti on-platform (ovvero nella piattaforma stessa). La politica ATT, infatti, non rende possibile la raccolta di dati off-platform.

Nella seconda parte dello studio Aridor et al. (2025) hanno cercato di capire come sono state riallocate le spese pubblicitarie tra Meta e Google. Il risultato è che Meta ha perso il 4,4% della sua quota di mercato pubblicitaria, mentre in Google è aumentata.

La ricerca nota che una parte della quota di mercato passa da Meta a Google. Sebbene sia stato evidenziato come l'ATT ha cambiato quali piattaforme e tipi di pubblicità gli inserzionisti utilizzano, i risultati mostrano come gli inserzionisti dipendenti da Meta sono ancora colpiti nel medio termine, soprattutto a causa della riduzione nell'acquisizione di nuovi clienti.

Lo studio di Aridor et al. (2025) dimostra che il tasso di click osservato in seguito all'implementazione della politica ATT è diminuito del 36,6% per le campagne pubblicitarie di Meta, mentre il costo per conversione è aumentato del 73,2%. Inoltre, si aggiunge che gli inserzionisti più piccoli sono maggiormente svantaggiati rispetto quelli di grandi dimensioni.

Un ulteriore studio sugli effetti della politica ATT è stato condotto da Kesler (2023). L'autore ricerca un'evidenza tangibile dell'aumento di applicazioni a pagamento in seguito alla regolamentazione sulla privacy introdotta da Apple.

Innanzitutto, Kesler (2023) dimostra che il numero di app a pagamento nel 2021 è aumentato del 6,4% mentre quello di applicazioni con pagamenti in app ha registrato un incremento del 11,8%. In particolare, a seguito della politica ATT, le applicazioni a pagamento hanno riscontrato un tempestivo aumento del 4% fino ad arrivare al citato 6,4% a fine anno.

In aggiunta, dallo studio risulta che nel trimestre seguente alla decisione di utilizzare la politica ATT, il numero di applicazioni su App Store è diminuito di molto, mentre su Google play l'andamento è rimasto costante. Gli sviluppatori di applicazioni, quindi, non trovavano più vantaggioso renderle disponibili su App Store. Infatti, se nel 2020 venivano introdotte circa 39.300 app, nel 2021 con la politica ATT ne vengono introdotte 35.900, registrando un calo del circa l'8,65%.

La nuova regolamentazione Apple, dunque, ha causato un aumento dei costi per i consumatori che ritrovano molte più app a pagamento rispetto a prima della sua introduzione.

Secondo l'Autorità Antitrust Italiana, caso A561, Apple, con l'implementazione di questa politica, provoca un aumento di oltre il 150% del "costo medio per azione" (CPA), riguardante l'acquisto di spazi pubblicitari sulle app dei concorrenti, nel territorio europeo. Questa riduzione ha fatto sì che ci fossero meno acquisti per gli spazi pubblicitari, riducendo di oltre il 50% i ricavi degli sviluppatori (Facebook ha registrato una perdita di 9,087 miliardi di euro). Sono inoltre aumentati dal 17% al 58% i download da App Store e anche i relativi ricavi pubblicitari.

3.5 Le conclusioni del caso

In conclusione, Apple vanta una posizione dominante nel mercato delle piattaforme per la distribuzione on-line di app per utenti del sistema operativo iOS. Ai sensi dell'articolo 102 del TFUE, Apple attua delle condotte identificate come abuso della propria posizione dominante. Come dichiarato nel documento ufficiale rilasciato dall'AGCM, la società in questione adotta delle politiche discriminatorie verso gli altri concorrenti e sviluppatori dell'App Store, avvantaggiando sé stessa grazie al meccanismo di self-preferencing.

Apple, infatti, attraverso la politica ATT, limita la raccolta dei dati dei consumatori ai concorrenti ma non a sé stessa. Questa condotta è discriminatoria e auto-preferenziale, in quanto applica due tipologie di privacy diverse, una a vantaggio della propria società e l'altra a svantaggio dei concorrenti. Inoltre, tale tesi è avvantaggiata dall'obbligo per i concorrenti di

utilizzare SkadNetwork, che, come già spiegato in precedenza, è di qualità inferiore rispetto ad Apple Ads Attribution.

L'ATT, tramite queste politiche discriminatorie, riduce la capacità di profilazione degli utenti da parte dei concorrenti che propongono app gratuite, spingendoli a produrre applicazioni a pagamento. Ma se le app concorrenti per ottenere un adeguato trattamento dei dati, devono essere a pagamento, diventano meno competitive rispetto alle app Apple. Una spiegazione a questo fenomeno è il fatto che il consumatore preferirà non spendere denaro per un'applicazione.

Questa circostanza rafforza ulteriormente la posizione dominante di Apple, in quanto i clienti preferiscono le app gratuite di Apple rispetto a quelle a pagamento di sviluppatori terzi.

In aggiunta, tale condotta è danneggiante non solo per il mercato nazionale ma anche europeo.

Nel Bollettino n.42 del 28 ottobre 2024 dell'Autorità Garante della Concorrenza e del Mercato, si stabilisce che il termine di conclusione del processo è fissato per il 31 ottobre 2025.

CONCLUSIONE

Il presente elaborato aveva l'obiettivo di comprendere in che modo il dato personale venga tutelato e se esso possa rappresentare un vantaggio competitivo per le aziende.

Innanzitutto, si è scoperto che lo Stato italiano e la Comunità Europea stanno lavorando al fine di fornire una tutela alle informazioni personali. Davanti ad una rapida evoluzione digitale, le varie regolamentazioni proposte vengono aggiornate continuamente al fine di risolvere le nuove esigenze.

Il GDPR sostiene che il dato personale ha bisogno di tutela in quanto è un bene prezioso se utilizzato a beneficio dell'individuo e della società. A tal fine la regolamentazione afferma che il dato personale può essere trattato solamente con l'esplicito consenso da parte dell'interessato. Inoltre, fondamentale è la trasparenza nelle finalità di trattamento del dato. In aggiunta, il GDPR fa riferimento al diritto di cancellazione dei propri dati quando questi non sono più utili alla società. In questo senso si può affermare che con l'entrata in vigore del GDPR c'è una maggiore tutela delle informazioni personali.

Accanto a questa politica, vi è il Data Governance Act, il quale punta a promuovere la condivisione di dati personali in quanto considerati utili positivamente per la società. Questa politica, infatti, contrariamente al GDPR permette il ritrattamento del dato senza l'esplicito consenso del consumatore.

In conclusione, al primo quesito, dunque, si può affermare che il dato è tutelato da diverse Regolamentazioni, le quali lo individuano come un bene da proteggere e valorizzare.

Considerando, poi, se il dato personale possa rappresentare un vantaggio competitivo per le imprese, la risposta non può che essere positiva.

Attraverso lo studio del caso Apple Inc. e la sua politica App Tracking Transparency (ATT), si è messo in evidenza che un facile accesso ai dati rende l'azienda economicamente e competitivamente più forte. La possibilità di poter consultare una grande quantità di dati, infatti, semplifica il processo di avvicinamento del potenziale consumatore. Infatti, una migliore conoscenza di esso consente una pubblicità mirata più efficace.

A sostegno di tale tesi, nel caso studio è stato dimostrato come l'accesso facile al dato ha permesso all'azienda di vincere contro la concorrenza, aumentando le proprie vendite e diminuendo il numero di imprese concorrenti, rafforzando così la propria posizione.

In conclusione, dunque, il dato personale è un bene prezioso per la società. Per questo motivo è tutelato da diverse Regolamentazioni, tra cui il GDPR e il DGA e il suo facile accesso rappresenta un chiaro vantaggio competitivo per le aziende, capace di incidere sul posizionamento nel mercato.

BIBLIOGRAFIA

- Acemoglu, D., Makhdoumi, A., Malekian, A., & Ozdaglar, A. (2022). Too much data: prices and inefficiencies in data markets. *American Economic Journal: Microeconomics*, 14(4), 218-256.
- Alpa, G. (2021). Il mercato unico digitale. *Contratto e impresa Europa*, (1), 1-23.
- Aridor, G., Che, Y. K., Hollenbeck, B., McCarthy, D., & Kaiser, M. (2025). Evaluating the impact of privacy regulation on e-commerce firms: evidence from apple's app tracking transparency. *Management Science* (forthcoming).
- Athey, S., Catalini, C., & Tucker, C. (2017). The digital privacy paradox: small money, small costs, small talk (No. w23488). *National Bureau of Economic Research*.
- Autorità Garante della Concorrenza e del Mercato, Bollettino n.42 del 28 ottobre 2024
- Autorità Garante della Concorrenza e del Mercato, Provvedimento n.30620 del 2 maggio 2023 (codice A561)
- Azzopardi, A. (2015). 'Dominant Position': a term in search of meaning. *The Cartels and Leniency Review*, 2.
- Barnes, S. B. (2006). A privacy paradox: social networking in the United States. *First Monday*.
- Bassini, M. (2023). Il diritto costituzionale alla privacy nel prisma dell'evoluzione tecnologica. *Diritto Costituzionale*, (2023/1).
- Bratman, B. (2001). Brandeis and Warren's the right to privacy and the birth of the right to privacy. *Tenn. L. Rev.*, 69, 623-651.
- Bougette, P., Budzinski, O., & Marty, F. (2022). Self-preferencing and competitive damages: a focus on exploitative abuses. *The Antitrust Bulletin*, 67(2), 190-207.
- Chang, Y. (2011). The distinction between 'privacy' and 'personal information' issues of personal information protection act in Japan. *Tokyo City University*.
- Conitzer, V., Taylor, C. R., & Wagman, L. (2012). Hide and seek: costly consumer privacy in a market with repeat purchases. *Marketing Science*, 31(2), 277-292.
- Convenzione Europea dei Diritti dell'uomo, 1950
- Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, 1981, n. 108
- Convention for the protection of individuals with regard to the processing of personal data, 2018, n. 108+
- Costituzione Italiana, 1947
- Direttiva del Parlamento Europeo e Consiglio (CE) n. 95/46 del 24 ottobre 1995 relativa alla "tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati"

- Goldfarb, A., & Que, V. F. (2023). The economics of digital privacy. *Annual Review of Economics*, 15(1), 267-286.
- Goldfarb, A., & Tucker, C. (2019). Digital economics. *Journal of Economic Literature*, 57(1), 3-43.
- Jones, C. I., & Tonetti, C. (2020). Nonrivalry and the economics of data. *American Economic Review*, 110(9), 2819-2858.
- Kesler, R. (2023). The impact of Apple's App Tracking Transparency on app monetization. *SSRN Working Paper 4090786*.
- Kummer, M., & Schulte, P. (2019). When private information settles the bill: money and privacy in Google's market for smartphone applications. *Management Science*, 65(8), 3470-3494.
- L. 10 ottobre 1990, n. 287 - Norme per la tutela della concorrenza e del mercato
- Lukács, A. (2016). What is privacy? The history and definition of privacy. 256-265.
- Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016
- Regolamento (UE) 2022/868 del Parlamento europeo e del Consiglio del 30 maggio 2022
- Regolamento (UE) 2022/1925 del Parlamento europeo e del Consiglio del 14 settembre 2022
- OJ N. C372, 09/12/1997, pp. 0005 - 0013
- OJ C 45, 24/2/2009, pp. 7–20
- Pace, A. (2010). Dai diritti del cittadino ai diritti fondamentali dell'uomo. *Rivista Aic*, 4, 1-22.
- Sun, T., Yuan, Z., Li, C., Zhang, K., & Xu, J. (2024). The value of personal data in internet commerce: a high-stakes field experiment on data regulation policy. *Management Science*, 70(4), 2645-2660.
- Trattato sul Funzionamento dell'Unione Europea
- Vardanyan, L., & Kocharyan, H. (2022). The GDPR and the DGA proposal: are they in controversial relationship?. *European Studies–The Review of European Law, Economics and Politics*, 9(1), 91-109.
- Zaem, R. N., & Barber, K. S. (2020). The effect of the GDPR on privacy policies: recent progress and future promise. *ACM Transactions on Management Information Systems (TMIS)*, 12(1), 1-20.