

UNIVERSITÀ DEGLI STUDI DI PADOVA

DIPARTIMENTO DI DIRITTO PUBBLICO INTERNAZIONALE E COMUNITARIO

Corso di laurea *Triennale* in
Diritto e Tecnologia



ANALISI COMPARATIVA DELL'INFORMATIVA PRIVACY E DEI CODICI ETICI DI GOOGLE, META E LINKEDIN

Relatore: prof. CLAUDIO SARRA

Laureando: LORENZO FREGNAN

Matricola N. 2109170

A.A. 2025/2026

INDICE

INTRODUZIONE.....	3
CAPITOLO 1 – Quadro normativo di riferimento	
1.1 <i>Gli obblighi informativi nel Regolamento (UE) 2016/679</i>	4
1.2 <i>I principi di trasparenza, correttezza e accountability</i>	5
1.3 <i>Il ruolo delle autorità di controllo e delle linee guida interpretative</i>	6
1.4 <i>Etica d'impresa e protezione dei dati personali</i>	7
CAPITOLO 2 – Criteri e metodologia di analisi	
2.1 <i>Metodologia comparativa adottata</i>	8
2.2 <i>Criteri di analisi delle informative privacy</i>	9
2.3 <i>Criteri di analisi dei codici etici</i>	10
2.4 <i>Limiti e potenzialità dell'approccio utilizzato</i>	12
CAPITOLO 3 – Analisi di Google	
3.1 <i>Struttura e contenuti dell'informativa privacy</i>	13
3.2 <i>Trasparenza su finalità, basi giuridiche e trattamento dei dati</i>	14
3.3 <i>Analisi del codice etico e dei principi di responsabilità</i>	15
3.4 <i>Coerenza tra obblighi normativi e impegni etici dichiarati</i>	17
CAPITOLO 4 – Analisi di Meta	
4.1 <i>Struttura dell'informativa privacy e modalità di comunicazione</i>	18
4.2 <i>Trattamento dei dati personali e profilazione degli utenti</i>	19
4.3 <i>Principi etici e responsabilità sociale dell'impresa</i>	20
4.4 <i>Criticità e punti di forza nel rapporto tra diritto ed etica</i>	21
CAPITOLO 5 – Analisi di LinkedIn	
5.1 <i>Caratteristiche dell'informativa privacy</i>	23
5.2 <i>Specificità del trattamento dei dati in ambito professionale</i>	24
5.3 <i>Codice etico e tutela degli utenti</i>	25
5.4 <i>Allineamento tra trasparenza informativa ed etica aziendale</i>	27
CAPITOLO 6 – Analisi comparativa	
6.1 <i>Confronto tra le informative privacy delle tre piattaforme</i>	28
6.2 <i>Confronto tra i codici etici</i>	29
6.3 <i>Trasparenza dichiarata e trasparenza effettiva</i>	31
6.4 <i>Implicazioni per la tutela dei diritti degli utenti</i>	32
CONCLUSIONI.....	33
Sintesi dei risultati emersi	
Risposta alla domanda di ricerca	
Considerazioni critiche e prospettive future	
Fonti Bibliografiche.....	36

Introduzione

Negli ultimi anni lo sviluppo dell'economia digitale ha determinato una crescente centralità delle grandi piattaforme online nella vita quotidiana degli utenti e nel funzionamento dei mercati digitali. Servizi offerti da piattaforme come Google, Meta e LinkedIn consentono agli individui di comunicare, informarsi, lavorare e accedere a numerose risorse disponibili in rete. L'utilizzo di tali servizi comporta tuttavia la raccolta e l'elaborazione di una quantità significativa di dati personali, che rappresentano spesso una componente essenziale dei modelli di business delle piattaforme digitali.

Nel contesto europeo, la disciplina in materia di protezione dei dati personali è stata progressivamente rafforzata attraverso l'adozione del General Data Protection Regulation (GDPR). Tale regolamento ha introdotto un quadro normativo organico volto a garantire che il trattamento dei dati personali avvenga nel rispetto di principi fondamentali. Tra gli strumenti previsti dal regolamento assume particolare importanza l'obbligo informativo, che impone ai titolari del trattamento di fornire agli interessati informazioni chiare e facilmente comprensibili riguardo alle modalità, alle finalità e alle basi giuridiche del trattamento dei dati. L'informativa privacy rappresenta quindi uno strumento fondamentale per favorire la consapevolezza degli utenti e per assicurare un adeguato livello di tutela dei diritti fondamentali.

Parallelamente all'evoluzione della normativa, negli ultimi anni le imprese hanno sviluppato ulteriori strumenti di autoregolamentazione volti a rafforzare la responsabilità nella gestione dei dati personali. Tra questi assumono particolare rilievo i codici etici e le politiche interne di responsabilità aziendale, documenti che contribuiscono a definire i valori e i principi alla base delle attività organizzative. Tali strumenti rivestono un ruolo sempre più significativo nella governance delle imprese e nella costruzione di rapporti di fiducia con utenti, partner e altri stakeholder.

Alla luce di queste considerazioni, appare rilevante analizzare le modalità attraverso cui le grandi piattaforme digitali regolano e comunicano il trattamento dei dati personali. L'analisi non si limita alle informative privacy previste dalla normativa vigente, ma prende in considerazione anche i codici etici e altri strumenti di soft law adottati dalle imprese. Lo studio di tali documenti consente infatti di valutare il grado di trasparenza adottato dalle piattaforme e di verificare se, e in quale misura, gli impegni etici dichiarati risultino coerenti con gli obblighi giuridici previsti dalla disciplina in materia di protezione dei dati personali.

Il lavoro si articola in diversi capitoli. Nei primi due vengono trattati i quadri normativi di riferimento, la metodologia e criteri utilizzati, ovvero costituiscono il quadro teorico e metodologico per comprendere la disciplina e impostare l'analisi comparativa sviluppata nei capitoli seguenti, dedicati all'esame delle singole piattaforme.

CAPITOLO 1

QUADRO NORMATIVO DI RIFERIMENTO

1.1 Gli obblighi informativi del regolamento

Nel contesto del **Regolamento (UE) 2016/679**, noto come **General Data Protection Regulation** (GDPR) viene garantita la trasparenza nel trattamento dei dati personali attraverso gli obblighi informativi¹ che impongono al titolare del trattamento di fornire all'interessato informazioni chiare, trasparenti e comprensibili circa le modalità, le finalità e i diritti connessi al trattamento dei dati personali, affinché l'utente possa conoscere ed esercitare consapevolmente i propri diritti.

Gli obblighi informativi si inseriscono in un contesto più ampio di **principi fondamentali sanciti dall'articolo 5 del GDPR**, che dirige l'intero trattamento dei dati personali e ne assicura la liceità, correttezza e trasparenza. In particolare, il regolamento stabilisce che il trattamento dei dati personali deve rispettare i seguenti principi:

- trasparenza, correttezza e accountability;
- limitazione delle finalità, ossia i dati devono essere raccolti per scopi specifici e legittimi;
- limitazione della conservazione, conservando i dati solo per il tempo necessario;
- minimizzazione dei dati, raccogliendo solo ciò che è strettamente necessario;
- esattezza, mantenendo i dati aggiornati e corretti;
- integrità e riservatezza, garantendo la protezione dei dati contro eventuali accessi non autorizzati o trattamenti illeciti.

Gli obblighi informativi costituiscono quindi lo strumento principale attraverso cui il titolare realizza il principio di **trasparenza**, fornendo all'interessato tutte le informazioni necessarie per esercitare i propri diritti.

In particolare, il GDPR disciplina gli obblighi informativi attraverso tre articoli principali:

- *Art. 12*: fissa il principio generale di trasparenza, imponendo al titolare del trattamento di fornire all'interessato le informazioni in modo conciso, trasparente, intelligibile e facilmente accessibile;
- *Art. 13*: disciplina le informazioni che devono essere fornite quando i dati personali sono raccolti direttamente presso l'interessato, specificando contenuti come identità del titolare, finalità del trattamento, base giuridica, destinatari dei dati e periodo di conservazione;

¹ G. Finocchiaro, *Il Regolamento europeo sulla protezione dei dati personali*, Bologna, Zanichelli, 2017., pp. 75-101

- *Art. 14*: regola le informazioni da fornire quando i dati non sono raccolti direttamente dall'interessato, prevedendo obblighi analoghi a quelli dell'articolo 13 e ulteriori indicazioni riguardanti la fonte dei dati.

L'interpretazione degli obblighi informativi previsti dal regolamento è stata ulteriormente sviluppata dalle autorità di controllo. In particolare, il Garante per la protezione dei dati personali ha evidenziato come il principio di trasparenza non possa ritenersi soddisfatto mediante la mera predisposizione di informative formalmente corrette, ma richieda che le informazioni siano effettivamente comprensibili, accessibili e redatte con un linguaggio chiaro e semplice². Alla luce di tali considerazioni, gli obblighi informativi previsti dal GDPR assumono un ruolo centrale nel garantire l'effettività del diritto alla protezione dei dati personali, in quanto consentono agli interessati di conoscere le modalità di trattamento dei propri dati e di esercitare in modo consapevole i diritti riconosciuti dalla normativa europea.

1.2 I principi di trasparenza, correttezza e accountability

Il sistema di tutela dei dati personali introdotto dal **General Data Protection Regulation** si basa su una serie di principi generali che devono guidare qualsiasi trattamento di dati personali. Tali principi, disciplinati dall'articolo 5 del regolamento, rappresentano i criteri fondamentali ai quali i titolari del trattamento devono conformarsi per lo svolgimento delle proprie attività. Tra questi, oltre a quelli esposti poc'anzi assumono particolare rilevanza i principi di trasparenza, correttezza e accountability, che svolgono un ruolo centrale nel garantire una gestione lecita, responsabile e consapevole dei dati personali.

Il principio di **trasparenza** assume un ruolo particolarmente rilevante in un contesto in cui gli utenti spesso forniscono dati personali per accedere a servizi, a fronte di ciò impone che il trattamento dei dati personali venga svolto in modo chiaro e comprensibile per l'interessato. Ciò significa che gli utenti devono essere informati in maniera adeguata circa le modalità con cui i loro dati vengono raccolti, utilizzati e conservati. La trasparenza si concretizza, in particolare, attraverso gli obblighi informativi previsti dal regolamento, che richiedono ai titolari del trattamento di fornire informazioni facilmente accessibili e comunicate con un linguaggio chiaro e comprensibile³.

Accanto alla trasparenza, il regolamento prevede il principio di **correttezza**, secondo cui il trattamento dei dati personali deve avvenire nel rispetto dei diritti e delle aspettative legittime degli interessati. Dunque il principio di correttezza implica che i

² Garante per la protezione dei dati personali, *Linee guida in materia di trasparenza*, 2018.

³ Regolamento (UE) 2016/679 (GDPR), considerando 39 e artt. 12-14.

dati non possano essere utilizzati in modo ingannevole o in contrasto con le finalità per le quali sono stati raccolti, e richiede che il trattamento sia svolto nel rispetto dei diritti fondamentali della persona.

Un ulteriore principio fondamentale introdotto dal GDPR è quello di **accountability**⁴, che può essere tradotto come principio di responsabilizzazione⁵. In base a tale principio, European Data Protection Board sostiene che il titolare del trattamento non è soltanto tenuto a rispettare le norme in materia di protezione dei dati personali, ma deve anche essere in grado di dimostrare di aver adottato misure adeguate per garantire e dimostrare la conformità alla normativa⁶.

Nel loro complesso, questi tre principi in particolare rappresentano gli elementi fondamentali del sistema di protezione dei dati personali previsto dal GDPR. Essi contribuiscono a consolidare la tutela dei diritti degli interessati e a promuovere una maggiore responsabilità da parte dei soggetti che trattano dati personali, soprattutto nel contesto delle piattaforme digitali, dove il trattamento dei dati costituisce spesso un elemento centrale del modello di business.

1.3 Il ruolo delle autorità di controllo e delle linee guida interpretative

Nel sistema definito dal **Regolamento (UE) 2016/679 (GDPR)**, le autorità di controllo rivestono un ruolo fondamentale. Il regolamento europeo, infatti, non si limita soltanto a stabilire principi e obblighi per titolari e responsabili del trattamento, ma prevede anche un articolato sistema istituzionale finalizzato a vigilare sul rispetto delle disposizioni normative e ad assicurare un'applicazione uniforme della disciplina all'interno dell'Unione europea.

Ai sensi degli articoli 51 e seguenti del GDPR, ogni Stato membro è tenuto a istituire una o più autorità pubbliche indipendenti incaricate di monitorare l'applicazione del regolamento. Tali organismi, comunemente denominati autorità di controllo, operano in piena autonomia rispetto ai poteri politici e amministrativi, al fine di garantire l'imparzialità delle loro decisioni. In Italia questa funzione è svolta dal Garante per la protezione dei dati personali, autorità amministrativa indipendente competente per la vigilanza sull'applicazione della normativa in materia di privacy.

⁴ Article 29 Working Party, *Guidelines on Transparency under Regulation 2016/679*, WP260, 2018, pp. 7-8, 16

⁵ G. Finocchiaro, *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna, Zanichelli, 2019, pp. 6-7.

⁶ European Data Protection Board, *Guidelines 4/2019 on Article 25 – Data Protection by Design and by Default*, Version 2.0, 20 ottobre 2020, p. 28.

Le autorità di controllo sono investite di numerosi compiti, elencati in particolare nell'articolo 57 del GDPR. Tra le principali funzioni rientrano il monitoraggio e l'applicazione del regolamento, la promozione della consapevolezza tra cittadini e operatori economici riguardo ai diritti e agli obblighi previsti dalla normativa, nonché la gestione dei reclami presentati dagli interessati.

Inoltre le autorità svolgono attività di consulenza nei confronti delle istituzioni nazionali e collaborano con altri organismi europei per favorire un'applicazione coerente della disciplina. Accanto a tali compiti, il regolamento attribuisce alle autorità di controllo anche specifici poteri di intervento, indicati nell'articolo 58 del GDPR. In particolare, esse possono svolgere indagini, richiedere informazioni ai titolari del trattamento, effettuare verifiche e applicare provvedimenti correttivi. Tra questi ultimi rientrano, ad esempio, l'ammonimento, l'ordine di conformarsi alla normativa, la limitazione, sanzioni in base alla gravità della violazione o il divieto del trattamento e l'irrogazione di sanzioni amministrative pecuniarie⁷. Le linee guida adottate dalle autorità europee costituiscono strumenti interpretativi volti a fornire indicazioni pratiche sull'applicazione degli obblighi previsti dal regolamento, contribuendo a garantire un'applicazione uniforme della disciplina in materia di protezione dei dati personali⁸. Possiamo dunque notare come il GDPR attribuisca alle autorità di controllo un ruolo essenziale nel garantire l'effettiva salvaguardia della privacy. Ciò contribuisce non solo al rispetto delle regole da parte di imprese e istituzioni, ma soprattutto alla tutela dei diritti e delle libertà fondamentali delle persone nell'utilizzo dei propri dati personali.

1.4 Etica d'impresa e protezione dei dati personali

Negli ultimi anni, la protezione dei dati personali ha assunto una rilevanza che va oltre il semplice adempimento normativo⁹, aprendo la questione a un livello etico legato alla responsabilità sociale delle imprese. In questo contesto, il concetto di **etica d'impresa**¹⁰ si può intendere come l'insieme dei principi, valori e linee guida che indirizzano il comportamento organizzativo e le decisioni aziendali, influenzando il modo in cui le attività vengono condotte nel rispetto degli utenti e della collettività.

L'attenzione verso l'etica d'impresa si è evoluta fino a riconoscere che le organizzazioni economiche, comprese le grandi piattaforme digitali, hanno una **responsabilità**

⁷ CNIL, *Deliberazione n. SAN-2019-001 del 21 gennaio 2019*; vedi anche *Deliberazione n. SAN-2021-023 del 31 dicembre 2021*.

⁸ Article 29 Working Party, *Guidelines on Transparency under Regulation 2016/679*, WP260, 2018, pp. 4

⁹ EDPS Ethics Advisory Group | *Report 2018*, pp. 7-12, 15-19

¹⁰E. D'Orazio, *Responsabilità sociale ed etica d'impresa*, in *Notizie di Politeia*, Politeia, Milano, 2003, pp.3

sociale¹¹ che non si limita al mero rispetto delle norme. Le imprese devono valutare l'impatto sociale delle proprie attività e promuovere condotte basate su trasparenza, correttezza e responsabilità. In questo quadro, le politiche interne e i modelli organizzativi diventano strumenti chiave per favorire comportamenti responsabili e sostenibili all'interno delle organizzazioni.

Tale dimensione è particolarmente rilevante nel settore digitale, dove la raccolta e l'elaborazione di dati personali costituiscono una componente centrale dei modelli di business. Le informazioni sugli utenti rappresentano una risorsa strategica, utilizzata per migliorare servizi, personalizzare offerte e sviluppare strumenti analitici. Garantire una gestione etica e responsabile di questi dati non solo tutela la privacy, ma contribuisce anche a consolidare la fiducia degli utenti e la legittimità delle operazioni aziendali.

La normativa europea, in particolare il **Regolamento (UE) 2016/679 – GDPR**, ha rafforzato questa prospettiva introducendo il principio di responsabilizzazione (accountability) dei titolari del trattamento. Le organizzazioni sono tenute ad adottare misure tecniche e organizzative che assicurino il rispetto dei principi di liceità, correttezza e trasparenza, integrando così la normativa nella pratica quotidiana di gestione dei dati.

Oltre agli obblighi legali, molte imprese hanno sviluppato strumenti di **autoregolamentazione**¹² per promuovere comportamenti etici e responsabili. Tra questi, i **codici etici** e i programmi di compliance assumono un ruolo centrale, definendo standard di condotta e linee guida operative che orientano le decisioni e le azioni dei membri dell'organizzazione. Tali strumenti favoriscono la diffusione di una cultura aziendale improntata alla trasparenza, all'integrità e al rispetto dei diritti degli individui.

In conclusione, l'etica d'impresa integra e rafforza la regolamentazione giuridica, contribuendo a promuovere una gestione dei dati personali più consapevole e responsabile. La combinazione tra compliance normativa e strumenti etici interni permette alle piattaforme digitali di coniugare legalità, responsabilità sociale e tutela dei diritti fondamentali, costituendo un modello sostenibile di governance dei dati.

¹¹E. D'Orazio, *Responsabilità sociale ed etica d'impresa*, in *Notizie di Politeia*, Politeia, Milano, 2003, p 6-7

¹²Organisation for Economic Co-operation and Development, *OECD Guidelines for Multinational Enterprises on Responsible Business Conduct*, OECD Publishing, Paris, 2023, pp 17

CAPITOLO 2

CRITERI E METODOLOGIA DI ANALISI

2.1 Metodologia comparativa adottata

La presente ricerca adotta una metodologia comparativa finalizzata ad analizzare gli strumenti di trasparenza e responsabilità nel trattamento dei dati personali, con particolare riferimento alle informative privacy e ai codici etici adottati dalle organizzazioni. L'approccio comparativo consente di mettere in relazione diversi modelli regolatori e prassi applicative, al fine di valutarne l'efficacia rispetto ai principi stabiliti dalla normativa europea in materia di protezione dei dati personali.

L'analisi si fonda su fonti istituzionali primarie e secondarie, tra cui il Regolamento (UE) 2016/679 (GDPR), i documenti interpretativi del Gruppo di lavoro Article 29 (WP29) e del Comitato europeo per la protezione dei dati (EDPB), nonché le indicazioni fornite dalla Commissione europea e dalle autorità nazionali di controllo, in particolare il Garante per la protezione dei dati personali.

Sono inoltre considerati contributi istituzionali di natura interpretativa ed etica, quali i pareri del Garante europeo della protezione dei dati, che evidenziano il ruolo della responsabilizzazione e dei principi etici nel trattamento dei dati personali.

Tali fonti sono state selezionate per la loro autorevolezza e per il loro ruolo nella definizione e nell'interpretazione dei principi di trasparenza, correttezza e accountability.

L'analisi comparativa è stata sviluppata sulla base di tre criteri principali che verranno di seguito analizzati.

2.2 Criteri di analisi delle informative privacy

L'analisi delle informative privacy è stata condotta alla luce dei principi di trasparenza, correttezza e accountability previsti dal Regolamento (UE) 2016/679 (GDPR), con particolare riferimento agli articoli 12, 13 e 14, nonché al considerando 39, che sottolinea l'esigenza che le informazioni fornite all'interessato siano facilmente accessibili e comprensibili.

In tale prospettiva, sono stati individuati alcuni criteri fondamentali di analisi, finalizzati a valutare l'effettiva idoneità delle informative a garantire una comunicazione chiara ed efficace nei confronti degli interessati. In primo luogo, è stato considerato il **criterio della chiarezza e comprensibilità del linguaggio**¹³. Le informative sono state

¹³ European Data Protection Board, *Guidelines 4/2019 on Article 25 – Data Protection by Design and by Default*, Version 2.0, 20 ottobre 2020, pp. 8-15.

esaminate per verificare l'utilizzo di un linguaggio semplice, chiaro e non eccessivamente tecnico, in linea con quanto richiesto dall'articolo 12 del GDPR e dalle linee guida del Gruppo di lavoro Articolo 29 (WP29)¹⁴ in materia di trasparenza. In particolare, è stata valutata la capacità dell'informativa di rendere comprensibili concetti giuridici complessi anche a utenti non esperti.

Un secondo criterio riguarda la **struttura e organizzazione delle informazioni**. È stata analizzata la modalità di presentazione dei contenuti, con particolare attenzione all'eventuale adozione di modelli di informativa "a livelli" (layered privacy notices), raccomandati dalle linee guida del WP29 (*Guidelines on Transparency under Regulation 2016/679*, WP260 rev.01). Tali modelli consentono di suddividere le informazioni in diversi livelli di approfondimento, facilitando la fruizione e riducendo il rischio di sovraccarico informativo.

Ulteriore elemento di analisi è rappresentato dalla **completezza delle informazioni fornite**. In questo senso, si è verificata la presenza di tutti gli elementi richiesti dagli articoli 13 e 14 del GDPR, quali l'identità del titolare del trattamento, le finalità e la base giuridica del trattamento, i destinatari dei dati, il periodo di conservazione, nonché i diritti riconosciuti all'interessato. La completezza è stata valutata non solo in termini formali, ma anche sostanziali, considerando la chiarezza con cui tali informazioni sono effettivamente comunicate.

Un ulteriore criterio riguarda la **accessibilità e facilità di reperimento delle informazioni**. In particolare, nel contesto digitale, è stata valutata la facilità con cui l'utente può accedere all'informativa e navigare tra le diverse sezioni, nonché la visibilità delle informazioni principali al momento della raccolta dei dati personali. Tale aspetto assume rilievo anche alla luce delle raccomandazioni del WP29, che sottolineano l'importanza di fornire le informazioni essenziali già nel primo livello dell'informativa¹⁵.

Infine, è stato considerato il **criterio della rilevanza e dell'impatto delle informazioni fornite**, con particolare attenzione alla capacità dell'informativa di evidenziare gli aspetti del trattamento che possono avere un impatto significativo sull'interessato o che potrebbero risultare inattesi. In linea con le indicazioni del WP29, l'informativa dovrebbe consentire all'interessato di comprendere le conseguenze del trattamento dei propri dati personali, favorendo così un consenso realmente informato.

Nel complesso, l'applicazione congiunta di tali criteri ha consentito di sviluppare un'analisi comparativa delle informative privacy non limitata al piano formale, ma orientata a valutare l'effettiva efficacia comunicativa e il grado di tutela garantito

¹⁴ Article 29 Working Party, *Guidelines on Transparency under Regulation 2016/679*, 2018, pp. 7–9, 16–18

¹⁵ Article 29 Working Party, *Guidelines on Transparency under Regulation 2016/679*, 2018, pp. 10-12.

all'interessato, in coerenza con i principi fondamentali della normativa europea in materia di protezione dei dati personali.

2.3 Criteri di analisi dei codici etici

Nel contesto delle piattaforme digitali, i codici etici rappresentano strumenti di autoregolamentazione attraverso i quali le imprese definiscono principi, valori e standard di comportamento destinati a orientare le proprie attività. Al fine di condurre un'analisi comparativa efficace, risulta necessario individuare criteri metodologici che consentano di valutare in modo sistematico il contenuto e la funzione di tali documenti.

Un primo criterio di analisi riguarda il **grado di chiarezza e accessibilità del codice etico**. In linea con quanto previsto in materia di trasparenza nel trattamento dei dati personali, anche i codici etici devono essere redatti in modo comprensibile e facilmente accessibile agli utenti e agli stakeholder. Le linee guida adottate a livello europeo sottolineano, infatti, l'importanza di utilizzare un linguaggio chiaro e semplice, evitando formulazioni eccessivamente tecniche che possano comprometterne la comprensione¹⁶.

Un secondo criterio è rappresentato dal **contenuto sostanziale degli impegni etici**, con particolare riferimento alla tutela dei dati personali. In questo senso, è necessario verificare se e in che misura i codici etici richiamino i principi fondamentali stabiliti dal General Data Protection Regulation, quali la trasparenza, la correttezza e la responsabilizzazione (accountability), nonché se tali principi siano tradotti in impegni concreti e operativi.

Un ulteriore criterio riguarda il **grado di vincolatività e di effettività del codice etico**. I codici etici si configurano generalmente come strumenti di soft law, privi di efficacia giuridicamente vincolante in senso stretto, ma comunque rilevanti nella misura in cui incidono sui comportamenti delle imprese e contribuiscono a orientare le loro pratiche. In ambito internazionale, le linee guida dell'Organisation for Economic Co-operation and Development evidenziano come le imprese siano chiamate ad adottare politiche interne idonee a garantire una gestione responsabile delle attività, anche attraverso meccanismi di controllo e monitoraggio¹⁷.

In questa prospettiva, assume rilievo anche il livello di integrazione tra codici etici e strumenti normativi, in particolare con riferimento alla disciplina della protezione dei dati personali. Le autorità di controllo, come il Garante per la protezione dei dati personali e l'European Data Protection Board, hanno più volte sottolineato l'importanza di adottare un approccio sostanziale alla tutela dei dati, che non si limiti al rispetto

¹⁶ Article 29 Working Party, *Guidelines on Transparency under Regulation 2016/679*, 2018, pp. 7–8.

¹⁷ Organisation for Economic Co-operation and Development, *Guidelines for Multinational Enterprises on Responsible Business Conduct*, OECD Publishing, Paris, 2023, pp. 14–16.

formale degli obblighi normativi, ma si traduca nell'adozione di misure concrete e verificabili, in linea con il principio di accountability e con le esigenze di trasparenza nei confronti degli interessati¹⁸. In tal senso, i sistemi di gestione della privacy previsti dallo standard ISO/IEC 27701 costituiscono oggi uno dei principali riferimenti internazionali per trasformare gli impegni etici in procedure organizzative verificabili¹⁹. Infine, un ulteriore criterio di analisi riguarda il **grado di trasparenza nei confronti degli utenti**, intesa non solo come chiarezza delle informazioni, ma anche come capacità del codice etico di rendere comprensibili le scelte aziendali relative al trattamento dei dati personali. In tal senso, le linee guida europee evidenziano come la trasparenza rappresenti uno strumento essenziale per garantire l'effettivo esercizio dei diritti da parte degli interessati e per rafforzare la fiducia nei confronti dei titolari del trattamento.

Alla luce di tali criteri, l'analisi comparativa dei codici etici delle principali piattaforme digitali consentirà di valutare non solo il contenuto formale dei documenti, ma anche la loro effettiva capacità di contribuire alla tutela dei diritti degli utenti e alla promozione di pratiche aziendali responsabili.

2.4 Limiti e potenzialità dell'approccio utilizzato

L'approccio metodologico adottato presenta sia aspetti positivi sia alcune criticità che meritano di essere considerate.

Tra i principali punti di forza vi è la possibilità di mettere in evidenza la natura dinamica del principio di accountability, che non si limita alla sua formulazione normativa, ma prende forma attraverso l'interpretazione e l'applicazione concreta. Il confronto tra fonti differenti consente, inoltre, di individuare in modo più chiaro gli strumenti attraverso cui il titolare del trattamento può dimostrare la propria conformità, offrendo una prospettiva maggiormente operativa del principio.

Accanto a tali elementi, emergono tuttavia alcuni limiti. La pluralità delle fonti può infatti dar luogo a interpretazioni non sempre uniformi, rendendo più complessa una ricostruzione sistematica. Inoltre, le linee guida e i documenti delle autorità, pur essendo autorevoli, non hanno carattere vincolante e possono subire modifiche nel tempo. Va infine considerata la limitata presenza di dati empirici, che riduce la possibilità di valutare in modo approfondito l'effettiva applicazione del principio nei diversi contesti organizzativi.

Nel complesso, nonostante tali aspetti, l'approccio adottato risulta adeguato rispetto agli obiettivi della ricerca, poiché consente di mettere in luce il ruolo centrale

¹⁸ Article 29 Working Party, *Guidelines on Transparency under Regulation 2016/679*, 2018, pp. 23-25

¹⁹ ISO/IEC 27701:2019, *Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management*, pp. 1-15.

dell'accountability nel sistema del GDPR, integrando la dimensione normativa con quella interpretativa e applicativa.

CAPITOLO 3

ANALISI DI GOOGLE

3.1 Struttura e contenuti dell'informativa privacy

L'informativa privacy di Google è organizzata in modo modulare, pensata per guidare l'utente passo dopo passo nel capire come avviene la raccolta, l'utilizzo e la gestione dei dati personali. Dato che Google offre servizi molto diversi tra loro – dal motore di ricerca a Gmail, fino ad Android e al cloud – il documento cerca di offrire una panoramica unitaria, rimandando poi a pagine di approfondimento specifiche per i singoli prodotti.

Il testo segue un percorso logico²⁰ che accompagna l'utente attraverso le varie fasi del trattamento. All'inizio vengono spiegate le categorie di dati raccolti, distinguendo tra quelli inseriti direttamente dall'utente, quelli generati dall'uso dei servizi e le informazioni catturate tramite dispositivi, browser o applicazioni. Più che un semplice elenco, questa sezione descrive proprio come questi dati vengano acquisiti durante l'uso quotidiano della piattaforma.

Subito dopo vengono approfondite le finalità²¹, cioè il perché questi dati vengono trattati. Google elenca le attività principali: l'erogazione dei servizi stessi, la sicurezza dei sistemi, il miglioramento dei prodotti, lo sviluppo di nuove funzioni e la personalizzazione delle pubblicità. Per rendere il tutto più chiaro, la descrizione è accompagnata da esempi pratici che mostrano come i dati vengano effettivamente impiegati nelle varie situazioni.

Una parte importante riguarda poi la condivisione dei dati personali²². Google distingue tra i dati scambiati internamente all'azienda e quelli trasferiti all'esterno a fornitori, partner commerciali, sviluppatori o autorità pubbliche. Inoltre, viene dedicato uno spazio specifico ai trasferimenti di dati all'estero, indicando gli strumenti usati per tutelare le informazioni quando escono dallo Spazio Economico Europeo.

Un punto interessante dell'informativa è l'attenzione agli strumenti di controllo. Google non si limita a elencare i diritti teorici dell'utente, ma inserisce nel testo i link diretti per

²⁰ Google LLC, *Norme sulla privacy di Google*, sez. "Informazioni che Google raccoglie"

²¹ Google LLC, *Norme sulla privacy di Google*, sez. "Perché Google raccoglie i dati".

²² Google LLC, *Norme sulla privacy di Google*, sez. "Quando Google condivide le informazioni"

gestire la propria privacy, come la dashboard dell'Account Google, il Privacy Check-up²³ o la cronologia delle attività. In questo modo il documento diventa anche operativo, permettendo all'utente di modificare le proprie opzioni direttamente mentre legge.

Dal punto di vista della scrittura, la caratteristica principale è la struttura multilivello²⁴ (layered). Le informazioni fondamentali sono riassunte all'inizio, mentre i dettagli tecnici si trovano cliccando sui vari link ipertestuali. Questo approccio serve a bilanciare la completezza dei contenuti con la leggibilità, cercando di rendere più accessibili concetti complessi attraverso schemi, domande frequenti ed esempi pratici.

Nel complesso, la struttura dell'informativa privacy di Google riflette la complessità dei servizi offerti dall'azienda e l'elevato numero di trattamenti effettuati quotidianamente. Se da un lato questa organizzazione multilivello mira a facilitare la consultazione e garantisce una formale leggibilità, dall'altro la dottrina e le autorità di controllo hanno evidenziato come l'eccessiva parcellizzazione delle informazioni in decine di link ipertestuali separati possa produrre un effetto di "trasparenza apparente"²⁵, costringendo l'utente a una navigazione complessa per ricostruire l'effettiva portata dei trattamenti e della profilazione pubblicitaria. Di conseguenza, l'analisi delle singole sezioni evidenzia come il documento non assolva soltanto a una funzione di conformità normativa o di comunicazione aziendale, ma rappresenti un terreno di scontro interpretativo sul reale soddisfacimento dei requisiti di trasparenza previsti dal legislatore europeo.

3.2 Trasparenza su finalità, basi giuridiche e trattamento dei dati

Analizzando l'informativa di Google, si nota subito un grande sforzo nel descrivere il perché i dati personali vengano raccolti e utilizzati. Data la quantità enorme di servizi offerti, il documento divide queste informazioni in categorie separate, cercando di mostrare all'utente il legame diretto tra le sue azioni quotidiane e i trattamenti che avvengono dietro le quinte.

La prima grande finalità riguarda il funzionamento stesso e il miglioramento dei prodotti. Google spiega che i dati servono concretamente a far funzionare le piattaforme, a garantire la sicurezza dei sistemi, a risolvere i bug tecnici e a progettare nuove funzionalità²⁶. In questo modo, l'informativa mette in chiaro che la raccolta delle informazioni è il motore principale per l'evoluzione dell'intero ecosistema aziendale.

²³ Google LLC, *Centro per la Privacy di Google; Account Google – Privacy Check-up*.

²⁴ European Data Protection Board, *Guidelines 4/2019 on Article 25 – Data Protection by Design and by Default, Version 2.0*, 20 ottobre 2020, p. 15

²⁵ CNIL, *Deliberazione n. SAN-2019-001 del 21 gennaio 2019*. Cfr. anche G. CASSANO - G. SCORZA (a cura di), *Diritti degli utenti e piattaforme digitali*, Pisa, Pacini Giuridica, 2023.

²⁶ Google LLC, *Norme sulla privacy di Google*, sez. "Perché Google raccoglie dati".

Un punto cruciale riguarda poi la personalizzazione dei contenuti e la pubblicità. Google descrive come la cronologia delle ricerche, le posizioni geografiche e le preferenze espresse online vengano usate per mostrare annunci pubblicitari su misura. Questo passaggio è fondamentale, poiché svela la logica economica della piattaforma, basata proprio sul mercato dell'advertising personalizzato.

Sul piano strettamente giuridico, Google associa ogni trattamento a una specifica base legale del GDPR²⁷. Il documento distingue tra i trattamenti indispensabili per eseguire il contratto (cioè per erogare il servizio richiesto), le attività che richiedono il consenso esplicito dell'utente e, infine, quelle che si fondano sul legittimo interesse dell'azienda, come la prevenzione delle frodi o la sicurezza informatica.

Un elemento a favore del documento è il fatto che la spiegazione teorica non resta isolata, ma è sempre collegata a strumenti pratici. Google inserisce nel testo i rimandi alle impostazioni del profilo, permettendo a chi legge di modificare subito le preferenze sulla privacy, bloccare determinate attività o limitare l'uso dei propri dati personali.

Il limite principale rimane però la mole complessiva delle informazioni. Anche se Google mette a disposizione molti strumenti di controllo, la varietà dei servizi trattati rende il testo inevitabilmente denso. Per un utente comune può essere difficile comprendere a fondo i meccanismi più complessi, in particolare quelli legati alla profilazione invisibile e agli algoritmi pubblicitari²⁸.

In conclusione, questa sezione dell'informativa offre un quadro molto dettagliato, cercando di trovare un punto di incontro tra le esigenze di trasparenza del GDPR e la necessità di essere comprensibile. Questa impostazione modulare e orientata ai servizi rappresenta un ottimo punto di partenza per il confronto che verrà fatto nei prossimi paragrafi con i modelli di Meta e LinkedIn.

3.3 Analisi del codice etico e dei principi di responsabilità

La responsabilità etica di Google si articola principalmente attraverso due documenti distinti ma complementari: il Google Code of Conduct²⁹, rivolto ai dipendenti e ai collaboratori dell'azienda, e i Google AI Principles³⁰, dedicati ai criteri etici che devono orientare lo sviluppo e l'utilizzo dell'intelligenza artificiale. Entrambi rappresentano strumenti attraverso cui Google definisce i propri valori organizzativi e il proprio approccio alla responsabilità aziendale.

²⁷ G. Finocchiaro, *Il Regolamento europeo sulla protezione dei dati personali*, Bologna, Zanichelli, 2017, commento all'art. 6 GDPR

²⁸ Article 29 Working Party, *Guidelines on Transparency under Regulation 2016/679*, 2018, pp. 9

²⁹ Google LLC, *Code of Conduct*

³⁰ Google LLC, *Google AI Principles*

Il Google Code of Conduct svolge una funzione interna, stabilendo i comportamenti richiesti ai soggetti che operano all'interno dell'organizzazione. Il documento pone al centro il principio dell'integrità, richiamando il rispetto delle normative, delle politiche aziendali e degli standard etici. Particolare attenzione viene dedicata alla tutela delle informazioni riservate, alla prevenzione dei conflitti di interesse, al contrasto della corruzione e alla promozione di un ambiente di lavoro basato sul rispetto e sull'inclusione.

Come evidenziato dalla dottrina sull'etica d'impresa, il codice etico non rappresenta soltanto una dichiarazione di valori, ma costituisce uno strumento di governance volto a orientare i processi decisionali e a rafforzare la fiducia degli stakeholder. In questa prospettiva, assumono particolare rilievo i meccanismi di controllo e segnalazione previsti da Google, che consentono di rendere effettivi i principi dichiarati attraverso procedure interne e strumenti di compliance³¹.

Accanto al codice di condotta, Google ha adottato i Google AI Principles, con l'obiettivo di definire un ³²o di riferimento etico per lo sviluppo dell'intelligenza artificiale. Il documento richiama alcuni principi fondamentali, tra cui il beneficio sociale della tecnologia, la sicurezza dei sistemi, la tutela della privacy, l'equità e la responsabilità nell'utilizzo degli algoritmi. Tale impostazione risulta coerente con l'orientamento della dottrina in materia di etica dell'intelligenza artificiale, secondo cui lo sviluppo di sistemi di IA deve essere accompagnato da principi di responsabilità, trasparenza e tutela dei diritti fondamentali³³.

Un elemento significativo riguarda inoltre l'individuazione di alcune applicazioni dell'intelligenza artificiale che Google dichiara di non voler sviluppare³⁴, in quanto ritenute incompatibili con i propri principi etici. Questa scelta evidenzia il tentativo dell'azienda di introdurre forme di autoregolamentazione in un settore caratterizzato da rilevanti implicazioni sociali e giuridiche.

Nel complesso, il sistema etico di Google si fonda quindi su due dimensioni complementari: una dimensione organizzativa, rappresentata dal Code of Conduct, che disciplina i comportamenti interni, e una dimensione tecnologica, rappresentata dagli AI Principles, che orienta lo sviluppo responsabile delle nuove tecnologie

³¹ E. Freeman, *Strategic Management: A Stakeholder Approach*, Boston, Pitman, 1984, pp. 85-115.

³² High-Level Expert Group on Artificial Intelligence, *Ethics Guidelines for Trustworthy AI*, Commissione europea, 2019, pp. 16-18.

³³ L. Floridi, *Etica dell'intelligenza artificiale. Sviluppi, opportunità, sfide*, Raffaello Cortina Editore, Milano, 2022, pp. 35-36 e pp. 287-301.

³⁴ Google LLC, *Google AI Principles*, sez. "Applications we will not pursue"

3.4 Coerenza tra obblighi normativi e impegni etici dichiarati

Dall'analisi dell'informativa sulla privacy, del *Google Code of Conduct* e dei *Google AI Principles* emerge un sostanziale allineamento tra gli obblighi giuridici imposti dal quadro normativo europeo e gli impegni etici assunti spontaneamente dall'azienda. Google, infatti, non si limita a recepire in modo passivo le disposizioni del Regolamento (UE) 2016/679 (GDPR)³⁵, ma integra i precetti di legge all'interno di un sistema di valori e di regole organizzative volti a promuovere una gestione responsabile dei dati e delle tecnologie digitali³⁶.

Tale convergenza risulta evidente, in primo luogo, nella centralità riconosciuta ai principi di trasparenza, sicurezza e responsabilizzazione (*accountability*). Se l'informativa sulla privacy disciplina sul piano formale e operativo le modalità di raccolta e trattamento dei dati degli utenti, il *Code of Conduct* interviene sul versante interno, imponendo ai dipendenti standard di condotta improntati all'integrità e alla tutela delle informazioni riservate. Parallelamente, i *Google AI Principles* estendono questa sensibilità deontologica allo sviluppo dell'intelligenza artificiale, subordinando l'innovazione tecnologica al rispetto dei diritti fondamentali e alla sicurezza dei sistemi. L'approccio del gruppo appare dunque orientato a coniugare la *compliance* normativa con l'autoregolamentazione etica. In quest'ottica, i codici interni non si pongono in termini di alternatività rispetto agli obblighi di legge³⁷, ma agiscono in funzione complementare, concorrendo a consolidare una cultura organizzativa orientata alla prevenzione del rischio. Si tratta di un'impostazione coerente con la recente evoluzione del diritto europeo delle nuove tecnologie, che valorizza sempre più i modelli di governance interna e l'adozione di presidi procedurali da parte delle imprese.

Permangono, tuttavia, precisi profili critici. Gli impegni etici formalizzati nei documenti aziendali conservano una natura volontaria e, a differenza delle norme giuridiche, risultano privi di un sistema sanzionatorio esterno e indipendente. Di conseguenza, l'efficacia reale di tali strumenti resta subordinata alla volontà dell'organizzazione di applicare le proprie dichiarazioni di principio in prassi operative verificabili. L'autoregolamentazione rappresenta quindi un valido presidio integrativo, ma non può sofferire alle tutele tipiche del sistema precettivo e giurisdizionale.

In conclusione, l'analisi evidenzia un modello di governance che tenta di bilanciare il vincolo legale e la responsabilità etica al fine di preservare il capitale reputazionale e la

³⁵ G. Finocchiaro, *Il Regolamento europeo sulla protezione dei dati personali*, Bologna, Zanichelli, 2017, commento all'art. 5 e 24 GDPR

³⁶ Google LLC, *Privacy Policy*

³⁷ *Ethics Guidelines for Trustworthy AI*, High-Level Expert Group on AI, Commissione europea, 2019, pp. 16-18

fiducia degli stakeholder³⁸. Questo equilibrio costituisce uno dei tratti più significativi della strategia di posizionamento di Google e rappresenterà, nei successivi capitoli, il parametro di riferimento per valutare comparativamente l'approccio adottato dalle altre due piattaforme oggetto della presente tesi.

CAPITOLO 4

ANALISI DI META

4.1 Struttura dell'informativa privacy e modalità di comunicazione

Per districarsi tra le complessità di un ecosistema digitale fortemente integrato, l'architettura informativa adottata da Meta³⁹ si affida a un modello a livelli (layered privacy notice). Questa tecnica espositiva mira a coniugare la sintesi con il rigore normativo: l'utente riceve in prima battuta una panoramica essenziale dei trattamenti in corso, per poi poter scendere in profondità attraverso rinvii ipertestuali mirati. Tale impostazione ricalca fedelmente l'imperativo di trasparenza delineato dal GDPR, volto a garantire notizie chiare, immediate e facilmente accessibili.

Entrando nel dettaglio, la policy disamina le diverse fasi del trattamento dalle categorie di dati raccolti alle finalità commerciali, dalle basi legali alle tempistiche di conservazione, fino ai flussi di dati transfrontalieri e ai diritti azionabili. Una simile modalità assolve in pieno agli obblighi di trasparenza imposti dagli articoli 12, 13 e 14 del Regolamento UE 2016/679, offrendo una mappa di navigazione utile a orientare l'utente tra i vari adempimenti.

Sotto il profilo comunicativo, si nota un deciso allontanamento dal consueto linguaggio burocratico in favore di un lessico più accessibile, caratterizzato da esempi concreti e rinvii a guide interattive. Ma il vero valore aggiunto risiede nella compenetrazione tra la policy e il Centro per la privacy: l'informativa cessa di essere un mero manifesto teorico e si concretizza. Tramite i link alle impostazioni dell'account, infatti, l'interessato può passare rapidamente dalla teoria alla pratica, revocando consensi, regolando la profilazione pubblicitaria o attivando i propri diritti.

Un capitolo centrale riguarda inevitabilmente la circolazione intra-gruppo dei dati e la loro esportazione oltre i confini dello Spazio Economico Europeo⁴⁰. Su questo fronte,

³⁸ E. Freeman, *Strategic Management: A Stakeholder Approach*, Boston, Pitman, 1984, pp. 131

³⁹ Meta Platforms, *Informativa sulla privacy, versione vigente*, Centro per la privacy di Meta.

⁴⁰ Meta Platforms, *Informativa sulla privacy, sezione « Come condividiamo le informazioni con terzi?»*.

l'informativa si impegna a mappare le garanzie legali adoperate per blindare i flussi informativi verso giurisdizioni terze, assicurando la continuità della tutela europea.

Ciononostante, permane una criticità di fondo: la mole documentale resta imponente. L'effetto labirinto generato dai continui rimandi interni e dalla densità tecnica dei trattamenti rischia di vanificare, nella pratica, gli sforzi di trasparenza. Come evidenziato dalla dottrina e dalle autorità di vigilanza, la conformità cartacea o formale al GDPR non si traduce automaticamente in una comprensione effettiva, specie quando ci si muove all'interno di piattaforme social iper-personalizzate e opache per l'utente comune⁴¹.

4.2 Trattamento dei dati personali e profilazione degli utenti

Il funzionamento delle piattaforme appartenenti al gruppo Meta si basa sul trattamento di un'ampia quantità di dati personali⁴². Oltre alle informazioni fornite direttamente dagli utenti, quali dati identificativi e informazioni contenute nel profilo, Meta raccoglie dati relativi alle attività svolte sulle proprie piattaforme, alle interazioni con altri utenti, ai contenuti visualizzati e alle caratteristiche dei dispositivi utilizzati. Tali informazioni possono essere elaborate anche attraverso l'integrazione dei dati provenienti dai diversi prodotti appartenenti all'ecosistema Meta.

Un ruolo centrale è svolto dalla profilazione, definita dall'art. 4, n. 4, del GDPR⁴³ come una forma di trattamento automatizzato finalizzata a valutare o prevedere aspetti personali, quali preferenze, interessi e comportamenti. Meta utilizza sistemi automatizzati per personalizzare i contenuti mostrati agli utenti, formulare suggerimenti e selezionare le inserzioni pubblicitarie in base alle informazioni raccolte⁴⁴.

La profilazione rappresenta pertanto un elemento essenziale del modello economico della piattaforma, poiché consente di proporre pubblicità personalizzata e di rendere maggiormente mirata l'esperienza dell'utente. L'attività di targeting può basarsi sulle interazioni effettuate all'interno delle piattaforme e, nei limiti previsti dalla normativa applicabile, sulle informazioni ricevute da partner e soggetti terzi. Secondo l'European Data Protection Board, tali trattamenti possono comportare la creazione di categorie di utenti sulla base di interessi e comportamenti, con possibili effetti sulle aspettative e sulla sfera informativa degli interessati.

⁴¹ G. Finocchiaro, *Privacy e protezione dei dati personali*, Zanichelli, Bologna, 2021, pp. 128-133.

⁴² Meta, *Informativa sulla privacy*, sez. «Quali informazioni raccogliamo?»

⁴³ Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016 (GDPR).

⁴⁴ Meta, *Informativa sulla privacy*, sez. «Perché e come trattiamo le tue informazioni»,

L'ampiezza dei dati trattati rende particolarmente rilevanti i principi di trasparenza, limitazione della finalità e minimizzazione dei dati previsti dall'art. 5 del GDPR⁴⁵. Meta mette a disposizione strumenti attraverso i quali gli utenti possono accedere alle proprie informazioni, modificare alcune impostazioni relative alla privacy e alla pubblicità ed esercitare i diritti riconosciuti dalla normativa⁴⁶.

In conclusione, il trattamento dei dati e la profilazione costituiscono elementi centrali dell'ecosistema Meta. Sebbene tali attività consentano la personalizzazione dei servizi e delle comunicazioni pubblicitarie, esse richiedono un elevato livello di trasparenza, affinché gli utenti possano comprendere quali informazioni siano utilizzate e per quali finalità.

4.3 Principi etici e responsabilità sociale dell'impresa

L'attività di Meta non si limita alla fornitura di servizi digitali, ma incide in modo significativo sulle modalità di comunicazione, sulla formazione delle relazioni sociali e sulla circolazione delle informazioni. In ragione della posizione dominante assunta dalle sue piattaforme nel panorama digitale globale, i principi etici e la responsabilità sociale dell'impresa assumono un ruolo rilevante nella valutazione delle modalità attraverso cui la società esercita il proprio potere tecnologico ed economico.

La responsabilità sociale d'impresa (Corporate Social Responsibility – CSR) rappresenta il complesso degli strumenti attraverso cui un'organizzazione integra considerazioni di carattere sociale, ambientale ed etico nella propria attività economica, andando oltre il semplice rispetto degli obblighi normativi. Secondo la dottrina, tale concetto evidenzia il passaggio da una concezione esclusivamente economica dell'impresa a un modello nel quale l'attività imprenditoriale deve tenere conto degli interessi degli stakeholder coinvolti, tra cui utenti, lavoratori, comunità e istituzioni.^[^1] Nel settore digitale, tale prospettiva assume una particolare rilevanza, poiché le grandi piattaforme non esercitano soltanto un'attività economica, ma svolgono anche una funzione di regolazione degli spazi di comunicazione online. Come osservato in dottrina, le imprese tecnologiche attraverso strumenti quali codici etici, linee guida interne e procedure di controllo adottano forme di autoregolamentazione privata, volte a disciplinare comportamenti e rischi derivanti dall'utilizzo delle proprie infrastrutture digitali⁴⁷.

⁴⁵ Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016 (GDPR).

⁴⁶ Meta, *Informativa sulla privacy*, sez. « Qual è la nostra base giuridica per il trattamento delle informazioni e quali sono i tuoi diritti? »

⁴⁷ G. Finocchiaro, *Il Regolamento europeo sulla protezione dei dati personali*, Bologna, Zanichelli, 2017. pp. 45-48

Meta dichiara di perseguire obiettivi connessi alla creazione di comunità, alla sicurezza degli utenti e allo sviluppo responsabile delle proprie tecnologie. Tali finalità trovano applicazione attraverso documenti interni come il “Code of Conduct”⁴⁸, che individua principi quali integrità, rispetto delle persone, conformità normativa e responsabilità individuale nello svolgimento delle attività aziendali.

Un ulteriore elemento dell’approccio etico di Meta è rappresentato dalle “Community Standards”, attraverso cui la società stabilisce le regole relative ai contenuti ammessi sulle proprie piattaforme. Tali standard mirano a contrastare fenomeni quali discorsi d’odio, violenza, molestie e diffusione di contenuti dannosi, costituendo un sistema di regolazione privata che affianca gli strumenti previsti dagli ordinamenti giuridici nazionali ed europei⁴⁹.

Tuttavia, l’applicazione concreta di tali principi presenta alcune criticità. La dimensione globale delle piattaforme, l’elevato numero di contenuti pubblicati quotidianamente e il ricorso a sistemi automatizzati di moderazione rendono complesso garantire decisioni sempre coerenti e trasparenti. Inoltre, il modello economico basato sulla raccolta e sull’analisi dei dati personali per finalità pubblicitarie pone una possibile tensione tra gli interessi commerciali dell’impresa e la tutela dei diritti fondamentali degli utenti.

In conclusione, l’esperienza di Meta mostra come la responsabilità sociale dell’impresa tecnologica non possa essere limitata alla dichiarazione formale di principi etici, ma debba essere valutata considerando l’effettiva applicazione degli stessi. I codici di condotta e gli standard interni rappresentano strumenti importanti di autoregolamentazione, ma la loro efficacia dipende dalla capacità dell’impresa di garantire trasparenza, controllo e tutela concreta degli interessi degli utenti⁵⁰.

4.4 Criticità e punti di forza nel rapporto tra diritto ed etica

L’analisi dell’Informativa privacy e dei documenti etici di Meta evidenzia una stretta relazione tra diritto ed etica nella regolazione delle attività svolte dalle grandi piattaforme digitali. Il diritto stabilisce obblighi vincolanti in materia di protezione dei dati personali, trasparenza e tutela degli utenti, mentre l’etica d’impresa individua principi e criteri di comportamento che possono integrare gli obblighi normativi e

⁴⁸ Meta, Code of Conduct, sezioni dedicate a integrità, rispetto, responsabilità e conformità normativa.

⁴⁹ Meta, Community Standards (Il nostro impegno per la libertà di espressione)

⁵⁰ La dottrina ha evidenziato come i codici etici e di condotta non siano semplici dichiarazioni di intenti, ma possano assumere una concreta funzione organizzativa all’interno dell’impresa. Come osservato da F. Benatti, essi contribuiscono a definire i principi e le regole che orientano il comportamento aziendale, diventando parte della cultura dell’organizzazione. Tale funzione emerge anche nel D. Lgs. 8 giugno 2001, n. 231, nel quale il codice etico rappresenta un elemento importante dei Modelli di Organizzazione, Gestione e Controllo (MOGC), finalizzati alla prevenzione dei reati e alla responsabilizzazione dell’ente.

orientare le decisioni aziendali anche in situazioni non espressamente disciplinate dalla legge⁵¹.

Un primo punto di forza è rappresentato dalla complementarità tra norme giuridiche e strumenti di autoregolamentazione. Il GDPR impone a Meta obblighi specifici relativi alla liceità del trattamento, alla trasparenza delle informazioni e alla tutela dei diritti degli interessati. I codici etici e gli standard interni possono invece contribuire a sviluppare una cultura aziendale orientata alla responsabilità, alla prevenzione dei rischi e alla tutela degli utenti. In questo senso, l'etica può svolgere una funzione preventiva, favorendo l'adozione di comportamenti responsabili prima che si verifichino violazioni o conseguenze dannose.

Un ulteriore elemento positivo è costituito dalla presenza di strumenti che consentono agli utenti di gestire le proprie informazioni e di modificare alcune preferenze relative alla privacy e alla pubblicità. La disponibilità di tali strumenti può rafforzare il controllo dell'interessato sui dati personali e contribuire alla concreta applicazione dei principi di trasparenza e responsabilizzazione previsti dal GDPR⁵².

Tuttavia, emergono anche importanti criticità. I documenti etici adottati dalle imprese sono generalmente strumenti di autoregolamentazione e non possiedono la stessa efficacia vincolante delle norme giuridiche. La loro applicazione dipende in larga misura dalle procedure interne e dalla volontà dell'impresa, mentre il rispetto degli obblighi previsti dal GDPR è soggetto al controllo delle autorità di protezione dei dati e può comportare l'applicazione di sanzioni. Di conseguenza, la presenza di principi etici formalmente dichiarati non garantisce necessariamente che essi siano applicati in modo effettivo e uniforme.

Un'ulteriore criticità riguarda la complessità dei trattamenti effettuati da Meta. Sebbene l'Informativa privacy presenti le principali finalità e categorie di dati trattati, la quantità di informazioni raccolte, l'integrazione tra i diversi servizi e l'utilizzo di sistemi automatizzati possono rendere difficile per gli utenti comprendere pienamente il funzionamento dei processi di profilazione. La trasparenza non richiede infatti soltanto la disponibilità delle informazioni, ma anche che queste siano formulate in modo chiaro, accessibile e comprensibile⁵³.

Può inoltre emergere una tensione tra gli obiettivi etici dichiarati e il modello economico della piattaforma, fondato in larga misura sulla pubblicità personalizzata e sul coinvolgimento degli utenti. La ricerca di una maggiore permanenza sulle piattaforme e la raccolta di dati finalizzata alla personalizzazione dei contenuti possono

⁵¹ G. Finocchiaro, *Privacy e protezione dei dati personali*, Bologna, Zanichelli, 2021, pp. 45-48

⁵² Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016 (GDPR).

⁵³ Article 29 Working Party, *Guidelines on Transparency under Regulation 2016/679*, 2018, pp. 7-11

entrare in conflitto con esigenze quali la tutela della privacy, la limitazione del trattamento e la protezione degli utenti più vulnerabili⁵⁴.

conclusione, l'esperienza di Meta dimostra come diritto ed etica debbano muoversi di pari passo, pur con ruoli ben distinti. Se da un lato le norme garantiscono un quadro vincolante fatto di obblighi, controlli e sanzioni, dall'altro l'etica aziendale può spingersi oltre, aiutando a prevenire rischi che la legge non è ancora riuscita a regolamentare nel dettaglio.

Tuttavia, per non rimanere semplici dichiarazioni di intenti o operazioni di facciata, i principi etici devono tradursi in regole di condotta pratiche, trasparenti e davvero verificabili. L'etica, insomma, non può e non deve sostituire il diritto, ma se applicata seriamente può diventare un valido alleato per rafforzare le tutele e stare al passo con la rapida evoluzione del digitale.

CAPITOLO 5

ANALISI DI LINKEDIN

5.1 Caratteristiche dell'informativa privacy

L'architettura dell'informativa sulla privacy predisposta da LinkedIn si articola in una serie di sezioni concepite per illustrare con precisione le tappe del trattamento, dalla raccolta all'impiego e alla comunicazione delle informazioni personali. Nello specifico, il documento analizza in premessa le diverse fonti di acquisizione, separando i dati forniti volontariamente dall'iscritto da quelli rilevati in modo automatico durante la navigazione o acquisiti tramite soggetti terzi, quali partner commerciali, datori di lavoro e altri utenti della rete. Oltre ai dati identificativi indispensabili per la creazione dell'account, l'attività di tracciamento comprende il percorso formativo e lavorativo, le competenze dichiarate, le interazioni sociali e i dati ottenuti mediante cookie e strumenti di tracciamento assimilabili⁵⁵.

La peculiarità di questo documento risiede nel costante raccordo tra l'elaborazione delle informazioni e la vocazione strettamente professionale della piattaforma. Gli elementi inseriti nel profilo vengono infatti elaborati per agevolare il *networking*, favorire l'incontro tra domanda e offerta di lavoro e calibrare la fruizione dei contenuti. LinkedIn precisa inoltre le ragioni alla base del trattamento, identificandole nella gestione

⁵⁴ European Data Protection Board, *Guidelines 4/2019 on Article 25 – Data Protection by Design and by Default, Version 2.0*, 20 ottobre 2020, pp. 8-13 e 17-22.

⁵⁵ LinkedIn, *Privacy Policy*

operativa delle funzionalità, nell'implementazione della sicurezza informatica, nello studio dei comportamenti di fruizione e nella profilazione a scopi pubblicitari.

Un riscontro analogo si rileva nella sezione focalizzata sulla trasmissione delle informazioni a terzi. La *policy* individua espressamente i destinatari dei dati, includendovi i fornitori di servizi esterni, le imprese collegate al gruppo societario, i partner di business e gli organi statali ove richiesto dalle disposizioni vigenti. Con riferimento al contesto europeo, la responsabilità del trattamento fa capo a *LinkedIn Ireland Unlimited Company*; la relativa appendice territoriale specifica le basi giuridiche applicabili, le tutele azionabili dall'interessato e le garanzie adottate nell'ambito dei trasferimenti informativi verso Paesi extra-UE⁵⁶.

Nel suo insieme, la documentazione offre una mappatura ordinata e orientata alla trasparenza, ripartendo la materia in aree dedicate all'acquisizione, alla gestione, alla condivisione e agli strumenti di controllo a disposizione dell'utente. Ciononostante, l'ampiezza delle categorie di dati gestite e la molteplicità degli scopi perseguiti determinano un quadro complessivo articolato, che può rendere complessa, per l'interessato, una comprensione immediata e lineare di tutte le dinamiche del trattamento.

5.2 Specificità del trattamento dei dati in ambito professionale

Una delle principali caratteristiche di LinkedIn riguarda la particolare natura professionale dei dati trattati. A differenza di altri social network, la piattaforma è infatti orientata principalmente alla costruzione dell'identità professionale dell'utente e alla creazione di collegamenti con colleghi, aziende e potenziali datori di lavoro. Nel profilo possono essere inserite informazioni quali formazione, esperienze lavorative, competenze, posizione professionale e azienda di appartenenza, che vengono utilizzate anche per favorire l'incontro tra domanda e offerta di lavoro⁵⁷.

Il trattamento assume quindi una particolare rilevanza nell'ambito del recruiting. LinkedIn utilizza le informazioni presenti nei profili per suggerire opportunità lavorative, mettere in contatto gli utenti con recruiter e individuare profili che corrispondono a determinate esigenze professionali. La piattaforma offre inoltre servizi specifici, come Recruiter e Sales Navigator, attraverso i quali le imprese possono effettuare ricerche mirate e utilizzare determinate informazioni professionali degli utenti.

⁵⁶ LinkedIn, *European Regional Privacy Notice*, "Consent", "Data Sharing with Third Parties" e "Transfers of your data"

⁵⁷ LinkedIn, *Privacy Policy*, sezioni relative al profilo, ai dati professionali e ai servizi di LinkedIn

Un ulteriore elemento caratterizzante riguarda la possibilità di utilizzare i dati professionali per attività di profilazione e personalizzazione. Informazioni come il settore lavorativo, le competenze, l'istruzione, le aziende seguite e le interazioni effettuate sulla piattaforma possono essere impiegate per proporre contenuti, contatti e annunci pubblicitari maggiormente pertinenti agli interessi professionali dell'utente⁵⁸. LinkedIn dichiara inoltre di poter elaborare alcune informazioni per ricavare elementi ulteriori, come il settore di appartenenza o il livello di seniority professionale⁵⁹.

La dimensione professionale del trattamento comporta quindi anche specifiche esigenze di tutela. La possibilità che il profilo sia consultato da recruiter, imprese e altri professionisti rende particolarmente importante il controllo esercitabile dall'utente sulla visibilità delle proprie informazioni. La stessa LinkedIn precisa che l'utente può scegliere quali informazioni inserire nel profilo e quali rendere pubbliche, sottolineando l'importanza di non pubblicare dati personali che non si desidera rendere accessibili.

In conclusione, il trattamento dei dati effettuato da LinkedIn presenta una specificità legata alla trasformazione delle informazioni personali in informazioni di carattere professionale, utilizzate per finalità di networking, ricerca del lavoro, selezione del personale, personalizzazione dei servizi e pubblicità. Questa caratteristica distingue LinkedIn dalle piattaforme social generaliste e rende particolarmente rilevante il rapporto tra valorizzazione dei dati professionali, trasparenza del trattamento e possibilità di controllo da parte dell'interessato⁶⁰.

5.3 Codice etico e tutela degli utenti

Nel confronto tra Google, Meta e LinkedIn, il caso di LinkedIn presenta caratteristiche specifiche, legate alla natura professionale della piattaforma. La tutela degli utenti non riguarda infatti esclusivamente la protezione dei dati personali, ma comprende anche l'autenticità dell'identità, la sicurezza delle interazioni e il mantenimento di un ambiente professionale affidabile⁶¹.

Le *Professional Community Policies* di LinkedIn costituiscono il principale riferimento per la definizione dei comportamenti ammessi sulla piattaforma. Le regole richiedono agli utenti di utilizzare la propria identità autentica e vietano la creazione di profili falsi,

⁵⁸ LinkedIn, *Privacy Policy*, sezioni relative alla personalizzazione, alla pubblicità e all'utilizzo dei dati; Gruppo di lavoro

⁵⁹ Article 29 Working Party, *Guidelines on Transparency under Regulation 2016/679*, WP260, 2018

⁶⁰ Garante per la protezione dei dati personali, *Approvazione del codice di condotta per il settore delle Agenzie per il lavoro e accreditamento dell'organismo di monitoraggio*, Provvedimento n. 12 dell'11 gennaio 2024

⁶¹ Regolamento (UE) 2016/679, artt. 5, 25 e 32.

l'utilizzo dell'identità di altre persone e la diffusione di informazioni ingannevoli⁶². A tali disposizioni si aggiungono specifici divieti relativi a molestie, minacce, truffe, spam e divulgazione non autorizzata di informazioni personali⁶³. La tutela dell'utente viene quindi strettamente collegata alla necessità di preservare la fiducia all'interno della comunità professionale.

Un ulteriore elemento caratterizzante è rappresentato dall'attività di controllo e applicazione delle regole. LinkedIn utilizza sistemi automatizzati e personale specializzato per individuare contenuti e comportamenti che possono violare le proprie policy⁶⁴. In relazione alla gravità della violazione, la piattaforma può limitare la diffusione di un contenuto, rimuoverlo oppure applicare restrizioni all'account dell'utente. È inoltre prevista, in determinate circostanze, la possibilità di presentare un ricorso contro le decisioni adottate⁶⁵. Tali strumenti evidenziano un modello di tutela che combina prevenzione, monitoraggio e possibilità di revisione.

Rispetto a LinkedIn, Google e Meta presentano principi etici maggiormente orientati alla gestione generale della privacy, della sicurezza e dei rischi tecnologici. Google pone particolare enfasi sulla fiducia degli utenti, sulla sicurezza e sulla protezione dei dati nella progettazione dei propri prodotti⁶⁶. Meta, invece, integra la tutela della privacy con temi quali sicurezza, diritti umani, trasparenza e responsabilità nell'intelligenza artificiale⁶⁷. LinkedIn si distingue quindi per il forte collegamento tra tutela dell'utente e qualità della comunità professionale.

In conclusione, il modello di LinkedIn mostra come il concetto di tutela dell'utente possa estendersi oltre la semplice protezione dei dati personali. Privacy, autenticità, sicurezza e correttezza dei comportamenti diventano elementi complementari finalizzati a mantenere un ambiente digitale professionale e affidabile. In questo senso, le policy etiche di LinkedIn svolgono una funzione complementare all'informativa privacy, contribuendo a definire non solo le modalità di trattamento dei dati, ma anche gli standard di comportamento richiesti agli utenti della piattaforma.

⁶² LinkedIn, *Professional Community Policies*, sezione "Be Trustworthy"

⁶³ LinkedIn, *Professional Community Policies*, sezioni "Be Safe", "Be Trustworthy" e "Be Professional".

⁶⁴ LinkedIn, *Professional Community Policies*

⁶⁵ Regolamento (UE) 2022/2065 (Digital Services Act), in particolare le disposizioni relative alla trasparenza della moderazione e ai meccanismi di ricorso.

⁶⁶ G. Finocchiaro, *La protezione dei dati personali e la tutela dell'identità*, cit., pp. 177-182; A. Mantelero, *Responsabilità aquiliana per uso della Rete e responsabilità del provider*, in E. Tosi (a cura di), *Internet e il diritto*, Milano, Giuffrè, 2013, pp. 785 ss.

⁶⁷ M. Franzoni, *Responsabilità derivante da trattamento dei dati personali*, in E. Tosi (a cura di), *Internet e il diritto*, Milano, Giuffrè, 2013, pp. 829 ss.

5.4 Allineamento tra trasparenza informativa ed etica aziendale

Nel quadro comparativo tra Google, Meta e LinkedIn, l'analisi di quest'ultima fa emergere specificità rilevanti, strettamente connesse alla funzione professionale dell'infrastruttura. La protezione riconosciuta all'interessato non si esaurisce infatti nella sola tutela dei dati personali, ma abbraccia l'autenticità dell'identità digitale, l'integrità delle relazioni di rete e la salvaguardia di un perimetro professionale fondato sulla fiducia.

Le *Professional Community Policies* di LinkedIn rappresentano il cardine regolatorio aziendale volto a disciplinare le condotte ammesse all'interno del network. Tali prescrizioni impongono agli iscritti l'adozione della propria identità reale, vietando la creazione di account fittizi, il furto d'identità e la veicolazione di dati o affermazioni ingannevoli⁶⁸. A questo nucleo di regole si affiancano severi divieti relativi a comportamenti quali molestie, atti intimidatori, frodi, invio di messaggi indesiderati (*spam*) e diffusione non autorizzata di dati riservati⁶⁹. La protezione dell'utente si trasforma così in una garanzia essenziale per preservare l'affidabilità reputazionale dell'intera comunità.

Un secondo profilo caratterizzante risiede nell'architettura di controllo ed *enforcement* delle regole di condotta. LinkedIn combina l'impiego di algoritmi automatizzati con la valutazione di team di moderazione umani per rilevare contenuti e comportamenti difforni rispetto alle proprie linee guida⁷⁰. In ragione della gravità delle violazioni riscontrate, la piattaforma può disporre la limitazione della visibilità dei contenuti, la loro definitiva rimozione o la sospensione temporanea/permanente del profilo dell'utente. È altresì garantita, per determinati casi, una procedura d'appello volta a contestare i provvedimenti sanzionatori adottati. Tale impostazione delinea un modello di tutela multilivello, basato sulla prevenzione, sul tracciamento costante e sulla facoltà di riesame.

Un ulteriore elemento di coerenza riguarda la moderazione dei contenuti. LinkedIn mette a disposizione un Transparency Center attraverso il quale comunica le modalità con cui applica le proprie regole e pubblica informazioni sulle attività di moderazione, sugli account falsi, sullo spam e sulle violazioni dei contenuti⁷¹. La trasparenza diventa così uno strumento di responsabilizzazione, poiché consente agli utenti e agli altri

⁶⁸ *Internet e il diritto*, Milano, Giuffrè, 2013, S. Romano, Art. 18, d.lg. 70/2003 e autodisciplina del commercio elettronico, pp. 3.; 484

⁶⁹ *Internet e il diritto*, Milano, Giuffrè, 2013, G. Finocchiaro pp. 151, 158-168; A. Ricci, *La reputazione nell'era digitale* pp. 197-218

⁷⁰ LinkedIn, *How LinkedIn Enforces Its Professional Community Policies*

⁷¹ Regolamento (UE) 2022/2065 (Digital Services Act), art. 27, "Trasparenza dei sistemi di raccomandazione"

soggetti interessati di comprendere maggiormente come la piattaforma applica i propri standard.

Nel complesso, emerge un significativo allineamento tra i principi etici dichiarati da LinkedIn e gli strumenti informativi messi a disposizione degli utenti. Tuttavia, sulla base dell'analisi condotta, la trasparenza di LinkedIn può essere considerata complessivamente adeguata, ma non pienamente accessibile e immediata⁷². L'azienda fornisce un'ampia quantità di informazioni sulle modalità di trattamento dei dati, sulla personalizzazione dei contenuti, sui sistemi di raccomandazione e sulle attività di moderazione, dimostrando un concreto impegno verso la trasparenza⁷³. Al tempo stesso, la presenza di numerose policy e documenti, caratterizzati da un linguaggio prevalentemente tecnico e giuridico, può rendere difficile per l'utente medio comprendere in modo immediato come i propri dati vengano effettivamente utilizzati e quali conseguenze derivino dalle proprie scelte. Pertanto, LinkedIn risulta trasparente sotto il profilo formale e informativo, ma presenta alcuni limiti sotto il profilo della comprensibilità sostanziale. La trasparenza appare quindi presente e coerente con i principi etici dichiarati dall'azienda, ma potrebbe essere ulteriormente migliorata attraverso informazioni più semplici, sintetiche e direttamente orientate a facilitare il controllo dell'utente sui propri dati.

CAPITOLO 6

ANALISI COMPARATIVA

6.1 Confronto tra le informative privacy delle tre piattaforme

Il confronto tra le informative privacy di Google, Meta e LinkedIn evidenzia significative analogie, ma anche differenze legate alla natura e alle finalità dei rispettivi servizi. Tutte e tre le piattaforme adottano informative articolate, organizzate secondo una struttura multilivello e accompagnate da strumenti attraverso i quali l'utente può gestire alcune impostazioni relative ai propri dati. Tale impostazione risponde all'esigenza di garantire una comunicazione trasparente e accessibile, in linea con quanto previsto dagli artt. 12, 13 e 14 GDPR e dalle Linee guida del Gruppo di lavoro ex art. 29 sulla trasparenza⁷⁴.

⁷² Regolamento (UE) 2016/679, art. 12; European Data Protection Board (EDPB), *Guidelines on transparency under Regulation 2016/679*.

⁷³ LinkedIn, *Privacy Policy*; LinkedIn, *User Agreement*; LinkedIn, *Transparency Center*

⁷⁴ Article 29 Working Party, *Guidelines on Transparency under Regulation 2016/679*, 2018

La principale differenza riguarda la tipologia e l'ampiezza dei dati trattati. Google presenta l'ecosistema informativo più diversificato, considerando la molteplicità dei servizi offerti e la possibilità di combinare dati derivanti dall'utilizzo di prodotti differenti. Meta presenta anch'essa un trattamento particolarmente esteso, soprattutto in relazione alle attività degli utenti sui social network, alle interazioni, ai contenuti prodotti e alle informazioni relative ai dispositivi. LinkedIn, invece, presenta una maggiore specializzazione dei dati raccolti, strettamente connessi alla dimensione professionale dell'utente, quali esperienze lavorative, formazione, competenze e relazioni professionali.

Anche con riferimento alle finalità del trattamento emergono elementi comuni. Tutte le piattaforme utilizzano i dati per fornire e migliorare i servizi, garantire la sicurezza e personalizzare l'esperienza dell'utente. Google e Meta evidenziano maggiormente il rapporto tra trattamento dei dati, personalizzazione dei contenuti e attività pubblicitaria, mentre LinkedIn collega più direttamente l'utilizzo delle informazioni alla propria funzione di rete professionale, pur prevedendo anch'essa finalità commerciali e pubblicitarie.

Nel complesso, le tre informative risultano formalmente coerenti con gli obblighi di trasparenza previsti dal GDPR. Tuttavia, la loro complessità costituisce un elemento critico comune: la disponibilità di un'elevata quantità di informazioni non garantisce necessariamente una piena comprensione da parte dell'utente. Ne deriva che l'effettiva trasparenza dovrebbe essere valutata non soltanto in relazione alla completezza dell'informazione, ma anche alla sua chiarezza, accessibilità e capacità di consentire all'interessato di comprendere concretamente le modalità e le finalità del trattamento.

Da questa prospettiva, il confronto tra Google, Meta e LinkedIn mostra come la sfida principale non consista soltanto nel garantire la presenza delle informazioni richieste dal GDPR, ma nel rendere tali informazioni effettivamente utili all'esercizio dell'autodeterminazione informativa dell'interessato. La qualità dell'informativa deve pertanto essere valutata non esclusivamente sulla base della quantità di informazioni fornite, ma anche considerando la loro organizzazione, accessibilità, comprensibilità e capacità di consentire all'utente di comprendere concretamente come e perché i propri dati vengono utilizzati⁷⁵.

6.2 Confronto tra i codici etici

Accanto alle informative sulla privacy, l'analisi dei codici etici di Google, Meta e LinkedIn offre una prospettiva complementare sull'approccio di *soft law* e di responsabilizzazione d'impresa (*Corporate Social Responsibility*) adottato dalle tre

⁷⁵ Garante per la protezione dei dati personali, *Rendere le informative privacy più comprensibili. Il legal design come approccio rivolto all'utente*, White Paper, 2025.

piattaforme. Sebbene tutti e tre gli strumenti condividano l'obiettivo di promuovere la fiducia e l'integrità aziendale, essi si differenziano sensibilmente per struttura, ambito di applicazione e posizionamento strategico. Concreta applicazione di tali codici ha tuttavia evidenziato significativi momenti di tensione tra i principi dichiarati e le dinamiche operative di ciascuna piattaforma.

Google declina il proprio impianto etico attraverso due direttrici principali: il *Code of Conduct*, rivolto alla condotta interna dei dipendenti, e i *Google AI Principles*, focalizzati sullo sviluppo responsabile dell'intelligenza artificiale. Il modello di Google si distingue per un forte orientamento all'innovazione tecnologica etica e per la formale individuazione di ambiti operativi che l'azienda dichiara di non voler perseguire, come le tecnologie dannose o lesive dei diritti umani. Un esempio emblematico di questo assetto si è verificato nel 2018 con il *Project Maven* (un contratto militare con il Dipartimento della Difesa USA per l'analisi di immagini da droni), in cui una vasta protesta interna dei dipendenti — fondata sulla palese violazione del Codice di Condotta e dello spirito del celebre motto "*Don't be evil*" — ha costretto l'azienda a recedere dall'accordo e a formalizzare ufficialmente i propri principi etici contro l'uso dell'IA per scopi bellici.

Meta adotta una struttura incentrata sulla regolazione degli spazi di comunicazione digitale, combinando il proprio *Code of Conduct* con gli *Standard della community* (*Community Standards*). L'approccio di Meta è orientato alla gestione della condotta degli utenti e dei rischi legati all'interazione sociale (quali discorsi d'odio e sicurezza online). Tuttavia, l'efficacia di tale impianto è storicamente messa alla prova dalla complessa tensione tra la moderazione dei contenuti e un modello economico basato sul massimo *engagement* e sulla profilazione pubblicitaria. Un caso significativo è rappresentato dalle rivelazioni della *whistleblower* Frances Haugen⁷⁶ nel 2021 (i cosiddetti *Facebook Files*), le quali hanno dimostrato come l'azienda fosse consapevole dell'impatto dannoso di Instagram sulla salute mentale dei minori e dell'amplificazione dei contenuti d'odio da parte degli algoritmi, evidenziando uno scarto netto tra le politiche etiche dichiarate a tutela della community e le priorità commerciali della piattaforma.

LinkedIn, infine, presenta un quadro etico fortemente integrato con la propria vocazione professionale, rappresentato dalle *Professional Community Policies*. A differenza di Google e Meta, LinkedIn focalizza i propri impegni etici sulla tutela dell'identità reale, sulla veridicità delle informazioni professionali e sul contrasto a comportamenti lesivi della reputazione o del decoro professionale (quali spam, truffe e molestie). In questo contesto, una vicenda rilevante riguarda il contenzioso emerso dinanzi a diversi tribunali

⁷⁶ Frances Haugen dinanzi al Congresso degli Stati Uniti (*Subcommittee on Consumer Protection*, 5 ottobre 2021) e al Parlamento Europeo (*Commissione IMCO*, 8 novembre 2021), i cui atti formali hanno costituito il riscontro istituzionale ai documenti interni resi pubblici (notia come *Facebook Files*) e hanno accelerato l'iter normativo del *Digital Services Act* (Regolamento UE 2022/2065).

europei a seguito della sospensione impropria o automatizzata di profili aziendali e professionali. I giudici hanno iniziato a sindacare le decisioni di moderazione etica di LinkedIn, stabilendo che l'applicazione arbitraria delle *Community Policies* non può ledere la reputazione o il diritto al lavoro dell'utente e che la piattaforma deve garantire motivazioni puntuali e il rispetto del giusto processo, in linea con i principi introdotti dal *Digital Services Act* (DSA)

Nel complesso, emerge una convergenza sui principi di responsabilità, sicurezza, trasparenza e tutela degli interessati, ma con differenti priorità. Google concentra maggiormente l'attenzione sull'innovazione tecnologica, Meta sulla regolazione della sfera sociale online, mentre LinkedIn sulla qualità e affidabilità delle relazioni all'interno della propria comunità professionale. I codici etici svolgono pertanto una funzione complementare rispetto alla disciplina giuridica, contribuendo confermare il valore dell'autoregolamentazione

6.3 Trasparenza dichiarata e trasparenza effettiva

Il confronto tra Google, Meta e LinkedIn evidenzia come la trasparenza costituisca un elemento centrale delle rispettive informative privacy. Tuttavia, è necessario distinguere tra trasparenza dichiarata e trasparenza effettiva. La prima consiste nella presenza formale di informazioni relative alla raccolta e al trattamento dei dati personali; la seconda richiede invece che tali informazioni siano concretamente comprensibili e utilizzabili dall'interessato. Tale distinzione assume particolare rilevanza alla luce dell'art. 12 GDPR, che impone che le informazioni siano fornite in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro⁷⁷.

Le tre piattaforme mostrano, sotto il profilo formale, un elevato livello di trasparenza. Le informative sono ampie, strutturate per sezioni e generalmente organizzate secondo una logica multilivello, attraverso collegamenti e approfondimenti dedicati ai diversi aspetti del trattamento.² Questa ricchezza informativa, tuttavia, può determinare una trasparenza soltanto apparente: la presenza di una grande quantità di informazioni non coincide necessariamente con la loro effettiva comprensione da parte dell'utente.

Il rischio è particolarmente evidente quando le informative descrivono trattamenti complessi attraverso formulazioni tecniche, riferimenti a numerosi servizi o collegamenti tra diverse finalità. In tali circostanze, l'utente può formalmente disporre di tutte le informazioni richieste, senza però riuscire a comprendere con immediatezza

⁷⁷ Regolamento (UE) 2016/679, art. 12

quali dati siano trattati⁷⁸, per quali finalità, con quali conseguenze e quali possibilità di controllo gli siano concretamente riconosciute. La trasparenza rischia così di trasformarsi in un adempimento prevalentemente formale.

Ne consegue che, nel confronto tra Google, Meta e LinkedIn, la trasparenza non dovrebbe essere valutata sulla sola quantità delle informazioni fornite, ma sulla loro chiarezza, accessibilità e comprensibilità effettiva. Una comunicazione realmente trasparente non è quella che semplicemente rende disponibili molte informazioni, bensì quella che consente all'utente di comprenderne il significato e di esercitare consapevolmente i propri diritti⁷⁹.

6.4 Implicazioni per la tutela dei diritti degli utenti

Il confronto tra Google, Meta e LinkedIn consente di evidenziare come le modalità di trattamento dei dati e di comunicazione adottate dalle piattaforme abbiano implicazioni che vanno oltre il semplice rispetto degli obblighi informativi previsti dal GDPR. La tutela dei diritti degli utenti dipende, infatti, dalla possibilità di comprendere le modalità di funzionamento dei servizi, conoscere l'utilizzo dei propri dati e disporre di strumenti effettivi per esercitare forme di controllo sulle attività della piattaforma⁸⁰.

In primo luogo, la trasparenza assume un ruolo essenziale per l'esercizio dei diritti riconosciuti dalla normativa in materia di protezione dei dati personali. Un'informazione eccessivamente complessa o soltanto formalmente completa può rendere più difficile per l'utente comprendere la portata dei trattamenti e, conseguentemente, esercitare consapevolmente diritti quali accesso, rettifica, cancellazione, opposizione e limitazione del trattamento.¹ La trasparenza costituisce quindi una condizione necessaria affinché la tutela giuridica non rimanga esclusivamente teorica.

Le implicazioni riguardano, tuttavia, anche altri ambiti. L'utilizzo di sistemi algoritmici, la personalizzazione dei contenuti e della pubblicità, la profilazione e le modalità di moderazione possono incidere sull'autonomia decisionale dell'utente e sulla sua possibilità di comprendere perché determinate informazioni, contenuti o comunicazioni gli vengano mostrati. Analogamente, i codici etici e le regole interne delle piattaforme possono contribuire alla tutela della sicurezza, della dignità e della correttezza delle

⁷⁸ *Linee Guida ed interventi sui Cookie (Provvedimento Garante n. 231/2021): Il Garante italiano ha sanzionato l'architettura con cui le piattaforme e i grandi siti di intermediazione presentano le informative brevi (banner cookie)*

⁷⁹ G. Finocchiaro, *Privacy e protezione dei dati personali*, Zanichelli, Bologna, 2021, in particolare la trattazione relativa ai principi di trasparenza e agli obblighi informativi

⁸⁰ European Data Protection Board (EDPB),

interazioni, ma la loro efficacia dipende dalla concreta applicazione dei principi dichiarati⁸¹.

Ne emerge una concezione più ampia della tutela dell'utente, nella quale diritto, trasparenza ed etica risultano strettamente collegati. Google, Meta e LinkedIn adottano strumenti differenti, ma per tutte la sfida consiste nel trasformare principi e garanzie formalmente riconosciuti in forme concrete di consapevolezza, controllo e possibilità di contestazione. La tutela effettiva non può quindi essere misurata esclusivamente sulla quantità di informazioni o sulla presenza di procedure previste, ma sulla loro concreta capacità di rafforzare la posizione dell'utente nei confronti della piattaforma.

CONCLUSIONI

L'analisi svolta nel presente elaborato ha avuto come obiettivo il confronto tra le informative privacy e i documenti di carattere etico adottati da Google, Meta e LinkedIn, con particolare attenzione al rapporto tra gli obblighi previsti dalla normativa in materia di protezione dei dati personali e le forme di autoregolamentazione sviluppate dalle singole piattaforme. Il confronto ha permesso di evidenziare come la gestione dei dati personali rappresenti oggi un elemento centrale nel rapporto tra imprese digitali e utenti e come la tutela di questi ultimi non possa essere ricondotta esclusivamente al rispetto formale delle disposizioni del GDPR.

Dall'analisi delle informative privacy è emerso innanzitutto che tutte e tre le piattaforme dedicano ampio spazio alla descrizione delle modalità di raccolta, utilizzo e condivisione dei dati personali, nonché agli strumenti messi a disposizione degli utenti per esercitare i propri diritti. Le differenze riguardano soprattutto la tipologia di dati trattati e le caratteristiche dei rispettivi ecosistemi. Google opera attraverso un insieme molto ampio di servizi e raccoglie dati derivanti da differenti attività dell'utente; Meta presenta un modello fortemente legato alle interazioni sociali, ai contenuti prodotti dagli utenti e alla personalizzazione dell'esperienza e della pubblicità; LinkedIn, invece, concentra maggiormente il trattamento sulla dimensione professionale, attraverso informazioni relative al profilo, alle esperienze lavorative, alle competenze e alle relazioni professionali.

Il confronto ha inoltre evidenziato l'importanza della trasparenza quale elemento fondamentale della protezione dei dati personali. Le tre piattaforme adottano informative articolate e, in diversa misura, strutturate secondo un approccio multilivello. Tuttavia, la presenza di una quantità elevata di informazioni non garantisce necessariamente una loro effettiva comprensione. Si è quindi evidenziata la distinzione

⁸¹ Regolamento (UE) 2022/2065 (Digital Services Act, art. 17, 20 e 21

tra una trasparenza meramente dichiarata e una trasparenza effettiva, nella quale l'utente sia realmente in grado di comprendere quali dati vengano trattati, per quali finalità, con quali modalità e quali possibilità di controllo siano concretamente disponibili. In questo senso, la trasparenza non dovrebbe essere valutata esclusivamente sulla quantità delle informazioni fornite, ma anche sulla loro chiarezza, accessibilità e comprensibilità.

Un secondo elemento emerso dall'indagine riguarda il ruolo dei documenti etici e degli strumenti di autoregolamentazione. Google, Meta e LinkedIn presentano approcci differenti: Google attribuisce particolare rilevanza ai principi relativi allo sviluppo responsabile delle tecnologie e dell'intelligenza artificiale; Meta concentra maggiormente la propria attenzione sulla sicurezza e sulla gestione delle interazioni all'interno delle proprie piattaforme; LinkedIn collega i propri principi alla natura professionale della comunità, ponendo particolare attenzione all'affidabilità delle identità e dei rapporti tra utenti. Nonostante tali differenze, tutti e tre i modelli condividono l'obiettivo di definire principi di comportamento che integrano, almeno sul piano dichiarativo, gli obblighi derivanti dalla disciplina giuridica.

Il rapporto tra diritto ed etica rappresenta pertanto uno degli aspetti più significativi emersi dalla ricerca. Il GDPR stabilisce obblighi giuridicamente vincolanti e attribuisce agli utenti specifici diritti, mentre i codici e i principi etici rappresentano strumenti attraverso i quali le imprese possono assumere ulteriori impegni in materia di responsabilità, sicurezza, correttezza e tutela degli interessati. Questi strumenti non sostituiscono la disciplina normativa, ma possono svolgere una funzione complementare, contribuendo a definire standard di comportamento ulteriori rispetto a quelli strettamente imposti dalla legge.

L'analisi ha tuttavia mostrato che la presenza di principi etici e di informative dettagliate non è, di per sé, sufficiente a garantire una tutela effettiva. La reale efficacia di tali strumenti dipende dalla loro concreta applicazione e dalla possibilità per l'utente di comprenderli e utilizzarli. In questo senso, assume particolare rilevanza il divario che può emergere tra i principi dichiarati dalle piattaforme e le modalità con cui questi vengono concretamente tradotti nelle loro attività. La trasparenza deve quindi essere considerata non soltanto come un obbligo informativo, ma come uno strumento attraverso il quale l'utente può acquisire consapevolezza e mantenere una forma di controllo sui propri dati e sul rapporto con la piattaforma.

Il confronto tra Google, Meta e LinkedIn evidenzia infine che non esiste un unico modello di tutela dei dati applicabile alle grandi piattaforme digitali. Le caratteristiche dei servizi offerti, le tipologie di dati trattati e le finalità perseguite determinano modalità differenti di comunicazione e di autoregolamentazione. Ciò che accomuna le tre realtà è però la necessità di rendere effettivi i principi di trasparenza, responsabilità e tutela dell'utente in un contesto tecnologico caratterizzato da una crescente complessità.

In conclusione, la ricerca conferma come la protezione dei dati personali nell'economia digitale richieda un equilibrio tra regolamentazione giuridica, trasparenza informativa e responsabilità d'impresa. Il GDPR costituisce il principale riferimento normativo, ma la sua efficacia concreta dipende anche dalla capacità delle piattaforme di comunicare le proprie pratiche in maniera comprensibile e di tradurre i principi etici dichiarati in comportamenti coerenti. La tutela dell'utente risulta quindi effettiva non quando le informazioni e le garanzie sono semplicemente presenti, ma quando queste consentono realmente alla persona di comprendere, controllare e, ove necessario, contestare il trattamento dei propri dati.

Il tema assume particolare rilevanza in prospettiva futura, considerando la crescente diffusione dell'intelligenza artificiale, della profilazione e dei sistemi algoritmici. L'evoluzione tecnologica renderà infatti sempre più necessario verificare non soltanto la conformità formale delle piattaforme alla normativa vigente, ma anche la loro capacità di mantenere un rapporto trasparente e responsabile con gli utenti. In tale prospettiva, il rapporto tra diritto, tecnologia ed etica continuerà a rappresentare un elemento fondamentale per garantire che l'innovazione digitale possa svilupparsi nel rispetto dei diritti e delle libertà delle persone.

Fonti Bibliografiche

- Article 29 Working Party, Guidelines on Transparency under Regulation 2016/679, WP260, 2018;
- CNIL, Deliberazione n. SAN-2019-001 del 21 gennaio 2019. Cfr. anche G. CASSANO - G. SCORZA (a cura di), Diritti degli utenti e piattaforme digitali, Pisa, Pacini Giuridica, 2023;
- CNIL, Deliberazione n. SAN-2019-001 del 21 gennaio 2019; vedi anche Deliberazione n. SAN-2021-023 del 31 dicembre 2021;
- E. D’Orazio, Responsabilità sociale ed etica d’impresa, in Notizie di Politeia, Politeia, Milano, 2003;
- E. Freeman, Strategic Management: A Stakeholder Approach, Boston, Pitman, 1984;
- EDPS Ethics Advisory Group | Report 2018;
- European Data Protection Board, Guidelines 4/2019 on Article 25 – Data Protection by Design and by Default, Version 2.0, 20 ottobre 2020;
- G. Finocchiaro, Il Regolamento europeo sulla protezione dei dati personali, Bologna, Zanichelli, 2017;
- Garante per la protezione dei dati personali;
- Garante per la protezione dei dati personali, Linee guida in materia di trasparenza, 2018;
- Garante per la protezione dei dati personali, Rendere le informative privacy più comprensibili. Il legal design come approccio rivolto all’utente, White Paper, 2025;
- Google LLC, Code of Conduct;
- Google LLC, Google AI Principles;
- Google LLC, Norme sulla privacy, policies.google.com/privacy;
- High-Level Expert Group on Artificial Intelligence, Ethics Guidelines for Trustworthy AI, Commissione europea, 2019;
- Internet e il diritto, Milano, Giuffrè, 2013;
- ISO/IEC 27701:2019, Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management;
- L. Floridi, Etica dell’intelligenza artificiale. Sviluppi, opportunità, sfide, Raffaello Cortina Editore, Milano, 2022;
- LinkedIn, Privacy Policy;
- Meta Platforms, Informativa sulla privacy, versione vigente, Centro per la privacy di Meta;
- Meta, Code of Conduct;
- Meta, Community Standards;

- Organisation for Economic Co-operation and Development, OECD Guidelines for Multinational Enterprises on Responsible Business Conduct, OECD Publishing, Paris, 2023;
- Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016 (GDPR);
- Regolamento (UE) 2022/2065 (Digital Services Act);
- Sito del Garante per la protezione dei dati personali - <https://www.garanteprivacy.it>;