UNIVERSITÀ DEGLI STUDI DI PAVIA

DIPARTIMENTO DI GIURISPRUDENZA, INGEGNERIA INDUSTRIALE E DELL'INFORMAZIONE, SCIENZE ECONOMICHE E AZIENDALI, SCIENZE POLITICHE E SOCIALI, STUDI UMANISTICI

CORSO DI LAUREA INTERDIPARTIMENTALE IN COMUNICAZIONE DIGITALE

IL RUOLO DELLA PROTEZIONE DEI DATI E DELL'INTELLIGENZA ARTIFICIALE NELLA GESTIONE DEL RISCHIO DIGITALE D'IMPRESA

Relatore:
Chiar.mo Prof. Emanuele Tuccari
Correlatore:
Chiar.mo Prof. Flavio Antonio Ceravolo

Tesi di Laurea Magistrale di Maria El handour
Matricola n. 544154

ANNO ACCADEMICO 2024-2025

ABSTRACT

Negli ultimi anni, la trasformazione digitale ha profondamente modificato le modalità attraverso cui individui, imprese e istituzioni producono, comunicano e gestiscono informazioni. L'aumento esponenziale dei dati trattati e la diffusione di tecnologie avanzate hanno reso la sicurezza informatica e la protezione dei dati personali elementi centrali per il funzionamento e la credibilità delle organizzazioni nel contesto digitale. In questo scenario, la Cybersecurity non rappresenta soltanto un insieme di misure tecniche, ma una componente strategica della gestione d'impresa e della costruzione della fiducia.

Il presente lavoro analizza il rapporto tra Cybersecurity, disciplina della protezione dei dati personali e utilizzo dell'Intelligenza Artificiale, con particolare attenzione al quadro normativo europeo delineato dal Regolamento (UE) 2016/679 (GDPR) e dalla Direttiva (UE) 2016/1148 (NIS). L'obiettivo della ricerca è quello di esaminare come l'adozione di sistemi di intelligenza artificiale incida sull'applicazione concreta dei principi del GDPR, mettendo in luce sia le potenzialità dell'IA come strumento di supporto alla compliance, sia le criticità e i rischi che essa introduce in termini di trasparenza, accountability, sicurezza e tutela dei diritti degli interessati.

Attraverso un'analisi teorica e l'esame di casi applicativi, la tesi evidenzia come l'impiego dell'Intelligenza Artificiale renda più complessa la gestione dei dati personali, richiedendo un rafforzamento dei modelli organizzativi, dei meccanismi di controllo e delle strategie di potere. In particolare, emerge come le difficoltà non derivino esclusivamente dalla tecnologia in sé, ma dal modo in cui essa viene integrata nei processi aziendali e nelle strutture decisionali.

Il lavoro si conclude sottolineando la necessità di un approccio integrato alla sicurezza digitale, in cui Cybersecurity, protezione dei dati e Intelligenza Artificiale siano considerate dimensioni interconnesse di una stessa strategia di responsabilità e sostenibilità. In tale prospettiva, la tutela dei dati personali non costituisce un limite all'innovazione tecnologica, ma una condizione essenziale per uno sviluppo digitale consapevole e conforme ai diritti fondamentali.

INDICE

INTRODUZIONE

La presente tesi si propone di analizzare il rapporto tra Cybersecurity, protezione dei dati e comunicazione d'impresa, con l'obiettivo di comprendere come la sicurezza delle informazioni possa rappresentare un elemento determinante per la costruzione della fiducia digitale. Attraverso un approccio interdisciplinare che unisce prospettive giuridiche e comunicative, il lavoro intende evidenziare il valore strategico della gestione sicura dei dati come sistema di reputazione, responsabilità e competitività nel contesto dell'economia digitale.

La trasformazione digitale ha inciso in modo profondo sulle modalità attraverso cui le imprese operano, comunicano e costruiscono relazioni con i propri interlocutori. L'uso sempre più diffuso di tecnologie informatiche, piattaforme online e sistemi di gestione dei dati ha determinato un cambiamento strutturale nei processi aziendali, rendendo la dimensione digitale un elemento imprescindibile dell'attività economica e organizzativa. La comunicazione d'impresa si svolge prevalentemente attraverso canali digitali e si fonda su un flusso continuo di informazioni, che coinvolge dati personali, dati aziendali e sistemi informativi complessi.

La centralità dei dati nell'economia digitale ha portato a una crescente attenzione verso i temi della Cybersecurity e della protezione dei dati personali. Le informazioni raccolte e trattate dalle imprese rappresentano oggi una risorsa strategica fondamentale, utile per migliorare l'efficienza dei processi, personalizzare i servizi e rafforzare il rapporto con clienti e stakeholder. Allo stesso tempo, però, l'utilizzo intensivo dei dati espone le organizzazioni a rischi significativi, legati a violazioni della sicurezza, accessi non autorizzati e utilizzi impropri delle informazioni. Tali eventi non producono soltanto conseguenze tecniche o economiche, ma incidono direttamente sulla reputazione aziendale e sulla fiducia degli utenti.

La Cybersecurity non può essere considerata un ambito esclusivamente tecnico, riservato agli specialisti informatici, ma assume una dimensione trasversale che coinvolge l'intera organizzazione. La sicurezza dei sistemi informativi e la protezione dei dati personali diventano parte integrante della strategia d'impresa e della sua comunicazione istituzionale. Un'azienda che dimostra attenzione alla sicurezza delle informazioni comunica implicitamente affidabilità, responsabilità e rispetto nei confronti delle persone

con cui interagisce. Al contrario, una gestione superficiale o inadeguata dei dati può compromettere in modo duraturo l'immagine e la credibilità dell'organizzazione.

La crescente complessità dell'ambiente digitale ha reso necessario l'intervento del legislatore europeo, che negli ultimi anni ha introdotto un quadro normativo articolato e stringente in materia di protezione dei dati e sicurezza informatica. Il Regolamento generale sulla protezione dei dati personali (GDPR) ha rappresentato una svolta significativa, ponendo al centro del sistema i diritti e le libertà fondamentali delle persone fisiche e imponendo alle imprese un approccio basato sulla responsabilizzazione e sulla gestione del rischio. La normativa europea non si limita a prescrivere obblighi formali, ma richiede alle organizzazioni di dimostrare concretamente di aver adottato misure tecniche e organizzative adeguate alla natura dei trattamenti effettuati.

La protezione dei dati personali si inserisce così in un più ampio processo di cambiamento culturale che coinvolge le imprese. Il rispetto della normativa non è più sufficiente se non è accompagnato da una reale consapevolezza dei rischi e delle responsabilità connesse al trattamento delle informazioni. In questa prospettiva, la sicurezza digitale diventa un elemento essenziale della *governance* aziendale e un fattore determinante per la costruzione della fiducia digitale, intesa come la percezione di affidabilità e trasparenza da parte degli utenti.

La presente tesi si propone di analizzare il rapporto tra Cybersecurity, protezione dei dati personali e comunicazione d'impresa, con l'obiettivo di evidenziare come la gestione sicura delle informazioni rappresenti oggi una leva strategica per le organizzazioni. L'analisi si colloca all'interno di un approccio interdisciplinare che integra aspetti giuridici, tecnologici e comunicativi, in linea con il percorso di studi in Comunicazione Digitale. L'intento non è soltanto quello di descrivere il quadro normativo di riferimento, ma anche di comprendere le conseguenze concrete che tali regole hanno sull'organizzazione e sulla comunicazione delle imprese.

Nel presente lavoro, l'Intelligenza Artificiale non viene analizzata come fenomeno tecnologico autonomo, bensì come strumento potenzialmente in grado di supportare l'attuazione concreta della disciplina della protezione dei dati personali. L'attenzione è rivolta, in particolare, al contributo che l'IA può offrire in termini di sicurezza, *accountability* e gestione del rischio, nonché ai limiti e alle criticità che emergono nel suo impiego a fini di *data protection*.

Il **primo capitolo** della tesi è dedicato all'analisi dei fondamenti concettuali della Cybersecurity e della protezione dei dati personali. In questa parte vengono esaminati i principali significati attribuiti al concetto di Cybersecurity, il suo sviluppo nel contesto della società digitale e il suo ruolo all'interno delle aziende. Il capitolo approfondisce inoltre i principi alla base della sicurezza delle informazioni, come la riservatezza, l'integrità e la disponibilità dei dati, mettendo in luce il legame tra sicurezza informatica e tutela dei diritti fondamentali. Una sezione rilevante è dedicata al Regolamento generale sulla protezione dei dati personali, analizzato attraverso le definizioni di dato personale, trattamento, titolare e responsabile del trattamento, nonché attraverso l'esame dei principi generali che regolano la gestione dei dati. L'obiettivo del capitolo è fornire un quadro teorico e normativo di riferimento, indispensabile per comprendere le successive analisi.
Il **secondo capitolo** si concentra sull'impatto del GDPR e della Cybersecurity sulle imprese, analizzando obblighi, rischi e trasformazioni organizzative derivanti dalla digitalizzazione. In questa parte vengono approfonditi gli effetti concreti della normativa europea sull'attività aziendale, con particolare attenzione agli adempimenti richiesti, al sistema sanzionatorio e alle conseguenze economiche e reputazionali delle violazioni dei dati. Inoltre, i l capitolo esamina strumenti operativi fondamentali, come il registro delle attività di trattamento e la valutazione d'impatto sulla protezione dei dati (DPIA), evidenziando le difficoltà e le sfide che le imprese incontrano nell'adeguarsi alle disposizioni normative. Viene inoltre analizzato il ruolo della Cybersecurity nella prevenzione degli incidenti informatici e nella gestione del rischio, nonché l'impatto delle nuove tecnologie, come l'Internet of Things, sulla protezione dei dati personali. L'analisi è completata da un caso di studio, utile per comprendere in modo concreto le conseguenze di una gestione non conforme dei dati.
Il **terzo capitolo** è dedicato all'analisi del ruolo dell'Intelligenza Artificiale all'interno delle imprese, con particolare riferimento alla protezione dei dati e alla sicurezza informatica. In questa sezione vengono esaminate le opportunità offerte dai sistemi di IA in termini di efficienza, automazione dei processi e creazione di valore, insieme alle criticità legate alla trasparenza degli algoritmi, alla protezione dei dati personali e ai rischi connessi ai trattamenti automatizzati. Il capitolo approfondisce i principi fondamentali della protezione dei dati applicati ai sistemi di Intelligenza Artificiale e analizza il ciclo di vita di tali sistemi, evidenziando come l'IA rappresenti un nuovo paradigma nella

gestione delle informazioni aziendali. L'attenzione è rivolta anche alle complessità organizzative e comunicative dell'adozione di tecnologie intelligenti.

Il **quarto capitolo** è dedicato all'analisi delle criticità e dei rischi che l'adozione dell'Intelligenza Artificiale comporta per l'applicazione concreta della disciplina della protezione dei dati personali. L'attenzione è rivolta, in particolare, alle difficoltà operative, organizzative che possono incidere sul rispetto dei principi del GDPR, nonché ai rischi legati alla trasparenza dei sistemi automatizzati, ai bias algoritmici e al trattamento dei dati personali. Il capitolo include inoltre l'esame di un caso concreto di applicazione dell'IA in ambito industriale, al fine di evidenziare come tali criticità si manifestino nella pratica e quali implicazioni ne derivino in termini di tutela dei diritti degli interessati e di accountability del titolare del trattamento.

Nel suo insieme, la tesi offre una visione organica e integrata della Cybersecurity come componente essenziale della comunicazione d'impresa. La sicurezza delle informazioni non emerge soltanto come un obbligo normativo, ma come un elemento strategico capace di incidere sulla reputazione, sulla fiducia degli utenti e sulla sostenibilità delle organizzazioni nel lungo periodo. Proteggere i dati significa tutelare le persone, garantire trasparenza e rafforzare la credibilità dell'impresa in un contesto digitale sempre più complesso e competitivo.

CAPITOLO PRIMO

FONDAMENTI CONCETTUALI DELLA CYBERSECURITY E DELLA PROTEZIONE DEI DATI

Il mondo digitale sta trasformando in modo significativo i metodi operativi delle aziende rinnovando sia la gestione delle informazioni sia le strategie di comunicazione e le attività aziendali nel loro complesso. L'essere connessi sempre più strettamente tra individui, organizzazioni e tecnologie ha fatto della dimensione digitale un'estensione naturale della vita quotidiana e professionale. Tuttavia, questa evoluzione ha introdotto nuove vulnerabilità e rischi, la cui considerazione è necessaria quando si tratta il problema della sicurezza informatica.

Il termine Cybersecurity non possiede una definizione univoca e universalmente condivisa. Sebbene venga spesso tradotto come "sicurezza informatica"[1], tale espressione descrive solo in parte la complessità del fenomeno. La Cybersecurity in realtà rappresenta infatti un sottoinsieme del più ampio concetto di *information security*[2], poiché riguarda in modo specifico la protezione tecnologica e digitale delle informazioni, dei sistemi e delle infrastrutture di rete.

La parola *Cyber* viene dal greco e significava "arte di guidare il timone di una nave". Oggi indica il fatto che le persone possono muoversi e incontrarsi nello stesso spazio virtuale: il web.

La sicurezza informatica è diventata un argomento molto importante quando si parla di protezione dei dati. Poiché usiamo sempre più spesso strumenti digitali, questi hanno un grande impatto sul modo in cui i dati vengono protetti e gestiti.

L'Unione Europea, consapevole del continuo sviluppo della tecnologia, interviene più volte su questo tema. Per questo esistono molte norme che obbligano chi gestisce i dati a prendere misure adeguate per garantire la sicurezza, anche dal punto di vista organizzativo, all'interno delle aziende. Alcune regole, ad esempio, richiedono

[1] P.L. Montessoro, *Cybersecurity: conoscenza e consapevolezza come prerequisiti per l'amministrazione digitale*, in *Istituzioni del federalismo*, 2019, 3.

[2] Vittorio Salvatore Piccolo, *Principi e pratiche della cybersecurity. Fondamenti e applicazioni*, Milano, Apogeo, 2021, p.5.

chiaramente di usare sistemi di protezione come la crittografia e di avere metodi per recuperare i dati in caso di problemi o danni. Queste indicazioni sottolineano quanto sia importante che chi tratta i dati faccia attenzione agli strumenti informatici utilizzati.
L'intero Regolamento europeo si basa su un approccio fondato sul rischio, che riguarda inevitabilmente anche le incertezze e i pericoli legati alla sicurezza informatica.
Secondo il Regolamento (UE) 2019/881, noto come *Cybersecurity Act*, la Cybersecurity comprende "l'insieme delle attività necessarie per proteggere le reti, i sistemi informativi, gli utenti e le persone interessate dalle minacce informatiche"[3].
Nella società attuale – in cui siamo sempre più invasi da dispositivi digitali come computer, smartphone o piattaforme digitali – c'è una condivisione permanente di dati personali: *"qualsiasi informazione riguardante una persona fisica identificata o identificabile (interessato), si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale [4]".* Ogni volta che un utente accede a un servizio online o crea un profilo digitale, si trova a fornire i dati personali più sensibili, spesso senza essere pienamente consapevole di come queste verranno trattate o conservate. Ciò solleva un interrogativo centrale: chi controlla realmente il destino dei dati e come può essere garantita la loro protezione? Per rispondere a tali domande, la Cybersecurity adotta un approccio basato su tre principi fondamentali: riservatezza, integrità e disponibilità (modello RID).

- La riservatezza assicura che i dati siano accessibili solo a soggetti autorizzati, evitando divulgazioni non consentite.
- L'integrità assicura che i dati non subiscano modifiche o corruzioni non autorizzate nel corso del loro ciclo di vita.
- La disponibilità garantisce che i dati e i sistemi siano sempre accessibili e operativi quando necessario.

Questi tre principi rappresentano l'essenza della fiducia digitale e la base tecnica per la piena attuazione del Regolamento (UE) 2016/679 (GDPR), che tutela i diritti e le libertà

[3] Regolamento (UE) 2019/881, Cybersecurity Act, art. 2.
[4] Regolamento (UE) 2016/679 (GDPR), art..4 n.1.

fondamentali delle persone fisiche rispetto al trattamento dei dati personali.[5] Al contempo, il GDPR specifica che la sicurezza dei dati è un meccanismo di garanzia delle libertà individuali e non un requisito di natura tecnica.

Nella dimensione digitale, la Cybersecurity e la protezione dei dati personali non rappresentano ambiti separati, ma si completano a vicenda: la Cybersecurity fornisce gli strumenti tecnici per garantire la protezione dei dati, mentre il rispetto delle norme contribuisce a rafforzare la fiducia e la reputazione dell'impresa. Come osservava Nicholas Negroponte (1995), la sicurezza digitale rappresenta la condizione necessaria affinché l'utente possa sentirsi protetto rispetto all'ambiente esterno, creando così un contesto di fiducia all'interno dell'ecosistema informativo [6].

Tuttavia, negli ultimi anni, il numero e la gravità degli attacchi informatici sono aumentati in modo esponenziale, coinvolgendo non solo governi e grandi imprese, ma anche piccole e medie realtà produttive. I dati personali e aziendali sono diventati uno dei beni più preziosi, e allo stesso tempo vulnerabili. Non a caso, nel 2017, l'allora Presidente della Commissione Europea, Jean-Claude Juncker, affermò che "la Cybersecurity è la seconda emergenza in Europa, dopo il cambiamento climatico e prima dell'immigrazione".[7]

Alla luce di tali sfide, la sicurezza informatica deve essere considerata una priorità strategica per le imprese contemporanee. Essa non si limita a un insieme di misure tecniche, ma comporta una vera e propria cultura della sicurezza, fondata su formazione, consapevolezza e responsabilità condivisa. Solo in questo modo la trasformazione digitale potrà realizzarsi in un contesto di fiducia, sostenibilità e tutela dei diritti individuali.

Dopo aver evidenziato l'importanza centrale della sicurezza digitale nel processo di trasformazione tecnologica, il passo successivo consiste nell'esaminare nel dettaglio il concetto di Cybersecurity e la sua connessione con la tutela dei dati personali. Tale analisi risulta fondamentale per delineare l'aspetto teorico e normativo entro la quale si inserisce la comunicazione d'impresa.

[5] Regolamento (UE) 2016/679, (GDPR), artt. 4 e 5.
[6] N. Negroponte, Essere digitali, Sperling & Kupfer, Milano, Sperling & Kupfer, 1995.
[7] Jean-Claude Junker, Avvocato e ex Presidente della Commissione europea, interventi e dichiarazioni sul digitale e sull'integrazione europea (2014-2019).

1.1 Una definizione generale di Cybersecurity

Nell'attuale contesto digitale, in continua espansione e presente in ogni aspetto della nostra vita, sia privata che pubblica, la sicurezza riveste un ruolo fondamentale. Senza adeguati sistemi di protezione, l'intero ecosistema digitale sarebbe a rischio di gravi malfunzionamenti o collassi. In questo quadro, la Cybersecurity, in particolare nel settore delle tecnologie dell'informazione, assume un'importanza cruciale. Negli ultimi decenni, questo ambito ha registrato progressi significativi, diventando il principale punto di riferimento per proteggere i nostri dati e interessi in caso di frodi o minacce digitali.

Secondo il NIST (National Institute of Standards and Technology), agenzia governativa statunitense che sviluppa e promuove standard tecnologici, compresi quelli per la sicurezza informatica, la Cybersecurity è definita come *"la prevenzione del danneggiamento, dell'uso non autorizzato, dello sfruttamento e, se necessario, del ripristino dei sistemi elettronici di informazione e comunicazione e delle informazioni in essi contenute, al fine di rafforzare la riservatezza, l'integrità e la disponibilità di tali sistemi." (NIST2017)*[8]. Questo implica che uno degli aspetti fondamentali della Cybersecurity è capire come prevenire e gestire eventuali incidenti di sicurezza informatica.

In pratica, la Cybersecurity comprende un insieme di misure volte a proteggere le informazioni scambiate attraverso sistemi aziendali globalmente connessi. Essa consiste nella protezione di reti, sistemi e applicazioni da attacchi digitali che possono compromettere l'accesso, modificare o distruggere dati sensibili, estorcere informazioni o interrompere i normali processi aziendali. L'obiettivo principale è garantire la riservatezza, l'integrità, la disponibilità e l'autenticità delle informazioni.

La Cybersecurity coinvolge aspetti tecnici, organizzativi, giuridici e umani, ed è finalizzata all'analisi delle vulnerabilità, delle minacce e dei rischi legati ai sistemi informatici. La sua importanza è particolarmente evidente per le aziende, in quanto protegge dati e risorse sia durante l'uso locale sia nel trasferimento di informazioni attraverso reti, dispositivi e utenti finali. In questo senso, la Cybersecurity assume una funzione sociale, oltre che tecnica: garantire la sicurezza delle infrastrutture digitali

[8] Definizione glossario: National Institute of Standards and Technology (NIST), *Glossary of Key Information Security Terms*, NISTIR 7298 Rev. 3.

significa tutelare la fiducia nelle attività economiche, nella comunicazione d'impresa e, più in generale, nel funzionamento delle istituzioni democratiche. La dimensione della fiducia, infatti, costituisce un presupposto essenziale affinché individui e organizzazioni possano interagire in un ambiente digitale percepito come sicuro.

In termini scientifici, la Cybersecurity può essere definita come l'insieme di politiche, processi, pratiche e strumenti finalizzati alla protezione di reti, sistemi, dati e infrastrutture digitali da minacce informatiche intenzionali o accidentali. Questa prospettiva comprende non solo la difesa da attacchi esterni, ma anche la riduzione delle vulnerabilità interne, la gestione dei rischi, la resilienza operativa e la capacità di risposta a incidenti. L'elemento centrale di tale approccio è il riconoscimento del rischio come dimensione intrinseca dell'ecosistema digitale, dovuto alla sua complessità crescente e alla sua continua evoluzione.

La Cybersecurity rappresenta una parte specifica della *sicurezza delle informazioni* (Information Security), concentrandosi in particolare sulle minacce informatiche e sulla protezione dei dati digitali.[9] La sicurezza delle informazioni, invece, ha un ambito più ampio, include non solo i dati digitali, ma anche documenti cartacei, informazioni sensibili e dati riservati. Quindi, per concludere, sia la Cybersecurity sia l'information security mirano a tutelare tutte le informazioni e i dati di un'organizzazione, adottando approcci completi che considerano sia il mondo fisico sia quello digitale.

1.1.1 Aspetti principali della Cybersecurity

È fondamentale comprendere che la Cybersecurity si concentra sulla protezione dei dati prevenendo accessi non autorizzati, mentre la sicurezza informatica, in senso più ampio, si estende anche alla protezione delle informazioni da accessi legittimi ma potenzialmente dannosi o errati. Entrambe le forme di sicurezza risultano quindi cruciali per le aziende, poiché negli ultimi anni numerose imprese, indipendentemente dalle loro dimensioni, hanno subito violazioni e attacchi informatici.

La sicurezza dei sistemi informatici si fonda su quattro principi fondamentali:

1. **Disponibilità:** indica la capacità del sistema di operare correttamente e di restare accessibile agli utenti autorizzati in qualsiasi momento, evitando interruzioni o

[9] Agenzia dell'Unione europea per la cybersicurezza (ENISA), definizione di *cybersecurity*.

problemi tecnici rilevanti. L'obiettivo è garantire che tutte le funzioni richieste siano sempre attive.

2. **Riservatezza:** riguarda la protezione dei dati durante lo scambio tra mittente e destinatari autorizzati, impedendo l'accesso, la lettura o l'intercettazione da parte di persone non autorizzate.
3. **Integrità:** assicura che i dati rimangano accurati, coerenti e affidabili, prevenendo modifiche accidentali o intenzionali da parte di terzi.
4. **Autenticità delle informazioni:** garantisce che i dati provengano da fonti autorizzate e che ogni modifica sia effettuata solo da sistemi o soggetti legittimi, confermando così la validità delle informazioni.

Questi pilastri sono strettamente interconnessi e costituiscono la base per creare un ambiente informatico sicuro, in cui le informazioni possano essere scambiate e utilizzate in modo protetto ed efficiente.

Le aziende possono usufruire dei vantaggi delle tecnologie di Cybersecurity anche senza possederle internamente. Infatti, esistono imprese specializzate nella fornitura di servizi di sicurezza informatica, che possono agire come partner esterni o essere acquisite da aziende che necessitano di protezione avanzata contro gli attacchi informatici.

1.1.2 La Cybersecurity: la società nell'era digitale

Se si osserva la realtà attuale, è evidente che viviamo in un mondo costantemente "intelligente" e connesso.

La diffusione delle tecnologie digitali ha trasformato profondamente la vita quotidiana e il funzionamento della società contemporanea. Oggi molte attività — comunicare, lavorare, studiare, fare acquisti o accedere a servizi pubblici — si svolgono online o tramite dispositivi connessi, generando vantaggi significativi in termini di velocità, efficienza e accesso immediato a servizi che fino a pochi decenni fa richiedevano tempi e procedure molto più complessi. Questa trasformazione, tuttavia, comporta nuove vulnerabilità. L'uso diffuso di internet e di dispositivi connessi aumenta la possibilità che dati personali vengano raccolti, analizzati o utilizzati senza piena consapevolezza dell'utente. Tecniche di profilazione, tracciamento online e sistemi di videosorveglianza

intelligenti possono minacciare la privacy, generando rischi significativi soprattutto per chi non adotta comportamenti consapevoli.

Oltre alla privacy, crescono le minacce legate alla sicurezza informatica. Virus, malware, attacchi informatici e furti di dati possono colpire chiunque, dai singoli cittadini alle grandi organizzazioni. La continua interconnessione tra reti, dispositivi e servizi aumenta la complessità della protezione, perché anche una piccola vulnerabilità può avere conseguenze gravi su scala locale o globale[10].

Per ridurre questi rischi, l'Unione Europea ha introdotto strumenti normativi specifici. Il Regolamento Generale sulla Protezione dei Dati (GDPR) tutela i diritti fondamentali degli individui e promuove principi come minimizzazione dei dati, trasparenza dei trattamenti e responsabilizzazione dei titolari. La direttiva NIS2 impone obblighi di sicurezza più rigorosi agli operatori di servizi essenziali e ai fornitori di infrastrutture critiche[11], mentre il *Cyber Resilience Act* mira a garantire che i prodotti digitali siano sicuri lungo tutto il loro ciclo di vita[12].

In questo contesto, la Cybersecurity non è più solo una questione tecnica, ma è anche un elemento strategico, sociale ed economico. Proteggere sistemi digitali, dati personali e infrastrutture critiche è fondamentale per garantire continuità dei servizi, fiducia dei cittadini e resilienza della società nell'era digitale. Comprendere i rischi e adottare comportamenti consapevoli è essenziale per affrontare in modo sicuro le sfide di un mondo sempre più interconnesso.

1.1.3 La Cybersecurity nelle aziende

Le aziende oggi sono chiamate a dotarsi di strategie e politiche di sicurezza informatica chiare e strutturate, con l'obiettivo di tutelare i propri beni digitali, garantire la conformità alle normative vigenti e assicurare la continuità operativa in un contesto caratterizzato da minacce informatiche in costante evoluzione.

[10] J. Andress, *The Basics of Information Security. Understanding the Fundamentals of InfoSec in Theory and Practice*, 2ª ed., Waltham, Syngress, 2019, p. 151.
[11] Direttiva (UE) 2022/2555 (NIS 2).
[12] Commissione europea, Proposta di regolamento relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali (Regolamento sulla ciberresilienza), Bruxelles, 2023.

Sviluppare una strategia complessiva e coerente per la gestione della sicurezza significa fornire all'organizzazione una guida per individuare e valutare i rischi, prevenire gli attacchi e reagire in modo tempestivo agli incidenti, limitandone gli effetti negativi. In questo modo, la Cybersecurity diventa non solo una misura tecnica, ma un vero e proprio strumento di *governance* aziendale volto a garantire stabilità, affidabilità e fiducia all'interno dell'ecosistema digitale.

Secondo l'Agenzia Europea per la Cybersicurezza un *cyber attack* comprende "*tutti gli incidenti informatici scatenati da un intento malevolo, in cui si verificano danni, interruzioni o disfunzioni"*[13]. In altri termini, questi incidenti di sicurezza consistono nella presa di mira da parte di malintenzionati di uno o più elementi della sicurezza informatica. L'incremento delle minacce informatiche è il principale motivo per l'aumento dell'attenzione alla sicurezza informatica.

Nel contesto economico attuale, caratterizzato da un'intensa digitalizzazione, il *cyber risk* rappresenta una minaccia crescente per le imprese di ogni settore e dimensione. L'aumento della connettività e l'uso diffuso delle tecnologie informatiche hanno portato vantaggi in termini di efficienza e innovazione, ma hanno anche esposto le aziende a nuove vulnerabilità, come la perdita di dati sensibili, il furto di proprietà intellettuale, gli attacchi ai sistemi di pagamento online e le interruzioni operative, con possibili conseguenze economiche e legali.

Affrontare un attacco informatico non riguarda solo la sicurezza dei sistemi informatici, ma è un aspetto fondamentale della gestione aziendale, perché influisce sulla stabilità finanziaria e sulla reputazione. Per proteggersi, le aziende devono adottare un sistema di sicurezza informatica che prevede la verifica costante delle vulnerabilità, l'uso di strumenti di protezione avanzati, la formazione del personale e un piano per reagire rapidamente agli incidenti. Collaborare con esperti e aggiornarsi sulle nuove minacce è essenziale per anticipare i rischi.

Il panorama delle minacce è in continua evoluzione, con nuovi modi di sfruttare debolezze note e sconosciute. Per questo motivo, le aziende devono non solo proteggersi dagli attacchi, ma anche essere resilienti, ossia capaci di rispondere rapidamente e limitare i danni, ripristinando le operazioni nel minor tempo possibile.

[13] Agenzia dell'Unione europea per la cybersicurezza (ENISA), definizione di *cyber attack.*

La crescente regolamentazione in materia di sicurezza informatica sottolinea l'importanza di misure preventive e piani di risposta strutturati. Investire in tecnologie di sicurezza, formazione del personale e politiche di gestione del rischio digitale diventa quindi parte integrante della strategia aziendale.

La Cybersecurity ha anche un valore reputazionale, garantire la sicurezza dei dati raccolti e trasmessi attraverso i canali digitali rafforza la fiducia di clienti e partner, consolidando l'identità comunicativa dell'azienda. Come sottolineato nel libro *Business Model 4.0* [14], gestire i dati in modo sicuro è oggi una risorsa fondamentale per la competitività, perché aiuta a prevenire violazioni e sanzioni e a migliorare la reputazione sul mercato.

In un mondo digitale sempre più connesso, proteggere i dati sensibili e gestirli in modo trasparente significa anche assumersi responsabilità sociale, comunicare in sicurezza equivale a comunicare in modo responsabile e trasparente.

Ogni anno il numero degli attacchi informatici tende ad aumentare.

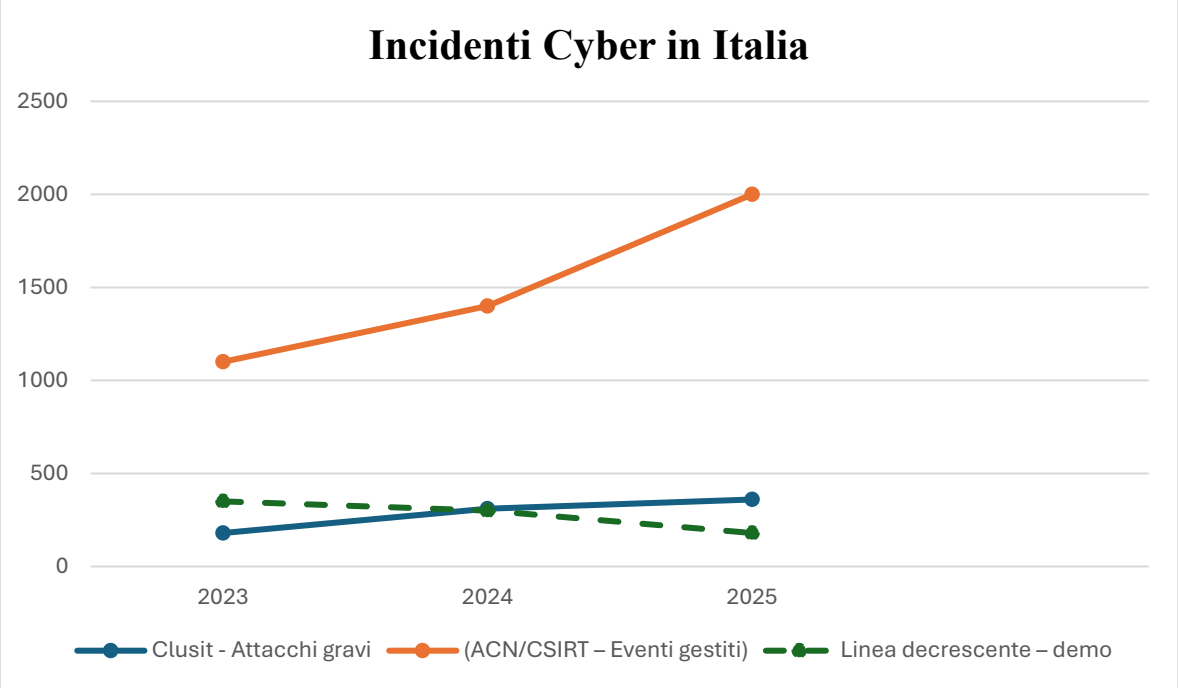

Figura 1: Andamento degli incidenti cyber nel periodo dal 2022 al 2024

Tra il 2020 e il 2025, in Italia la questione Cybersicurezza è diventata una questione sempre più centrale nella strategia aziendale e nella *governance* nazionale. Nel 2023

[14] C. Bagnoli, A. Bravin, M. Massaro, *Business Model 4.0*, Milano, FrancoAngeli, 2018, p. 112.

l'ACN: Agenzia per la cybersicurezza nazionale ha registrato ben *1.411 attacchi cyber*, con un aumento del 29% rispetto all'anno precedente[15]. Nel 2024 il numero di eventi monitorati è salito a *1.979 incidenti*, con *573 incidenti confermati* (+89% rispetto al 2023)[16]. Nel primo semestre del 2025, l'ACN ha già rilevato 1.549 eventi, con un incremento del 53% rispetto allo stesso periodo del 2024[17]. Questi dati confermano che, negli ultimi tre anni, il panorama delle minacce informatiche ha subito un'accelerazione significativa, rendendo imprescindibile per le imprese integrare la gestione del *cyber risk* nelle proprie strategie operative e di continuità.

1.2 Il GDPR: definizioni e principi chiave

Il Regolamento generale sulla protezione dei dati personali, noto con l'acronimo GDPR *(General Data Protection Regulation*) e identificato come Regolamento (UE)n. 2016/679, costituisce il principale strumento normativo dell'Unione europea in materia di tutela della privacy e trattamento dei dati personali.

Adottato il 27 aprile 2016 e pubblicato nella Gazzetta ufficiale dell'Unione europea il4 maggio 2016, il regolamento è entrato in vigore il 24 maggio 2016 ed è divenuto pienamente applicabile il 25 maggio 2018 [18].

Poiché si tratta di un regolamento europeo e non di una direttiva, le disposizioni sono direttamente vincolanti per tutti gli Stati membri, senza necessità di recepimento tramite leggi nazionali, garantendo così un'applicazione uniforme delle norme in tutta l'Unione. In Italia, tuttavia, che già disponeva di una disciplina nazionale per la protezione dei dati personali, il GDPR ha comportato una modifica del Codice della privacy a seguito dell'emanazione del d.lgs. n. 101/2018, al fine di adeguare la normativa nazionale alle disposizioni europee.

L'origine del GDPR risale al 2012, quando la Commissione Europea presentò una riforma dell'allora Direttiva 95/46/CE, divenuta ormai inadeguata rispetto ai rapidi cambiamenti

[15] Redazione ANSA, «411 attacchi cyber nel 2023 in Italia: aumento del 29%», ANSA, 24 aprile 2024, fonte giornalistica online, consultata il 10 novembre 2025, https://www.ansa.it/.
[16] Redazione ANSA, «Raddoppiati gli incidenti cyber in Italia nel 2024», ANSA, 13 maggio 2025, fonte giornalistica online, consultata il 10 novembre 2025, https://www.ansa.it/.
[17] Cybersecurity Italia, «Attacchi cyber in Italia: 53 gli eventi nel primo semestre 2025», *Cybersecurityitalia.it,* consultato il 10 novembre 2025, https://www.Cybersecurityitalia.it/.
[18] Centro Studi Fiscali SEAC (a cura di), *GDPR e codice privacy. Le regole per studi e aziende*, SEAC, Trento, 2025, p. 11.

tecnologici e dell'evoluzione digitale. Nel 2010 ci furono le prime riflessioni sul futuro della protezione dei dati personali, che portarono alla presentazione del "Pacchetto di protezione dei dati" da parte della Commissione il 25 gennaio 2012 [19]. L'obiettivo era quello di rafforzare i diritti dei cittadini in ambito digitale e favorire lo sviluppo dell'economia fondata sui dati.

Il percorso legislativo proseguì con l'approvazione del Parlamento Europeo il 12 marzo 2014 (621 voti favorevoli, 10 contrari e 22 astenuti) e con l'accordo politico raggiunto il 17 dicembre 2015 tra Consiglio, Parlamento e Commissione Europea, che portò alla versione definitiva del testo nel 2016.

Il Regolamento, articolato in 99 articoli suddivisi in 11 capitoli, affronta in modo ampio e sistematico i temi della protezione dei dati personali. Uno degli elementi più innovativi del GDPR è la sua portata extraterritoriale. Il GDPR si applica non solo alle organizzazioni con sede nell'Unione europea, ma anche a quelle situate al di fuori dell'UE che offrono beni o servizi a persone nell'Unione o che monitorano il comportamento di individui presenti nel territorio europeo. Ciò significa, ad esempio, che se un cittadino francese utilizza un'applicazione sviluppata da un'azienda statunitense, come WhatsApp, i suoi dati devono comunque essere trattati nel rispetto delle disposizioni del GDPR.

1.2.1 Il concetto di dato personale e la questione dell'identificabilità dell'interessato

Il Regolamento (UE) 2016/679 (GDPR) definisce il "dato personale" come qualsiasi informazione riferita a una persona fisica identificata o identificabile [20]. Tale definizione ha portata molto ampia e comprende una molteplicità di informazioni, che possono riguardare direttamente o indirettamente un individuo. Ciò che rileva, infatti, non è la natura dell'informazione in sé, ma la sua capacità di ricondurre, anche potenzialmente, a un soggetto determinato.

Il punto più complesso da chiarire è cosa si intende esattamente per *persona fisica identificabile*. L'identificabilità non è un concetto statico, bensì dinamico, poiché dipende dal contesto e dai mezzi tecnici disponibili. Il legislatore europeo, al fine di precisare tale nozione, ha stabilito che una persona è da considerarsi identificabile quando può essere

[19] A. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali: dalla Direttiva 95/46 al nuovo Regolamento europeo*, Torino, Giappichelli, 2016, pp. 36–37.
[20] Regolamento (UE) 2016/679 (GDPR), art. 4, par. 1.

individuata, direttamente o indirettamente, attraverso un identificativo specifico o uno o più elementi caratteristici della sua identità[21].

Gli identificatori possono essere di diversa natura: anagrafica (come il nome o il numero di identificazione), economica (codice fiscale o coordinate bancarie), tecnologica (indirizzi IP, identificativi online), geografica (dati di localizzazione GPS), o ancora riguardare aspetti fisici, fisiologici, genetici, psichici, culturali e sociali. È quindi sufficiente che un dato, anche apparentemente neutro, possa permettere – da solo o combinato con altri – di risalire a una persona, affinché rientri nella categoria dei "dati personali".

Il criterio chiave per determinare se un'informazione consenta l'identificazione di un soggetto è quello della ragionevole probabilità; occorre valutare se, tenendo conto dei mezzi tecnici, dei costi e del tempo necessari, sia realisticamente possibile identificare una persona fisica[22]. Tale valutazione non è assoluta ma relativa, e deve essere condotta caso per caso, in considerazione dell'evoluzione delle tecnologie e del contesto di trattamento dei dati.

Ne consegue che l'identificabilità di un individuo non è un concetto oggettivo e immutabile, ma un parametro variabile nel tempo. Gli identificativi, dunque, non rappresentano elementi statici, bensì indicatori che consentono di stabilire, in concreto, se un'informazione possa essere qualificata come "dato personale".

1.2.2 Il trattamento dei dati personali e il ruolo dell'automatizzazione

Una volta chiarito il concetto di dato personale, è necessario individuare cosa si intenda per *trattamento* al fine di delimitare l'ambito applicativo del GDPR. L'articolo 4, paragrafo 2, definisce il trattamento come qualsiasi operazione o insieme di operazioni eseguite su dati personali, con o senza l'ausilio di strumenti automatizzati[23].

Rientrano in tale definizione attività molto diverse tra loro, come la raccolta, la registrazione, l'organizzazione, la conservazione, la modifica, la consultazione, la comunicazione, la diffusione o la cancellazione dei dati. Il legislatore, attraverso questa

[21] Ibidem.
[22] Regolamento (UE) 2016/679 (GDPR), considerando n. 26.
[23] Regolamento (UE) 2016/679 (GDPR), art. 4, par. 2.

formulazione ampia, ha inteso ricomprendere ogni possibile interazione con il dato personale, a prescindere dal mezzo tecnico impiegato.

Tuttavia, il Regolamento precisa che non tutte le operazioni sui dati rientrano necessariamente nel suo campo di applicazione. Il trattamento deve infatti essere automatizzato o, se manuale, riferirsi a dati contenuti in un archivio strutturato, ossia un insieme organizzato di informazioni accessibili secondo criteri determinati[24]. Tali archivi possono essere centralizzati o distribuiti, ma ciò che rileva è l'esistenza di un sistema che consenta un'interazione sistematica e continuativa tra il soggetto e i dati personali.

In sostanza, il criterio distintivo che attiva l'applicazione del GDPR è la presenza di strumenti o modalità organizzative che permettano un trattamento efficiente, sistematico e potenzialmente invasivo dei dati personali. È proprio in tali circostanze che emergono i maggiori rischi per i diritti e le libertà fondamentali delle persone fisiche cui i dati si riferiscono[25].

1.2.3 Il titolare e il responsabile del trattamento dei dati

Il titolare del trattamento (data controller) è definito come la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che, da solo o congiuntamente ad altri soggetti, stabilisce le finalità e i mezzi attraverso i quali vengono trattati i dati personali[26]. Tale figura riveste un ruolo centrale nel sistema di protezione dei dati, in quanto su di essa grava la responsabilità generale per ogni operazione di trattamento, sia essa svolta direttamente sia tramite altri soggetti che agiscono per suo conto.

Il titolare è pertanto tenuto ad adottare *misure tecniche e organizzative adeguate* a garantire che le attività di trattamento siano conformi al Regolamento (UE) 2016/679 (GDPR) e deve essere in grado di *dimostrarne l'efficacia e la conformità* [27]. Nella scelta di tali misure, egli deve considerare la natura, l'ambito di applicazione, il contesto e le finalità del trattamento, nonché i rischi potenziali per i diritti e le libertà delle persone fisiche, valutati in base alla loro probabilità e gravità[28].

[24] Regolamento (UE) 2016/679 (GDPR), art. 4, par. 6.
[25] Regolamento (UE) 2016/679 (GDPR), considerando nn. 15 e 26.
[26] Regolamento (UE) 2016/679 (GDPR), art. 4, par. 1, n. 7.
[27] Regolamento (UE) 2016/679 (GDPR), considerando n. 74.
[28] Regolamento (UE) 2016/679 (GDPR), art. 24, par. 1.

Rientra inoltre tra i compiti del titolare l'individuazione delle persone autorizzate al trattamento dei dati personali, assicurandosi che tali soggetti operino nel rispetto delle norme vigenti e delle istruzioni ricevute[29].

Per quanto riguarda i trattamenti basati sul consenso dell'interessato: "*qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso esprime il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, al trattamento dei dati personali che lo riguardano*[30]*",* il titolare deve essere in grado di dimostrare che il consenso sia stato espresso in modo libero, specifico, informato e inequivocabile. Tale consenso deve costituire una manifestazione di volontà chiara e diretta da parte dell'interessato, e l'onere della prova ricade sul titolare del trattamento. Qualora il consenso sia raccolto all'interno di una dichiarazione scritta che riguarda anche altre questioni, devono essere previste garanzie che assicurino la consapevolezza dell'interessato riguardo all'atto di prestare il consenso e alla sua portata.

Conformemente ai principi stabiliti dalla Direttiva 93/13/CEE, il *consenso* deve essere espresso mediante una dichiarazione formulata in modo comprensibile e accessibile, con un linguaggio semplice, chiaro e privo di clausole abusive; questa informativa preliminare consente all'interessato di esercitare un consenso effettivamente informato[31]. Ai fini della validità di tale consenso, l'interessato deve almeno essere informato sull'identità del titolare del trattamento e sulle finalità del trattamento stesso. Non si può ritenere che il consenso sia liberamente espresso qualora l'interessato non sia realmente in grado di scegliere, o se non può rifiutare o revocare il consenso senza subire conseguenze negative[32].

Per agevolare l'esercizio dei diritti riconosciuti all'interessato dal Regolamento, il titolare deve predisporre strumenti adeguati per consentire la presentazione delle richieste anche in formato elettronico, specialmente quando il trattamento avviene mediante sistemi informatici. Egli è obbligato a rispondere alle richieste dell'interessato entro un mese, senza ingiustificati ritardi, e a motivare la decisione nel caso in cui intenda non dare seguito a tali richieste[33].

---

[29] Regolamento (UE) 2016/679 (GDPR), considerando n. 29.
[30] Regolamento (UE) 2016/679 (GDPR), art. 4, Altalex, 24 gennaio 2019.
[31] Regolamento (UE) 2016/679 (GDPR), art. 12.
[32] Regolamento (UE) 2016/679 (GDPR), considerando n. 42.
[33] Regolamento (UE) 2016/679 (GDPR), considerando n. 59.

Il responsabile del trattamento (processor)

L'articolo 4 del Regolamento (UE) 2016/679 (GDPR) definisce il *responsabile del trattamento* come: "*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento*"[34]. Tale definizione, chiarisce la funzione che il responsabile opera nell'interesse del titolare e non in autonomia, limitandosi a svolgere le attività di trattamento secondo le finalità e le istruzioni fornite da quest'ultimo[35].

Un elemento centrale è presente dal paragrafo 1 dell'articolo 28 del GDPR, che impone al titolare, qualora decida di nominare un responsabile, di assicurarsi preventivamente che quest'ultimo offra garanzie sufficienti in termini di competenza tecnica e di misure organizzative idonee a garantire la tutela dei dati personali[36].

Una delle principali innovazioni introdotte dal Regolamento (UE) 2016/679 consiste nella possibilità, per il responsabile del trattamento, di avvalersi di sub-responsabili, previa autorizzazione scritta del titolare[37]. Tale delega può avere ad oggetto esclusivamente lo svolgimento di attività specifiche di trattamento e comporta, per il sub-responsabile, l'assunzione dei medesimi obblighi contrattuali che vincolano il responsabile principale nei confronti del titolare[38].

Il responsabile originario conserva, tuttavia, la responsabilità per le condotte del sub-responsabile, rispondendo verso il titolare anche per gli eventuali danni derivanti da trattamenti illeciti, salvo che riesca a dimostrare che l'evento dannoso non gli sia in alcun modo imputabile[39]. In tale contesto, il titolare è tenuto a vigilare costantemente sulla corretta esecuzione delle disposizioni normative e delle istruzioni impartite, come previsto dal Codice in materia di protezione dei dati personali[40].

---

[34] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali e alla libera circolazione di tali dati (General Data Protection Regulation – GDPR)*, art. 28, par. 1.

[35] Cfr. Pizzetti, Privacy e il diritto europeo alla protezione dei dati personali: il Regolamento europeo 2016/679 cit., p. 58.

[36] Regolamento (UE) 2016/679 (GDPR), art. 28, par. 1.

[37] Ibidem, art. 28, par. 2.

[38] Ibidem, art. 28, par. 4

[39] Ibidem, art. 82, parr. 2 e 3.

[40] D.lgs. 30 giugno 2003, n. 196, *Codice in materia di protezione dei dati personali*, come modificato dal d.lgs. 10 agosto 2018, n. 101, art. 29, comma 5.

La scelta del responsabile deve avvenire mediante un contratto o altro atto giuridicamente vincolante, che definisca in modo preciso e per iscritto le mansioni affidate, le responsabilità e l'ambito operativo del soggetto designato[41]. Tale documento deve specificare la natura, la durata e la finalità del trattamento, il tipo di dati personali trattati, le categorie di interessati e le istruzioni dettagliate che il responsabile è tenuto a seguire. Devono inoltre essere indicate le misure tecniche e organizzative necessarie a garantire la sicurezza e la conformità del trattamento alle disposizioni del GDPR[42].

L'articolo 28 del GDPR individua, in modo espresso, i principali compiti del responsabile del trattamento dei dati. Tra questi rientrano:

– la tenuta del registro delle attività di trattamento[43];

– l'adozione di misure tecniche e organizzative adeguate per assicurare la sicurezza dei dati personali, come previsto dall'articolo 32 del Regolamento[44];

– la designazione di un responsabile della protezione dei dati (RPD o DPO) nei casi stabiliti dal Regolamento o dal diritto nazionale[45];

– la redazione del documento programmatico sulla sicurezza, da aggiornare con cadenza annuale, entro il 31 marzo, al fine di garantire un costante monitoraggio delle misure di protezione adottate[46].

Nel caso in cui il titolare o il responsabile del trattamento non siano stabiliti all'interno dell'Unione Europea, essi devono designare per iscritto un rappresentante nell'Unione, che operi in uno degli Stati membri in cui si trovano gli interessati i cui dati vengono trattati. Tale figura garantisce alle autorità di controllo nazionali e agli interessati stessi un interlocutore stabile per tutte le questioni connesse alla conformità e alla sicurezza del trattamento dei dati personali.

[41] Regolamento (UE) 2016/679, art. 28, par. 3.
[42] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali e alla libera circolazione di tali dati (General Data Protection Regulation – GDPR)*, art. 28, par. 1.
[43] Art. 30, Reg. (UE) 2016/679 (GDPR)
[44] Ibidem, art. 30.
[45] Ibidem, art. 32.
[46] Ibidem, art. 37.

1.2.4 Principi generali del Regolamento alla base del trattamento dei dati

L'art. 5 del GDPR elenca tutti i principi generali che si applicano al trattamento dei dati personali. Questa norma assume particolare rilevanza poiché costituisce la base concettuale dell'intera disciplina sulla protezione dei dati personali. Inoltre, la spiegazione di tali principi riflette le intenzioni del legislatore europeo, il quale ha voluto istituire una sorta di "carta dei diritti individuali" riferita ai dati personali.

In dettaglio, l'articolo, 5 par. 1, del GDPR stabilisce i seguenti principi: a) liceità, correttezza e trasparenza; b) limitazione della finalità; c) minimizzazione dei dati; d) esattezza; e) limitazione della conservazione; f) integrità e riservatezza (*confidentiality*); g) responsabilizzazione (*accountability*).[47]

Questi principi indicano le regole da seguire durante la raccolta, l'elaborazione e la conservazione dei dati personali.

Liceità, correttezza e trasparenza: questo principio è centrale e richiede completa trasparenza da parte di chi tratta i dati. Le organizzazioni devono chiarire sempre perché i dati vengono raccolti e come saranno utilizzati. Se un soggetto interessato chiede informazioni sul trattamento dei propri dati, l'organizzazione è obbligata a fornirle rapidamente. Tutte le operazioni sui dati devono rispettare la legge[48].

La correttezza e la trasparenza si realizzano su due livelli:

- Fornire agli interessati tutte le informazioni necessarie per comprendere come i loro dati vengono trattati.
- Garantire che queste informazioni siano chiare e facilmente comprensibili.

La liceità significa che qualsiasi trattamento di dati, ossia qualsiasi operazione eseguita sui dati personali, anche con strumenti automatizzati deve avere una base giuridica prevista dal GDPR, come: consenso dell'interessato, esecuzione di un contratto, obbligo legale, protezione di interessi vitali, compiti di interesse pubblico o legittimo interesse del titolare o di terzi (art. 6, par. 1).

Alcuni trattamenti particolarmente rischiosi richiedono **consenso esplicito**:

- categorie particolari di dati (opinioni politiche, salute, genetici, sindacali, ecc.) – art. 9

[47] Cfr. Tuccari, I principi del trattamento cit., p. 119
[48] Ivi, p.120.

- trasferimento di dati verso paesi terzi senza adeguate garanzie – art. 49
- processi decisionali automatizzati e profilazione – art. 22

Il consenso deve essere libero, specifico, informato e inequivocabile (art. 4, par. 11). L'interessato può revocarlo in qualsiasi momento (art. 7, par. 3), con una procedura semplice quanto quella per prestarlo. La revoca può riguardare una o più finalità specifiche, e il titolare deve registrare sia il consenso sia eventuali revoche, con date e dettagli aggiornati.

Limitazione della finalità: i dati devono essere trattati solo per scopi specifici, chiari e legittimi. Non possono essere utilizzati per finalità diverse senza il consenso dell'interessato.

Minimizzazione dei dati: si devono raccogliere solo i dati strettamente necessari agli scopi del trattamento. Non è consentito accumulare dati "per eventuali esigenze future".

Esattezza dei dati: i dati devono essere esatti, aggiornati e completi. Devono essere adottate misure per evitare perdita, accesso non autorizzato o modifiche errate. Gli interessati possono richiedere la rettifica o la cancellazione dei dati inesatti entro 30 giorni. L'uso di dati errati può avere conseguenze gravi, come il rifiuto di finanziamenti, e può comportare risarcimenti secondo l'art. 82.

Limitazione della conservazione: i dati devono essere conservati solo per il tempo necessario a raggiungere lo scopo del trattamento. I termini di conservazione possono derivare da obblighi legali, contrattuali o dalla decisione del titolare (es. marketing). Alcuni esempi di dati con tempi di conservazione regolamentati: rapporti di lavoro, videosorveglianza, log di accesso bancario o amministrativo…

Se la legge non specifica tempi di conservazione, il titolare deve stabilirli in maniera ragionevole e documentabile. Quando lo scopo viene raggiunto o il termine scade, i dati devono essere cancellati o anonimizzati. Se cambiano le finalità, occorre comunicare la nuova finalità e stabilire un nuovo periodo di conservazione.

Integrità e riservatezza: i dati devono essere protetti in modo adeguato per poter garantire un'adeguata sicurezza contro minacce interne (uso non autorizzato, perdita, danneggiamento) ed esterne (phishing, malware, furti). Non esiste un'unica soluzione, ma le misure devono essere proporzionate ai rischi. La sicurezza dei dati non riguarda solo le informazioni personali degli interessati, ma anche i dati di soggetti coinvolti

indirettamente, come clienti o fornitori, che potrebbero subire danni in caso di accessi non autorizzati.

Il GDPR rappresenta un cambiamento radicale nella gestione dei dati personali, mettendo al centro i diritti degli interessati e la responsabilità dei titolari. I principi dell'art. 5 non sono solo obblighi legali, ma anche linee guida per promuovere trasparenza, sicurezza e fiducia. Osservare il GDPR significa garantire una gestione responsabile dei dati, proteggere i diritti degli individui e creare un vantaggio competitivo. Applicare questi principi favorisce una maggiore sicurezza digitale.

1.3 La protezione dei dati tra Italia ed Europa

Il diritto alla protezione dei dati personali, nell'ordinamento italiano, rappresenta una manifestazione del più ampio diritto alla personalità garantito dall'articolo 2 della Costituzione[49]. Esso si affianca al diritto alla riservatezza, ma, a differenza di quest'ultimo sviluppatosi soprattutto attraverso le decisioni dei giudici, nasce da una precisa fonte legislativa: la legge n. 675 del 1996, intitolata *Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali*. Questa legge recepiva la Direttiva 95/46/CE del Parlamento Europeo e del Consiglio, che è stata la prima grande normativa europea in materia di privacy[50]. Nel 2003 la legge fu abrogata e sostituita dal decreto legislativo n. 196, conosciuto come *Codice in materia di protezione dei dati personali* o *Codice della Privacy*, che introdusse un sistema organico di regole comprendente anche la disciplina sui trattamenti dei dati nelle comunicazioni elettroniche, in attuazione della Direttiva 2002/58/CE[51]. L'articolo 2 del Codice chiariva che la tutela si riferiva non solo alla riservatezza, ma anche all'identità personale e alla protezione dei dati, sancendo così la coesistenza di queste tre dimensioni all'interno di un unico impianto normativo.

Il Codice della Privacy è tuttora in vigore, ma ha subito importanti modifiche con il decreto legislativo 10 agosto 2018, n. 101, emanato per adeguare la normativa italiana al Regolamento (UE) 2016/679, noto come GDPR. Da allora, la disciplina italiana sulla protezione dei dati personali si fonda principalmente sul diritto europeo, mentre le norme

[49] Cfr. P. Guarda, G. Bincoletto, *Diritto comparato della privacy e della protezione dei dati personali*, Giappichelli, Torino, 2021, p.106

[50] Direttiva 95/46/CE del Parlamento europeo e del Consiglio, 24 ottobre 1995.

[51] Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, 12 luglio 2002.

nazionali hanno funzione integrativa e di coordinamento. La legge di delegazione europea n. 163 del 2017 aveva stabilito i criteri per tale adeguamento, imponendo di eliminare le norme incompatibili con il GDPR e di modificare quelle necessarie per garantirne la piena applicazione, oltre a coordinare il sistema sanzionatorio[52]. La commissione incaricata della riforma ha scelto la tecnica della *novellazione*, cioè la modifica puntuale del testo esistente invece della sua riscrittura completa: una scelta funzionale, ma che ha reso il Codice meno chiaro e più complesso.

Tra le disposizioni nazionali che integrano il Regolamento europeo, meritano attenzione l'articolo 2-quinquies, che fissa a quattordici anni l'età minima per il consenso al trattamento dei dati dei minori nei servizi online[53], e l'articolo 2-terdecies, che disciplina i diritti sui dati delle persone decedute, consentendo a chi abbia un interesse legittimo o agisca per motivi meritevoli di tutela di esercitare i diritti previsti dal GDPR (come accesso, rettifica, cancellazione o opposizione), salvo che l'interessato non lo abbia espressamente vietato prima della morte[54]. Il Codice regola anche il trattamento dei dati contenuti nei provvedimenti giudiziari, valutando il principio di pubblicità del processo con la tutela della riservatezza. In particolare, è possibile chiedere l'anonimizzazione del proprio nome nelle sentenze o negli atti processuali, specialmente nei casi riguardanti minori o reati di natura sessuale[55]. Inoltre, il Codice contiene disposizioni specifiche per il trattamento dei dati a fini di ricerca scientifica, per i rapporti di lavoro, per le comunicazioni elettroniche e per il funzionamento dell'autorità Garante per la protezione dei dati personali. A completare questo sistema complesso vi sono le *Regole deontologiche* e le *Prescrizioni generali* del garante, che stabiliscono come trattare i dati in ambiti particolari, come la sanità, la ricerca scientifica, il giornalismo, il lavoro e i dati genetici[56].

Quando si utilizzano dati personali per la ricerca scientifica, è necessario comprendere quali basi giuridiche legittimano il trattamento e quali eccezioni consentano di agire anche in assenza del consenso esplicito dell'interessato. Le regole deontologiche italiane sulla ricerca aiutano a interpretare correttamente queste situazioni. Esse chiariscono che una persona è considerata "identificabile" quando, usando mezzi ragionevoli, è possibile

[52] Legge n. 163/2017, *Legge di delegazione europea 2016–2017*.
[53] Art. 2-quinquies, D.lgs. 196/2003, introdotto dal D.lgs. 101/2018.
[54] Ibidem.
[55] Ibidem.
[56] Allegati al D.lgs. 196/2003 – Regole deontologiche e Prescrizioni del Garante.

collegare in modo probabile un insieme di dati a un individuo specifico[57]. Tale possibilità dipende dai mezzi economici, dal tempo e dagli strumenti tecnologici disponibili, come archivi, banche dati o software capaci di mettere in relazione più informazioni. In questo senso, il concetto di "dato personale" è strettamente legato a quello di "sicurezza dei dati": più le misure di protezione sono deboli, maggiore è il rischio che qualcuno possa risalire all'identità delle persone. Tuttavia, con l'evoluzione della *data science* e dei *Big Data*, la possibilità di "ri-identificare" dati apparentemente anonimi è cresciuta in modo significativo[58].

L'anonimizzazione totale dei dati non è sempre una soluzione ideale, poiché rende difficile aggiornare, verificare o riutilizzare le informazioni per nuove ricerche. Per questo motivo si ricorre spesso alla *pseudonimizzazione*, che consiste nel sostituire i dati identificativi con codici o chiavi, mantenendo così la possibilità di collegarli alla persona in casi specifici. Il GDPR riconosce l'importanza di questa pratica, ma considera comunque i dati anonimizzati come dati personali e soggetti alle stesse tutele. L'articolo 89 del Regolamento incoraggia comunque, quando possibile, l'uso di dati anonimi, bilanciando la protezione della persona con la libertà della ricerca[59].

Il Regolamento prevede anche alcune limitazioni ai diritti individuali quando il trattamento è effettuato per fini di ricerca, purché siano rispettati i principi di necessità e proporzionalità. Possono quindi subire restrizioni il diritto di accesso, di rettifica, di limitazione del trattamento e di opposizione (articoli 15, 16, 18 e 21 del GDPR). Sono ammesse eccezioni anche per il diritto all'oblio e per l'obbligo di informare l'interessato (articoli 14 e 17), quando fornire tali informazioni sarebbe impossibile o richiederebbe uno sforzo sproporzionato, o se ciò comprometterebbe la ricerca. In questi casi, chi tratta i dati deve comunque adottare misure adeguate per tutelare i diritti e gli interessi delle persone, come informarle con mezzi pubblici e trasparenti[60].

L'articolo 17, paragrafo 3, lettera d), stabilisce che il diritto alla cancellazione non vale quando i dati sono necessari per scopi di ricerca scientifica, a condizione che siano rispettate le garanzie previste dall'articolo 89. In questi casi, il diritto può essere escluso

[57] G. Malgieri, G. Comandè (a cura di), *Guida al trattamento e alla sicurezza dei dati personali*, Giuffrè Francis Lefebvre, Milano, 2021, p. 180.
[58] Ivi, pp. 181–182.
[59] Art. 89 GDPR.
[60] Artt. 14(5)(b), 17(3)(d), 89(2) GDPR.

se cancellare i dati renderebbe impossibile, o molto difficile, raggiungere gli obiettivi della ricerca. Anche il diritto di opposizione può essere limitato quando i dati sono usati solo per fini di ricerca e non esistono motivi personali specifici dell'interessato che vadano in senso contrario.

La normativa sulla privacy cerca di mantenere un equilibrio, da un lato garantire la tutela delle persone, dall'altro non ostacolare il progresso della conoscenza scientifica.

Nel suo insieme, questo sistema di regole, completato dal decreto legislativo n. 51 del 2018 sulla protezione dei dati nei settori della giustizia e della sicurezza pubblica, rappresenta la base attuale del diritto italiano in materia di protezione dei dati personali. L'obiettivo è conciliare le esigenze informative della società, la libertà di ricerca e l'effettiva tutela della persona.

CAPITOLO SECONDO

IMPATTO DEL GDPR E DELLA CYBERSECURITY NELLE IMPRESE: OBBLIGHI, RISCHI E TRASFORMAZIONE DIGITALE

Nel contesto della trasformazione digitale, il marketing, e in particolare quello diretto, rappresenta una delle attività aziendali maggiormente influenzate dal GDPR e dalle nuove esigenze di Cybersecurity. La crescente disponibilità di dati personali e l'uso di tecniche sempre più sofisticate di profilazione hanno reso necessario un quadro normativo che tuteli i diritti degli interessati senza ostacolare l'innovazione e la competitività delle imprese. Per questo motivo il legislatore europeo, nel creare il Regolamento sulla protezione dei dati personali, non ha potuto ignorare l'impatto che queste attività hanno sul trattamento delle informazioni delle persone. L'obiettivo del Regolamento non è quello di ridurre o ostacolare le attività delle imprese, ma di permetterlo nel rispetto dei diritti dei cittadini[61]. L'idea di fondo è quindi quella di bilanciare l'interesse delle aziende a promuovere i propri prodotti con la tutela delle persone, che devono essere messe nella condizione di capire come vengono utilizzati i loro dati e di poter intervenire quando non lo ritengono opportuno.

Per le imprese, questo equilibrio si traduce in alcune regole fondamentali. La prima è che il trattamento dei dati per queste finalità è consentito, a condizione che l'azienda rispetti tutte le norme previste sul trattamento dei dati personali. La seconda regola, forse la più importante, è che la persona interessata ha sempre il diritto di opporsi all'uso dei suoi dati per il marketing, e può esercitare questo diritto in qualunque momento e senza dover dare spiegazioni. Anche quando il marketing viene effettuato tramite tecniche di profilazione, cioè attraverso la raccolta e l'analisi di informazioni utili a proporre messaggi personalizzati, resta valido lo stesso principio, basta che la persona si opponga perché l'azienda debba interrompere immediatamente l'attività[62].

[61] Cfr. G. Malgieri, G. Comandè (a cura di), *Guida al trattamento e alla sicurezza dei dati personali*, Giuffrè Francis Lefebvre, Milano, 2021, p. 215-217.
[62] Art. 21, par. 2, Regolamento (UE) 2016/679 (GDPR).

Gran parte delle tutele riconosciute alle persone riguarda il diritto di essere informate. L'azienda deve spiegare con chiarezza che cosa farà con i dati, per quali finalità li utilizzerà e quali diritti spettano all'interessato. L'informativa deve essere facilmente comprensibile e deve arrivare alla persona in tempo utile, così da permetterle di decidere se accettare o opporsi al trattamento. Questo vale in modo particolare per il marketing diretto e per la profilazione, perché entrambe le attività possono influire sulle scelte e sui comportamenti delle persone.

L'effetto pratico del diritto di opposizione è molto significativo. Una volta che l'interessato comunica di non voler più ricevere comunicazioni promozionali, l'azienda deve smettere subito di usare i dati a questo scopo. Questo richiede una certa organizzazione interna, occorre che l'azienda sia pronta a registrare tempestivamente le opposizioni e a modificarne di conseguenza il trattamento dei dati. Se questo non avviene, si rischia di violare il Regolamento, anche involontariamente [63].

Per questo motivo il Regolamento richiede alle aziende un certo impegno: devono predisporre un'informativa chiara e specifica per il marketing e per la profilazione, devono fornirla agli interessati al momento opportuno, devono soprattutto essere in grado di dare seguito con efficienza alle richieste di opposizione, sia a livello tecnico sia organizzativo[64]. È solo attraverso queste misure che il diritto di opposizione può funzionare davvero e che l'interessato può mantenere una gestione effettiva sui propri dati personali.

2.1 Impatto del GDPR sulle aziende

L'entrata in vigore del Regolamento Generale sulla Protezione dei Dati (GDPR, Regolamento UE 2016/679) ha segnato un punto di svolta nella gestione dei dati personali da parte delle imprese, segnando un passaggio da un approccio basato su misure minime e prescrittive, come previsto dal precedente Codice Privacy italiano (D.Lgs. 196/2003), a un modello fondato sull'*accountability*[65]. In questo nuovo paradigma, il titolare del

[63] G. Finocchiaro, Il nuovo diritto europeo della protezione dei dati personali, Zanichelli, Bologna, 2017, pp. 143-145.
[64] P. Guarda, La trasparenza nel trattamento dei dati personali, in Rivista italiana di informatica e diritto, 2019, pp. 102-105.
[65] G. Malgieri, G. Comandè (a cura di), *Guida al trattamento e alla sicurezza dei dati personali*, Giuffrè Francis Lefebvre, Milano, 2021, p. 196.

trattamento assume una responsabilità attiva. Non basta rispettare prescrizioni standardizzate, ma occorre valutare autonomamente i rischi specifici dei trattamenti, adottare misure proporzionate e dimostrare la conformità normativa. Tale modello teorico, per quanto avanzato, non garantisce automaticamente l'efficacia della protezione dei dati, poiché l'effettivo impatto dipende fortemente dalle risorse disponibili, dalla cultura organizzativa e dalle competenze interne delle aziende.

Il GDPR ha imposto alle imprese un aumento significativo dei costi operativi e organizzativi. Oltre agli investimenti in strumenti tecnologici, sistemi di archiviazione centralizzati, procedure automatizzate e misure di sicurezza, le aziende devono destinare risorse rilevanti alla formazione del personale, alla mappatura dei dati e all'adozione di processi interni coerenti con i principi di *privacy by design* e *privacy by default*. Studi empirici indicano che, in Italia, solo circa un terzo delle imprese aveva predisposto un piano strutturato di adeguamento alla normativa all'inizio del suo periodo di applicazione e che ben due terzi delle aziende italiane dichiarano tuttora di non essere del tutto certe di rispettare pienamente la normativa vigente[66]. Secondo i dati riportati da *Ernst & Young* (azienda di riferimento a livello globale nei servizi professionali di revisione contabile, gestione amministrativa, consulenza fiscale, operazioni straordinarie e *advisory*), la compliance resti un obiettivo complesso e disomogeneo, soprattutto per le piccole e medie imprese, e come la tutela dei diritti possa essere influenzata da disparità strutturali ed economiche.

Nonostante questi ostacoli, il GDPR ha stimolato opportunità significative. Le imprese che hanno interpretato la compliance come un'occasione strategica hanno modernizzato le proprie infrastrutture di gestione dei dati, rafforzato la *governance* interna, migliorato la sicurezza dei sistemi e accresciuto la fiducia dei clienti. In particolare, la creazione di archivi centralizzati e controllati, la definizione di procedure di classificazione e indicizzazione coerenti e l'adozione di strumenti automatizzati per la gestione dei dati personali, hanno consentito di ridurre rischi legali e migliorare l'efficienza operativa. Tuttavia, il reale beneficio dipende dalla capacità delle imprese di integrare la protezione dei dati nei processi decisionali, nella *governance* e nella cultura aziendale.

[66] Ernst & Young (2018), "Privacy: la metà delle imprese italiane non è pronta per la nuova normativa", *Brand News*, https://brand-news.it/intelligence/normative/privacy-ricerche-ey/?utm_source

Una delle principali criticità riguarda la gestione dei diritti degli interessati, quali il diritto di accesso, di rettifica, di cancellazione e di portabilità. Se in teoria questi strumenti rafforzano il controllo dei cittadini sui propri dati, nella pratica rappresentano una sfida complessa per le aziende italiane, in particolare per quelle con sistemi informativi frammentati o processi non digitalizzati. La corretta gestione di tali diritti richiede procedure tracciabili e strumenti tecnologici avanzati, oltre a competenze organizzative e legali adeguate. In assenza di tali capacità, la compliance rischia di rimanere formale, senza tradursi in protezione reale per gli interessati.

La figura del *Data Protection Officer* (DPO) è pensata per supportare la messa in pratica della compliance, coordinare le valutazioni di impatto e promuovere consapevolezza interna. Tuttavia, nella pratica molte aziende limitano il ruolo del DPO a un adempimento formale, senza conferirgli reale autonomia decisionale o posizionamento strategico, vanificando parte dell'efficacia della *governance* dei dati[67]. Questo fenomeno evidenzia come la compliance non possa essere intesa solo come un obbligo normativo, ma richieda un reale cambiamento culturale, organizzativo e strategico.

Il GDPR introduce inoltre una tensione intrinseca tra flessibilità e certezza normativa. La normativa concede discrezionalità nella scelta delle misure, ma al contempo richiede di dimostrarne adeguatezza. Questa ambivalenza genera incertezza interpretativa, soprattutto per le PMI (piccole medie imprese) o le imprese con risorse limitate, accentuando il rischio di disomogeneità nella protezione dei dati tra grandi e piccole realtà. L'efficacia della normativa, dunque, non dipende esclusivamente dal testo legislativo, ma dalla capacità delle aziende di integrare misure tecniche, organizzative e culturali, e di interpretare correttamente i principi generali nella propria realtà operativa.

L'impatto del GDPR sulle imprese italiane evidenzia come la tutela dei dati personali non sia un risultato automatico della regolamentazione, ma il frutto di un complesso intreccio di *governance*, competenze multidisciplinari, strumenti tecnologici e cambiamento culturale. La compliance può diventare un mezzo competitiva e di reputazione solo se considerata parte integrante della strategia aziendale; in assenza di un approccio organico, rischia invece di trasformarsi in un mero adempimento formale, incapace di garantire protezione reale ai soggetti interessati e di valorizzare i dati come asset strategico. Le

[67] ASSO DPO, "Il Data Protection Officer nello sviluppo delle organizzazioni aziendali", 2 ottobre 2020, https://www.assodpo.it/2020/10/02/il-data-protection-officer-nello-sviluppo-delle-organizzazioni-aziendali/?utm_source

evidenze empiriche italiane confermano la necessità di superare la logica burocratica, puntando su cultura, consapevolezza e strumenti coerenti per rendere effettiva la protezione dei dati personali.

2.2 Sviluppi per le imprese

Secondo quanto riportato da Finocchiaro (2017), il Regolamento Europeo sulla protezione dei dati personali ha trasferito il centro di gravità della normativa direttamente sulle imprese, imponendo obblighi stringenti che non si limitano al semplice adeguamento tecnico e organizzativo, ma richiedono un approccio strategico e multidisciplinare alla gestione dei dati personali. In tale contesto, il rispetto dei termini previsti per l'adeguamento non può essere considerato un mero adempimento formale, ma rappresenta una responsabilità attiva, la cui inosservanza comporta conseguenze sanzionatorie significative[68]. Se per le multinazionali e le grandi imprese l'applicazione del GDPR non ha costituito un ostacolo insormontabile, grazie alla presenza di strutture organizzative consolidate, sistemi informativi avanzati e personale dedicato alla compliance, per gli enti pubblici e per le piccole e medie imprese la situazione si è dimostrata più complessa sin dall'inizio. La difficoltà principale risiede non solo nella limitata disponibilità di risorse economiche e tecnologiche, ma anche nella scarsa maturità culturale rispetto alla protezione dei dati e alla gestione del rischio associato ai trattamenti, fattori che hanno rallentato l'adeguamento e in alcuni casi ne hanno compromesso l'efficacia pratica, riducendo le misure a un esercizio prevalentemente formale.

L'analisi critica del ruolo delle imprese nel contesto del GDPR evidenzia come la normativa richieda azioni che, pur chiaramente codificate, necessitano di interpretazione e adattamento alla realtà concreta di ciascuna organizzazione. La nomina del *Data Protection Officer* (DPO) rappresenta uno dei passaggi più rilevanti in questo percorso, poiché non si tratta semplicemente di individuare una figura con competenze giuridiche o tecniche, ma di assicurare che tale soggetto disponga di reale autonomia, potere decisionale e capacità di influenzare le scelte strategiche dell'impresa. La nomina del

[68] Cfr. G. Finocchiaro, Il nuovo diritto europeo della protezione dei dati personali, Zanichelli, Bologna, 2017.

DPO rischia di ridursi a un adempimento formale se la figura non è collocata in modo chiaro all'interno della struttura aziendale e non possiede competenze multidisciplinari che integrino diritto, tecnologia e organizzazione aziendale. Questa dinamica mette in luce come la compliance non possa essere considerata un obbligo puramente normativo, ma debba tradursi in un cambiamento culturale e organizzativo profondo.

La gestione dei trattamenti ad alto rischio costituisce un'ulteriore sfida, poiché il GDPR richiede l'effettuazione di una valutazione d'impatto sulla protezione dei dati (DPIA), *Data Protection Impact Assessment*), strumento previsto dall'articolo 35 del Regolamento. La DPIA consente di analizzare la necessità e la proporzionalità dei trattamenti rispetto agli obiettivi aziendali, individuando il livello di rischio tollerabile e le misure necessarie a contenerlo. Tuttavia, nella pratica, molte imprese percepiscono la DPIA come un obbligo tecnico-legale piuttosto che come una tecnica di gestione strategica del rischio, con il rischio che le valutazioni restino astratte e non si traducano in interventi concreti o nel miglioramento dei processi. Ciò evidenzia la necessità di un approccio integrato, che leghi la DPIA alla pianificazione delle risorse, alla formazione del personale e alla revisione continua dei sistemi informativi, rendendo effettivamente operativa la protezione dei dati personali.

Analogamente, la tenuta del registro delle attività di trattamento, obbligatoria secondo l'articolo 30 del GDPR, non può essere intesa come semplice compilazione dei campi richiesti, ma deve garantire una visione completa e aggiornata di tutte le operazioni di trattamento. Il registro diventa così uno strumento dinamico di *governance*, in grado di monitorare i flussi dei dati, identificare criticità e supportare interventi correttivi tempestivi. La sua efficacia dipende dalla capacità dell'impresa di integrare procedure operative, strumenti tecnologici e competenze professionali, trasformando il registro da adempimento burocratico a leva concreta di accountability e trasparenza.

Gli effetti pratici del GDPR non si limitano alla gestione interna dei dati, ma si estendono ai rapporti con gli interessati. Le imprese devono aggiornare costantemente le informazioni fornite ai clienti e agli utenti, adeguare la modulistica e garantire la possibilità di esercitare i diritti previsti dal Regolamento, come accesso, rettifica, cancellazione e portabilità dei dati. In Italia, molte imprese, in particolare le PMI, hanno incontrato difficoltà nell'implementare procedure efficaci per gestire questi diritti, evidenziando come la compliance richieda strumenti organizzativi, tecnologici e culturali

adeguati per garantire protezione reale e continuativa, e non un semplice rispetto formale della normativa.
In definitiva, le implicazioni per le imprese derivanti dal GDPR richiedono una riflessione critica che vada oltre la mera elencazione degli obblighi normativi. L'effettiva applicazione del Regolamento implica una complessa interazione tra *governance*, tecnologia, processi aziendali e cultura organizzativa. Le imprese devono essere in grado di tradurre i requisiti normativi in strumenti concreti di gestione strategica del rischio e protezione dei dati, integrando la compliance nella pianificazione aziendale, nella formazione continua del personale e nello sviluppo dei sistemi informativi. Solo attraverso questo approccio integrato e consapevole la normativa può trasformarsi in un'opportunità reale, capace di rafforzare e migliorare la gestione dei dati e consolidare la reputazione aziendale, piuttosto che limitarsi a costituire un mero adempimento formale.

2.3 Risarcimento per violazione del GDPR e della privacy

Con l'entrata in vigore del Regolamento (UE) 2016/679 (GDPR), la disciplina del risarcimento per danni derivanti da violazioni della normativa sulla protezione dei dati personali ha acquisito un ruolo centrale nella tutela degli interessati, ponendo sul titolare o sul responsabile del trattamento l'onere di rispondere non solo in caso di danni materiali, ma anche di danni immateriali[69]. Tuttavia, l'applicazione pratica dell'articolo 82 GDPR, pur delineando un principio chiaro, mostra complessità e incertezze che richiedono una lettura critica e un approccio analitico.
Secondo la normativa, chi subisce un danno derivante da un trattamento illecito ha diritto al risarcimento da parte del titolare o, in determinati casi, del responsabile del trattamento. In particolare, il titolare risponde sempre dei danni causati da trattamenti non conformi, mentre il responsabile risponde solo se ha violato obblighi specifici a lui attribuiti o se ha agito diversamente dalle istruzioni legittime del titolare. La figura del DPO, invece, non comporta responsabilità diretta per i danni, sebbene in casi eccezionali, quando dimostrabile incompetenza grave o errori rilevanti il titolare possa rivalersi su di lui.

[69] G. Malgieri, G. Comandè (a cura di), *Guida al trattamento e alla sicurezza dei dati personali*, Giuffrè Francis Lefebvre, Milano, 2021, p.113.

Questo quadro evidenzia come la responsabilità civile nel GDPR non si limiti al rispetto formale delle norme, ma richieda una gestione attiva del rischio e delle decisioni operative.

Perché il risarcimento sia effettivamente riconosciuto, è necessario che sussistano tre condizioni fondamentali: l'esistenza di un danno concreto, la correlazione diretta tra il danno e la violazione normativa e l'attribuibilità della responsabilità al titolare o al responsabile del trattamento. L'Articolo 82 GDPR stabilisce inoltre che il risarcimento deve essere "effettivo e completo", comprendendo sia i danni materiali, come perdite economiche dirette, sia quelli immateriali, quali stress, turbamento o perdita di fiducia. Tuttavia, la giurisprudenza europea ha chiarito che la semplice violazione normativa non garantisce automaticamente il risarcimento: è necessario dimostrare il danno concreto e il nesso causale, con evidenze oggettive[70].

Un esempio concreto è offerto dalla sentenza della Corte di Giustizia dell'Unione Europea nella causa C-300/21 *Österreichische* (Austria) Post AG (2023). In questo caso, l'interessato lamentava un danno non materiale consistente in turbamento e perdita di fiducia a seguito del trattamento senza consenso dei dati concernenti le sue affinità politiche[71]. La CGUE ha stabilito che, pur riconoscendo la possibilità di risarcire danni immateriali, l'ammissibilità del risarcimento è subordinata alla prova del danno concreto e del nesso causale, nonché alla normativa nazionale di riferimento per la quantificazione. Questo orientamento mostra chiaramente che il rischio legale non deriva solo dalla violazione del GDPR, ma dalla combinazione tra violazione, danno concreto e capacità di dimostrarlo in giudizio.

Da questa analisi emergono due ordini di effetti critici per le imprese. Il primo riguarda la *governance* e gestione del rischio, in cui il titolare deve adottare un sistema organico che comprenda misure tecniche, organizzative e procedurali in grado di prevenire e diminuire i rischi, documentare le decisioni e mantenere audit costanti. Solo attraverso una gestione strutturata e documentata delle attività di trattamento, il titolare può dimostrare di aver agito con diligenza e correttezza, riducendo la probabilità di responsabilità diretta. Il secondo ordine riguarda la certezza del diritto e la tutela effettiva

[70] Art. 82 del GDPR ("Diritto al risarcimento e responsabilità").

[71] ECC Net Italia, "Violazione del Regolamento Privacy: la Corte di Giustizia UE chiarisce quando è possibile ottenere un risarcimento", https://ecc-netitalia.it/it/news/violazione-del-regolamento-privacy-la-corte-di-giustizia-ue-chiarisce-quando-e-possibile-ottenere-un-risarcimento

degli interessati. L'assenza di criteri uniformi per la quantificazione del danno immateriale e la valutazione del nesso causale genera incertezza interpretativa e possibili disparità tra ordinamenti nazionali o tribunali diversi.
Un'analisi più approfondita mostra che il diritto al risarcimento, pur essendo teoricamente solido, resta in molti casi difficile da concretizzare. Le imprese non possono limitarsi a conformarsi formalmente alle procedure previste dal GDPR. Esse devono integrare la compliance in una strategia di gestione del rischio, garantendo processi trasparenti, formazione continua del personale, sistemi di documentazione e controlli periodici. Allo stesso tempo, gli interessati devono essere in grado di dimostrare in maniera chiara il danno subito e il nesso con la violazione, soprattutto nei casi di danno immateriale, difficilmente quantificabile e verificabile.
La disciplina sul risarcimento dei danni da violazione del GDPR, pur rappresentando un avanzamento significativo nella tutela dei dati personali, non garantisce da sola protezione effettiva. L'efficacia pratica del diritto al risarcimento dipende dalla capacità delle imprese di integrare *governance*, controllo, documentazione e gestione del rischio, nonché dalla capacità degli interessati di provare il danno e il nesso causale. Solo in questo contesto il risarcimento può essere strumento reale di tutela e deterrente, andando oltre il mero adempimento formale.

2.4 Le regole sulle sanzioni amministrative

Il Regolamento Europeo 2016/679 (GDPR) ha introdotto anche un sistema di sanzioni amministrative che si discosta nettamente dall'approccio precedente della Direttiva 95/46/CE, segnando una nuova fase nella gestione delle violazioni in materia di protezione dei dati. L'innovazione normativa risponde a due esigenze principali: da un lato, armonizzare le regole tra gli stati membri per garantire applicazioni simili e coerenti delle sanzioni; dall'altro, conferire alle autorità di controllo poteri effettivi e uniformi per intervenire in modo incisivo, evitando disparità di trattamento che in passato hanno indebolito la tutela dei dati personali.
A differenza della precedente normativa, dove ogni Stato poteva definire liberamente l'entità e le modalità delle sanzioni, il GDPR stabilisce con precisione i limiti e i criteri per l'applicazione delle multe pecuniarie, distinguendo tra violazioni meno gravi, ad

esempio, inerenti obblighi di registro o comunicazioni agli interessati e violazioni più rilevanti, che riguardano principi fondamentali del trattamento, trasferimenti illeciti di dati o mancato rispetto dei diritti degli interessati. L'articolo 83 del Regolamento prevede sanzioni fino a 10 milioni di euro o al 2% del fatturato annuo mondiale per le violazioni meno gravi, e fino a 20 milioni di euro o al 4% del fatturato mondiale annuo per quelle più gravi[72].

Tuttavia, l'introduzione di soglie elevate e di criteri dettagliati non elimina le complessità interpretative e operative. La determinazione dell'ammontare della sanzione richiede valutazioni caso per caso che considerano natura, gravità e durata della violazione, misure preventive adottate dall'impresa, cooperazione con l'autorità e recidiva. Questo genera un margine di incertezza per le imprese, poiché la stessa violazione può produrre esiti differenti a seconda dell'interpretazione discrezionale dell'autorità nazionale competente. Tale incertezza, se non gestita strategicamente, può tradursi in rischi economici e reputazionali rilevanti, soprattutto per le realtà più piccole che non dispongono di risorse legali e organizzative significative.

Un'ulteriore dimensione critica riguarda le disparità di impatto tra grandi imprese e piccole medie imprese. Se da un lato le multinazionali possono assorbire l'impatto economico di sanzioni calcolate sul fatturato mondiale, per le PMI anche una violazione considerata "minore" può determinare conseguenze finanziarie gravissime, potenzialmente compromettendo la continuità operativa. Questo squilibrio evidenzia una tensione intrinseca nel sistema. Mentre l'armonizzazione mira a tutelare uniformemente i diritti dei cittadini europei, l'effetto concreto delle sanzioni rischia di penalizzare in misura maggiore chi dispone di risorse limitate, introducendo un elemento di disuguaglianza strutturale tra le imprese.

Dal punto di vista strategico, le sanzioni amministrative impongono alle imprese di adottare approcci proattivi e sistemi di gestione del rischio mirati, indipendenti dalla semplice compliance formale. In particolare, l'analisi preventiva dei rischi, la definizione di protocolli per il trattamento dei dati sensibili, la verifica periodica dei processi aziendali e la documentazione completa delle decisioni operative diventano strumenti indispensabili per ridurre la probabilità e la gravità delle sanzioni. Un caso emblematico

[72] Garante per la Protezione dei Dati Personali, *"Regolamento Europeo e sanzioni amministrative*", 2025, https://www.garanteprivacy.it/sanzioni-amministrative-ai-sensi-del-regolamento-ue-2016/679-?utm_source

è rappresentato dalla sanzione irrogata nel 2023 dall'Autorità Garante italiana a un'importante società di servizi digitali, che ha visto una multa significativa per la mancanza di misure di sicurezza adeguate nella gestione di dati di clienti minorenni. L'analisi del caso mostra come non sia sufficiente ottemperare formalmente agli obblighi normativi. La valutazione del contesto, la documentazione delle procedure e la tempestiva attuazione di misure preventive sono elementi determinanti per la modulazione della sanzione[73].

Il sistema sanzionatorio del GDPR rappresenta un avanzamento rilevante in termini di efficacia e tutela dei diritti degli interessati. Tuttavia, la sua validità reale dipende dalla capacità delle autorità di controllo di applicare le norme in modo coerente, dalla trasparenza dei criteri di determinazione delle sanzioni e dalla capacità delle imprese di integrare compliance, valutazione dei rischi e gestione documentata dei trattamenti.

Le sanzioni possono funzionare come strumento di protezione effettiva dei dati e di mitigazione del rischio, andando oltre la semplice imposizione di un obbligo formale.

2.4.1 Come funzionano le sanzioni

Secondo il Regolamento, per far rispettare le regole possono essere comminate sanzioni, comprese le multe: *"Per rafforzare il rispetto delle norme del regolamento dovrebbero essere imposte sanzioni, comprese sanzioni amministrative pecuniarie per violazione del Regolamento, in aggiunta o sostituzione di misure appropriate imposte dall'autorità di controllo"*[74]. Il Considerando 148, spesso richiamato in dottrina, chiarisce che per assicurare il rispetto della normativa le autorità devono poter infliggere sanzioni, incluse quelle di natura pecuniaria, adottate da sole oppure insieme ad altre misure correttive. Ciò evidenzia che la logica del sistema non è puramente punitiva, ma orientata a ristabilire un corretto assetto di tutela del dato personale e prevenire il ripetersi di condotte scorrette. La sanzione, quindi, non rappresenta un automatismo, cioè l'autorità non applica

[73] Carmignani Consulenza. (2023, 18 aprile). Il Garante privacy ha sanzionato una società che offre servizi di digital marketing con una multa di 300mila euro per aver trattato in modo illecito dati personali a fini di marketing, Garante della Privacy provvedimento del 23.02.2023. Recuperato da https://carmignaniconsulenza.com/2023/04/18/il-garante-privacy-ha-sanzionato-una-societa-che-offre-servizi-di-digital-marketing-con-una-multa-di-300mila-euro-per-aver-trattato-in-modo-illecito-dati-personali-a-fini-di-marketing-garante-della/#

[74] Regolamento (UE) 2016/679 (GDPR), considerando 148.

automaticamente una multa solo perché c'è stata una violazione, ma bensì l'esito di una valutazione complessiva su come la violazione abbia inciso sui diritti degli interessati e sul grado di responsabilità del titolare o del responsabile del trattamento.

L'autorità, nel modulare la risposta sanzionatoria, non si limita a constatare l'irregolarità né applica una tariffazione predeterminata. Al contrario, deve prendere in considerazione il comportamento del soggetto coinvolto prima, durante e dopo la violazione, con particolare riguardo all'effettiva capacità dell'intervento sanzionatorio di correggere il processo illecito e di prevenire ulteriori rischi. In questa prospettiva, il sistema si distingue per un approccio progressivo. La multa rappresenta solo una delle possibili opzioni, mentre altre misure come l'ordine di conformarsi alla normativa entro un certo termine, l'imposizione di limitazioni ai trattamenti oppure la sospensione dei flussi di dati possono risultare più efficaci per ripristinare un adeguato livello di protezione.

Un elemento significativo nella struttura del GDPR è la possibilità per l'autorità di ricorrere al semplice ammonimento quando la violazione è di scarsa gravità oppure quando la sanzione pecuniaria risulterebbe sproporzionata, soprattutto nei confronti delle persone fisiche. Questa scelta non è indice di un atteggiamento indulgente, ma riflette la consapevolezza che, in determinate circostanze, il valore preventivo e formativo dell'ammonimento può essere maggiore rispetto a una multa, soprattutto quando l'interessato dimostra collaborazione e adozione tempestiva delle misure correttive. L'ammonimento svolge dunque una funzione rilevante nell'economia del sistema sanzionatorio, in quanto informa il titolare dell'irregolarità, lo avverte delle conseguenze e contribuisce a orientare i comportamenti futuri senza incidere eccessivamente sulla sua situazione economica.

Particolarmente evidente è il ruolo della valutazione contestuale del caso concreto. La natura della violazione, la vulnerabilità dei soggetti coinvolti, l'eventuale tempestività dell'autodenuncia e il grado di rischio effettivamente generato rappresentano elementi che permettono all'autorità di modulare il proprio intervento. Questo approccio casistico è confermato anche dalla prassi applicativa del garante per la protezione dei dati personali, il quale nelle proprie decisioni sottolinea frequentemente l'importanza della cooperazione del titolare e della rapidità con cui vengono attuate le misure di riduzione del rischio. Da questo punto di vista, il sistema non solo punisce la violazione, ma

incentiva comportamenti virtuosi, migliorando nel complesso la *governance* dei dati personali.

In definitiva, il funzionamento delle sanzioni nel GDPR non può essere compreso in un'ottica meramente retributiva. Esso si articola in un insieme di strumenti graduati, pensati per promuovere un atteggiamento responsabile degli operatori e per garantire la tutela effettiva dei diritti delle persone. È proprio questa combinazione tra severità potenziale e flessibilità applicativa a rendere il sistema coerente con il principio di accountability (presente in tutta la normativa), cioè quando il Regolamento si basa sul principio di responsabilizzazione (*accountability*), secondo cui titolari e responsabili devono adottare comportamenti attivi e dimostrare di aver applicato concretamente le misure previste dal Regolamento[75].

2.4.2 Come si decide l'ammontare della sanzione

La determinazione dell'ammontare di una sanzione ai sensi del GDPR richiede un'analisi complessa, ponderata e discrezionale da parte dell'autorità di controllo, che non si limita ad applicare regole fisse ma valuta ogni singolo caso nel suo contesto specifico. Nella decisione vengono considerati diversi fattori: la gravità e la durata della violazione, le conseguenze effettive sui soggetti interessati, il numero di persone coinvolte, la natura dei dati trattati e il grado di responsabilità del titolare o del responsabile del trattamento. L'autorità prende in esame anche precedenti violazioni, il livello di collaborazione dell'ente con l'istruttoria, l'adozione di codici di condotta o sistemi di certificazione e, nei casi rilevanti, eventuali vantaggi economici ottenuti o perdite evitate grazie alla violazione.

Questo approccio sottolinea come la gestione del rischio sanzionatorio non possa essere affrontata come un mero adempimento formale, ma debba essere integrata nella *governance* aziendale: le imprese devono prevedere scenari di rischio, implementare misure preventive e documentare tutte le azioni correttive o attenuanti, affinché eventuali contestazioni possano essere gestite con efficacia. La capacità di dimostrare diligente

[75] Garante per la protezione dei dati personali, *Approccio basato sul rischio e misure di accountability (responsabilizzazione) di titolari e responsabili*, www.garanteprivacy.it/regolamentoue/approccio-basato-sul-rischio-e-misure-di-accountability-responsabilizzazione-di-titolari-e-responsabili, consultato il 10 dicembre 2025.

gestione dei dati diventa così un elemento essenziale per ridurre l'esposizione al rischio economico e reputazionale.

Un caso emblematico riguarda *Enel Energia*, sanzionata nel 2024 per € 79,1 milioni a causa di violazioni legate al telemarketing abusivo e alla gestione inadeguata dei dati personali dei clienti. L'autorità ha rilevato difetti nei sistemi di sicurezza e carenze nei processi organizzativi interni, evidenziando come anche una grande impresa possa essere soggetta a sanzioni significative quando le misure preventive risultano insufficienti o mal implementate. Questo esempio mette in luce che la determinazione della sanzione non dipende esclusivamente dalla violazione tecnica, ma dalla capacità dell'impresa di dimostrare misure organizzative e tecnologiche coerenti con il GDPR[76].

Il caso di Enel Energia conferma che l'ammontare della sanzione riflette un equilibrio tra la gravità della violazione e l'efficacia delle contromisure adottate dall'impresa, sottolineando l'importanza di integrare la compliance nella gestione strategica del rischio e nella *governance* quotidiana dei dati personali. La documentazione accurata di tutte le valutazioni e decisioni assume un ruolo centrale non solo per garantire trasparenza e responsabilizzazione, ma anche per costituire prova difensiva in eventuali contenziosi.

2.4.3 Quali criteri influenzano la multa

La determinazione dell'importo di una sanzione ai sensi del GDPR non segue un meccanismo automatico, bensì un processo valutativo articolato che richiede alle autorità di controllo di esaminare l'insieme delle circostanze del caso concreto. Sebbene il Regolamento fissi dei massimali chiari, fino a 20 milioni di euro o al 4% del fatturato annuo mondiale dell'impresa è lasciato un margine significativo di discrezionalità nell'individuazione dell'importo effettivo da applicare. Tale discrezionalità è regolata da criteri uniformi, indicati dall'art. 83 GDPR, che impongono un esame integrato delle caratteristiche della violazione, del comportamento del titolare e delle conseguenze prodotte sugli interessati, evitando qualsiasi approccio sanzionatorio meramente schematico[77].

[76] CMS Law, *GDPR Enforcement Tracker Report – Italy, 2024*, https://cms.law/en/pol/publication/gdpr-enforcement-tracker-report-2024/italy?utm_source

[77] Art. 83, par. 2 del GDPR.

Uno dei criteri centrali riguarda l'entità del pregiudizio subito dai soggetti coinvolti, valutata non soltanto in termini di numero di persone interessate, ma anche di natura dei dati trattati e di tipo di danno prodotto, che può assumere dimensioni patrimoniali, morali o addirittura sociali, quando compromette diritti fondamentali quali la dignità o la libertà personale. Rispetto al previgente quadro normativo, in cui contava soprattutto la grandezza della banca dati, il GDPR pone al centro la qualità del rischio, riconoscendo che anche un numero ridotto di interessati può essere esposto a danni particolarmente gravi.

La valutazione prosegue poi con l'esame dell'elemento soggettivo, ossia del grado di colpa o dolo del titolare o del responsabile. Una violazione determinata da negligenza sistemica o peggio da un comportamento intenzionale può condurre a un aggravamento significativo della sanzione, mentre la presenza di un incidente non volontario, pur imputabile, può essere esaminata in modo più favorevole. Tale criterio consente all'autorità di distinguere tra imprese che adottano un modello organizzativo improntato alla prudenza e soggetti che invece operano con scarsa attenzione ai rischi.

Un ruolo determinante è poi attribuito alle modalità della condotta, vale a dire alle azioni intraprese dal titolare per contenere l'impatto del problema. La rapidità nell'intervenire, la tempestiva attivazione di misure di mitigazione e la capacità di predisporre un piano correttivo strutturato rappresentano indicatori fondamentali dell'impegno dell'impresa e influenzano positivamente la valutazione finale. Di particolare rilievo è anche il grado complessivo di responsabilità dell'organizzazione, misurato attraverso le misure tecniche e organizzative adottate, in conformità con gli obblighi di sicurezza e con i principi di *privacy by design* e *by default*: un sistema che dimostri coerenza e prevenzione può attenuare anche l'impatto di una violazione seria.

Nel processo valutativo trova spazio anche l'eventuale esistenza di precedenti violazioni, che può costituire un aggravante quando rivela mancanza di continuità nella compliance. Parallelamente, la cooperazione con l'autorità riveste un ruolo attenuante. Un soggetto che collabora pienamente, fornisce dati tempestivi e contribuisce attivamente alla risoluzione della vicenda dimostra un approccio responsabile che l'autorità non può ignorare.

Un ulteriore criterio è rappresentato dalla natura dei dati coinvolti. Le violazioni che riguardano categorie particolarmente sensibili come dati sanitari, genetici, giudiziari o

relativi a minori comportano un rischio intrinsecamente più elevato per gli individui e possono quindi condurre ad importi sanzionatori maggiori. Analogamente, è rilevante la modalità con cui l'autorità viene a conoscenza della violazione. Il GDPR valorizza la notifica spontanea e tempestiva da parte del titolare, considerandola espressione del principio di accountability e attenuando l'entità della sanzione quando tale comportamento è presente.

Non va poi sottovalutata l'importanza del rispetto di eventuali provvedimenti precedenti dell'autorità. L'inosservanza di ordini già impartiti, anche se riferiti a trattamenti diversi, può essere letta come indice di scarsa affidabilità del titolare e giustifica un aggravio sanzionatorio. Viceversa, l'adesione a codici di condotta o a meccanismi di certificazione riconosciuti dall'ordinamento è considerata un elemento favorevole, poiché rappresenta un impegno concreto verso modelli di conformità strutturati e verificabili.

L'autorità conserva la possibilità di valutare ulteriori circostanze aggravanti o attenuanti, come eventuali vantaggi economici ottenuti tramite la violazione o le perdite evitate, la buona fede mostrata dal soggetto o la sua condotta complessiva, anche antecedente alla contestazione formale[78]. Ciò consente un margine di personalizzazione che evita di equiparare situazioni notevolmente diverse, garantendo che la sanzione sia realmente proporzionata, effettiva e preventiva.

2.4.4 Tipologie di sanzioni

Le sanzioni pecuniarie previste dal Regolamento si dividono in due categorie principali. La prima riguarda le violazioni meno gravi, che possono comportare multe fino a dieci milioni di euro o fino al 2% del fatturato annuo dell'impresa se superiore. Queste includono ad esempio violazioni relative al consenso dei minori, al trattamento di dati che non richiede identificazione, agli obblighi di sicurezza, alla tenuta dei registri, alla cooperazione con le autorità e agli obblighi di certificazione [79].

La seconda categoria (già menzionata nel paragrafo precedente) riguarda le violazioni più gravi, per le quali le multe possono arrivare fino a venti milioni di euro o fino al 4%

[78] Garante per la Protezione dei Dati Personali, *Linee guida in materia di applicazione delle sanzioni amministrative pecuniarie ai sensi del GDPR*, 2022.

[79] G. Malgieri, G. Comandè (a cura di), *Guida al trattamento e alla sicurezza dei dati personali*, Giuffrè Francis Lefebvre, Milano, 2021, pp.119-120.

del fatturato dell'impresa se superiore. Qui rientrano le infrazioni ai principi fondamentali del trattamento dei dati, le violazioni dei diritti degli interessati, comprese quelle legate al processo decisionale automatizzato, i trasferimenti verso paesi terzi, la mancata osservanza di ordini o limitazioni imposti dall'autorità, l'inosservanza di obblighi nazionali particolari e il mancato rispetto di provvedimenti restrittivi sui flussi di dati [80]. In aggiunta, il D.Lgs. 101/2018 ha previsto ulteriori sanzioni amministrative pecuniarie, dettagliatamente individuate all'articolo 166, che completano il quadro delle conseguenze in caso di violazioni delle norme sulla protezione dei dati personali.

2.5 I costi delle violazioni informatiche e le conseguenze sulla reputazione aziendale

I dati aziendali rappresentano oggi uno dei beni più importanti per qualunque organizzazione. Informazioni come dati dei clienti, piani strategici, documenti riservati o contenuti finanziari sono fondamentali per il funzionamento di un'impresa. Quando questi dati vengono rubati o resi pubblici dopo un attacco informatico, le conseguenze sono molto pesanti non solo dal punto di vista economico, ma anche per l'immagine dell'azienda, che rischia di perdere credibilità e fiducia presso clienti, partner e mercato. Secondo il *Cost of a Data Breach Report 2025* di IBM (International Business Machines Corporation) azienda tecnologica multinazionale statunitense, il costo medio globale di una violazione è pari a 4,44 milioni di dollari[81]. Sebbene i dati siano globali, in Europa i valori risultano generalmente più contenuti rispetto al Nord America, e l'uso di strumenti basati sull'intelligenza artificiale per la sicurezza può ridurre significativamente sia i costi che i tempi di risposta[82]. In Italia, il *Rapporto Clusit 2025* segnala che una parte significativa delle organizzazioni ha subito danni finanziari stimati in almeno 50.000 €, [83]mentre altre fonti riportano un costo medio di 4,37 milioni di euro per violazione[84].
Una parte consistente dei costi deriva dal tempo necessario per accorgersi della violazione e per fermarla. Nel 2025, le aziende europee hanno impiegato mediamente diverse settimane per identificare e contenere gli attacchi, e più a lungo un attacco passa

[80] Ibidem.
[81] IBM Security e Ponemon Institute, Cost of a Data Breach Report 2025.
[82] ENISA Threat Landscape 2024, European Union Agency for Cybersecurity, 2024.
[83] Clusit, *Rapporto sulla Sicurezza ICT in Italia 2025*.
[84] Innovation Post, "Quanto costano le intrusioni informatiche in Italia", 2025.

inosservato, più aumentano i costi dovuti all'interruzione dei servizi, al recupero dei sistemi, al supporto ai clienti e alle attività di comunicazione interna ed esterna. In molti casi, una gestione lenta peggiora anche la percezione dei clienti, che possono decidere di abbandonare l'azienda perché la ritengono poco affidabile.

Un elemento che emerge con forza dai rapporti europei e italiani è il ruolo dell'intelligenza artificiale. Sempre più aziende stanno introducendo strumenti basati sull'AI per svolgere attività quotidiane e per automatizzare diversi processi. Tuttavia, secondo *IBM*, il 63% delle organizzazioni non ha ancora definito regole o controlli adeguati per gestire queste tecnologie, generando un cosiddetto "divario di *governance*" che può favorire errori, uso improprio degli strumenti e una minore capacità di difendersi in caso di attacco[85].

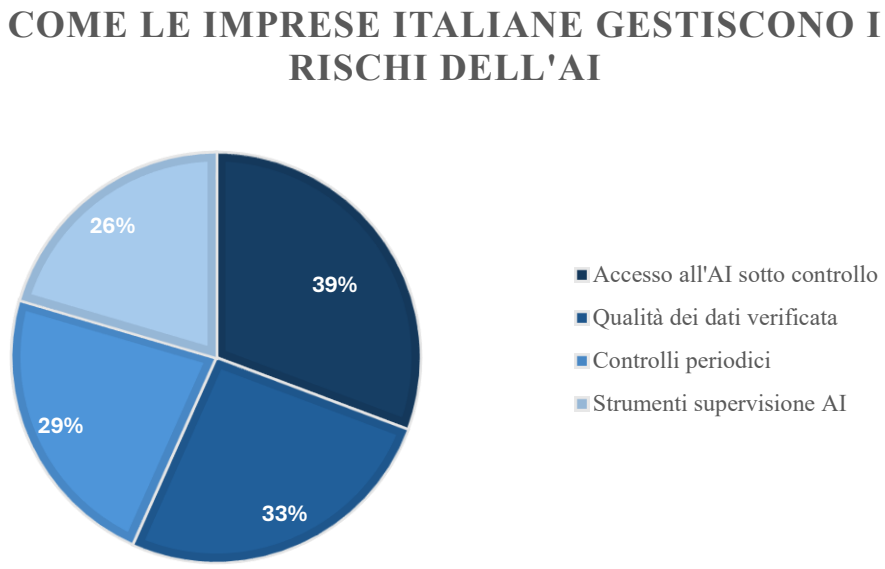

Figura 2: Percentuale delle misure adottate contro AI (IBM 2025)

In Italia, come evidenziato dal report *IBM,* le imprese affrontano i rischi legati all'IA soprattutto controllando chi può accedere agli strumenti (39%), verificando l'affidabilità dei dati utilizzati (33%), effettuando controlli regolari sui sistemi (29%) e utilizzando strumenti che aiutano a monitorare il corretto uso dell'AI (26%).

[85] IBM Security e Ponemon Institute, Report IBM 2025, https://it.newsroom.ibm.com/cost-of-data-breach-2025?utm_source.

Il report di *IBM*, mostra inoltre che alcune violazioni hanno riguardato modelli o applicazioni di IA, e che gran parte delle organizzazioni interessate non disponeva di controlli sufficienti sull'accesso agli strumenti di intelligenza artificiale. Allo stesso tempo, anche gli aggressori informatici hanno iniziato a usare l'IA per rendere i loro attacchi più convincenti e difficili da individuare, tramite email di phishing automatiche o contenuti manipolati come i deepfake, ovvero foto o video generati dall'intelligenza artificiale [86].

Accanto a ciò, si sta diffondendo un fenomeno chiamato *shadow AI*, cioè l'uso di strumenti di intelligenza artificiale non autorizzati o non controllati dalle regole aziendali. In contesti con molta *shadow AI*, i costi delle violazioni aumentano sensibilmente, e in Italia solo il 31% delle organizzazioni dichiara di avere politiche chiare per gestirla[87].

La mancanza di visibilità su questi strumenti aumenta i rischi, perché gli strumenti non autorizzati possono raccogliere o archiviare dati in modo non sicuro.

Se, da un lato, l'IA può aumentare i rischi quando non viene governata correttamente, dall'altro rappresenta anche una delle soluzioni più efficaci per ridurre costi e tempi di risposta. Le aziende che adottano l'IA e l'automazione nella sicurezza informatica riescono a risparmiare mediamente 1,9 milioni di dollari per ogni violazione, rispetto a quelle che non la utilizzano[88]. Questo perché l'IA permette di individuare anomalie più rapidamente e di ridurre i tempi di intervento, limitando così l'estensione del danno.

Oltre ai costi economici immediati, uno degli effetti più rilevanti degli attacchi informatici riguarda la reputazione aziendale. Una violazione può generare sfiducia nei clienti, ridurre il valore del brand e complicare la gestione dei rapporti commerciali. Le attività svolte dopo l'attacco, come l'assistenza ai clienti colpiti, la comunicazione ufficiale, la ricostruzione dei sistemi e l'eventuale supporto psicologico ai dipendenti coinvolti, rappresentano una parte consistente della spesa complessiva. Una gestione poco chiara o ritardata può amplificare la sensazione di insicurezza nei clienti, con conseguenze sulla fedeltà al marchio e sulla capacità dell'azienda di mantenere o attrarre nuovi utenti.

Alla luce di questi dati, emergono alcune strategie che possono aiutare le imprese a ridurre l'impatto economico e reputazionale delle violazioni. La prima riguarda la creazione di regole chiare per l'uso dell'IA, stabilendo chi può utilizzare gli strumenti, come devono

[86] Ibidem.
[87] Ibidem.
[88] IBM Security e Ponemon Institute, Cost of a Data Breach Report 2025.

essere gestiti i dati e come monitorare eventuali comportamenti anomali. La seconda consiste nell'introdurre controlli precisi sugli accessi, in modo da contenere il più possibile l'uso improprio dell'IA. Un'altra misura importante è l'automazione dei processi di sicurezza. Adottare sistemi che segnalano automaticamente attività sospette permette di intervenire prima che la violazione si estenda. Infine, è fondamentale monitorare e limitare la *shadow AI.*

Un altro elemento decisivo è la preparazione interna. Avere un piano di risposta agli incidenti, con ruoli definiti e procedure già strutturate, permette di agire rapidamente e di ridurre l'impatto dell'attacco. È importante anche assicurare una comunicazione chiara e trasparente verso clienti, dipendenti e stakeholder, poiché una comunicazione efficace riduce il danno reputazionale e contribuisce a mantenere la fiducia.

I dati del 2025 mostrano come il costo delle violazioni sia ancora molto elevato, e come la reputazione aziendale resti un elemento fragile che può essere compromesso rapidamente. L'intelligenza artificiale, se non gestita con attenzione, può aumentare il rischio, ma allo stesso tempo rappresenta una delle risorse più efficaci per ridurlo. Le organizzazioni che investono nella *governance* dell'IA, nella prevenzione e nella risposta tempestiva possono non solo ridurre i costi economici, ma anche proteggere il proprio rapporto con clienti e partner.

2.5.1 I costi richiesti alle aziende per adeguarsi al GDPR

Adeguarsi al GDPR continua a essere un impegno importante per le aziende anche nel 2025. Non si tratta più di un costo una tantum per mettere tutto in regola all'inizio, ma di un'attività costante. Le imprese devono dedicare tempo, personale e risorse per gestire i dati, controllare i rischi e rispondere a eventuali controlli delle autorità.

Negli ultimi anni, il mercato dei servizi legati al GDPR come consulenze, software per la gestione dei dati e controlli periodici è cresciuto molto. Questo mostra che le aziende non vogliono solo evitare multe, ma investono in protezione dei dati in modo continuativo, con spese regolari per mantenere tutto in ordine.

Dal punto di vista economico, il GDPR porta benefici concreti oltre ai costi di compliance. Secondo uno studio della *CNIL* (Commission Nationale de l'informatique et des Libertés, l'organo amministrativo e di regolamentazione francese responsabile

dell'attuazione della legge sulla privacy dei dati[89]) le misure di sicurezza imposte dal Regolamento hanno contribuito a ridurre in modo significativo i danni legati ai furti di identità e ai *data breach* (violazione dei dati). In Europa, le perdite dirette evitate grazie al GDPR sono stimate tra 405 e 988 milioni di euro, mentre considerando anche i costi indiretti, come la perdita di fiducia dei consumatori, il totale sale a 585–1.427 milioni di euro, di cui circa l'82% a beneficio delle aziende. In Francia, le stime indicano un risparmio tra 54 e 132 milioni di euro solo per i furti di identità[90]. Il GDPR, imponendo obblighi di sicurezza e notificazione, incentiva le imprese a investire in Cybersecurity, trasformando vincoli normativi in vantaggi economici tangibili. Rispetto al semplice rispetto della legge, adottare correttamente le misure previste dal regolamento contribuisce dunque a ridurre rischi finanziari concreti, aumenta la fiducia degli utenti e può essere considerato un investimento redditizio per le aziende.

Però, chi non rispetta le regole rischia multe pesanti. Nel 2025 le autorità europee hanno inflitto sanzioni per oltre 6 miliardi di euro, soprattutto a chi gestisce dati sensibili come quelli della sanità.

In Italia la situazione conferma l'importanza del GDPR. Dal 2018 al 2025 sono state comminate più di 2.330 sanzioni per un totale superiore a 6,19 miliardi di euro[91]. Il nostro Paese è al secondo posto per numero di multe, con oltre 237 milioni di euro di sanzioni accumulate. Questo dimostra che per molte aziende italiane rispettare il GDPR non è solo una formalità, ma una vera priorità[92].

Per affrontare questi costi e ridurre i rischi, le aziende si muovono in diversi modi: alcune affidano il ruolo del responsabile dei dati a professionisti esterni, altre investono in sistemi informatici aggiornati, software di protezione dei dati e strumenti per controlli e crittografia. Fondamentale è anche la formazione dei dipendenti, per far capire come trattare i dati e cosa fare in caso di problemi.

---

[89] CookieHub. *Che cos'è la CNIL?* [Blog post], https://www.cookiehub.com/it/blog/che-cose-la-cnil

[90] Ponti, Chiara, *"Investimenti cyber e benefici del GDPR: un'economia che fa bene alle aziende"*, *Cybersecurity360*, 6 giugno 2025, https://www.Cybersecurity360.it/news/investimenti-cyber-e-benefici-del-gdpr-uneconomia-che-fa-bene-alle-aziende/

[91] Key4Biz, *"GDPR, dal 2018 ad oggi sanzioni per 6,1 miliardi di euro: Italia al secondo posto per numero di multe"*, 6 maggio 2025, https://www.key4biz.it/gpdr-dal-2018-ad-oggi-sanzioni-per-61-miliardi-di-euro-italia-al-secondo-posto-per-numero-di-multe/532356/.

[92] Redazione, *"GDPR: calo del 33% per le sanzioni in Europa. Multe per 237,3 milioni in 7 anni in Italia"*, *AziendaBanca*, 04 febbraio 2025, https://www.aziendabanca.it/notizie/banche/report-dla-piper-gdpr-in-italia-sanzioni-per-237-milioni.

Adeguarsi al GDPR nel 2025 non è solo una questione legale, è un investimento continuo e strategico per proteggere dati, risorse economiche e reputazione. Ignorare le regole può costare molto di più che rispettarle.

2.6 Come le aziende mettono in pratica il GDPR

L'applicazione del GDPR nelle imprese costituisce uno dei passaggi più complessi dell'intero quadro europeo sulla protezione dei dati, poiché richiede alle organizzazioni di tradurre principi giuridici spesso astratti in procedure operative verificabili e continuativamente aggiornate. Le linee guida pubblicate dal Garante per la protezione dei dati personali, disponibili anche in formato sintetico, svolgono un ruolo fondamentale nel rendere intellegibili tali obblighi, poiché trasformano i precetti regolamentari in indicazioni concrete, orientate sia alla conformità sia alla capacità dell'impresa di dimostrare tale conformità secondo il principio di accountability[93]. Tuttavia, la loro importanza non è solo pratica. Esse rappresentano un punto di osservazione privilegiato sul modo in cui il GDPR opera realmente nel tessuto produttivo italiano, rivelando la distanza, talvolta ancora significativa tra la norma e la fisiologia dei processi aziendali.
Il primo elemento che emerge dall'analisi è che la conformità non può essere raggiunta senza una ricognizione preliminare e accurata dei trattamenti svolti. In molte imprese, soprattutto di dimensioni medio-piccole, l'effettiva mappatura dei dati risulta più complessa del previsto per la presenza di processi non formalizzati, sistemi *legacy*, utilizzo di software differenti e prassi operative consolidatesi nel tempo. La guida del garante suggerisce un percorso lineare: individuare quali dati vengono raccolti, per quali finalità, con quali strumenti e per quanto tempo, ma la sua traduzione pratica obbliga spesso le aziende a un ripensamento strutturale dei flussi informativi interni. In altre parole, l'adempimento non è solo una verifica tecnica, ma diventa anche un momento di analisi interna organizzativa che porta alla luce inefficienze, ridondanze e, talvolta, trattamenti inutili o sproporzionati. È proprio in questo passaggio che il GDPR dimostra la sua portata trasformativa, poiché il requisito di documentare le finalità e di assicurare

[93] Garante per la protezione dei dati personali, *"Guide e norme – Guide"*, GarantePrivacy.it, consultato il 21 novembre 2025, https://www.garanteprivacy.it/guide-e-norme/guide

la correttezza delle basi giuridiche impone alle imprese una revisione sostanziale, più che formale.

I principi di *privacy by design* e *by default* accentuano ulteriormente questa trasformazione. Pur essendo spesso richiamati in termini generali, essi implicano un modo diverso di concepire la progettazione di sistemi e procedure aziendali. La *privacy by default*, che richiede impostazioni iniziali sempre orientate alla minimizzazione del trattamento, forza le imprese ad abbandonare prassi tradizionali basate sull'accumulo indiscriminato dei dati "nel caso servissero" [94]. La *privacy by design*, invece, introduce un elemento di razionalizzazione preventiva. Ogni nuovo processo, prodotto o servizio deve essere preceduto da una valutazione strutturale del rischio e dall'individuazione di misure protettive adeguate. Le aziende che intendono applicare correttamente tali principi non possono limitarsi a modifiche superficiali delle informative o ad aggiornamenti tecnici minimi, ma devono integrare la logica della protezione dei dati all'interno dei processi decisionali strategici. Questa impostazione, sebbene onerosa, permette infatti di ridurre il rischio complessivo e di evitare interventi correttivi *ex post*, spesso più costosi.

Un ulteriore punto chiave è costituito dalla predisposizione del **registro dei trattamenti**. Sebbene esso venga talvolta percepito come un adempimento meramente compilativo, la sua funzione è in realtà strutturale. Rappresenta il documento cardine attraverso cui l'impresa rende trasparente la propria architettura del trattamento. La guida del garante, attraverso modelli semplificati, cerca di ridurre la complessità dell'adempimento, ma è l'azienda a dover affrontare la vera difficoltà, ossia mantenere il registro aggiornato nel tempo. Questo richiede non solo una supervisione centralizzata, ma anche un coinvolgimento costante delle diverse aree aziendali che effettuano i trattamenti. Ciò dimostra che l'*accountability* non è un requisito isolato, bensì una condizione organizzativa permanente che presuppone la capacità dell'impresa di monitorare se stessa in modo continuo. Proprio per questo, il registro diventa anche un banco di prova dell'effettiva maturità digitale e organizzativa dell'azienda.

In questo processo, la differenza tra imprese grandi e piccole non è tanto nelle prescrizioni normative che rimangono identiche quanto nella capacità di dotarsi degli strumenti e delle competenze necessari. Se le grandi organizzazioni possono contare su risorse interne dedicate, le PMI devono spesso ricorrere a consulenti esterni, il che rende il percorso di

[94] Ibidem.

adeguamento più disomogeneo e suscettibile di soluzioni minime, orientate più alla forma che alla sostanza. Tale dinamica offre una chiave interpretativa utile per analizzare l'attuazione del GDPR nel contesto italiano. La normativa, pur essendo uniforme, produce effetti differenti a seconda della struttura aziendale, mettendo in luce come l'effettiva protezione dei dati non dipenda solo dalle regole ma dal grado di maturità organizzativa dei soggetti chiamati a rispettarle.

2.6.1 Tenuta registro delle attività del trattamento dei dati personali

Il registro delle attività di trattamento dei dati personali, introdotto dall'articolo 30 del Regolamento Generale sulla Protezione dei Dati (GDPR – Regolamento UE 2016/679), rappresenta oggi un elemento centrale non solo per la compliance normativa, ma anche per la *governance* interna delle imprese. Se da un lato il registro è spesso percepito come un adempimento burocratico, dall'altro la sua funzione reale va ben oltre la semplice compilazione. Esso costituisce infatti uno strumento strategico per garantire trasparenza, responsabilità e supervisione dei processi di trattamento dei dati personali.

Dal punto di vista normativo, l'articolo 30 GDPR richiede che il registro includa informazioni fondamentali, tra cui: i dati identificativi del titolare del trattamento e, se nominato, del responsabile; le finalità dei trattamenti; le categorie di interessati e di dati personali trattati; i destinatari dei dati, compresi eventuali trasferimenti verso paesi terzi o organizzazioni internazionali; i termini di conservazione; e una descrizione delle misure tecniche e organizzative adottate per proteggere i dati[95]. Questi requisiti, se letti con uno sguardo critico, mostrano chiaramente come il registro non sia soltanto una raccolta di informazioni statiche, ma un documento dinamico che riflette il reale livello di protezione e di gestione dei dati nell'organizzazione.

L'attuazione pratica del registro pone diverse sfide per le imprese, soprattutto per le piccole e medie realtà. La complessità aumenta con il numero di trattamenti effettuati, la varietà dei dati raccolti e la partecipazione di soggetti terzi al trattamento. A questo proposito, il ruolo del *Data Protection Officer* (DPO) diventa cruciale, in quanto non solo garantisce che le informazioni siano corrette e aggiornate, ma agisce come supervisore della qualità del registro, integrando le informazioni con le valutazioni dei rischi e le

[95] Art..30 del GDPR –Registro delle attività di trattamento.

misure di sicurezza adottate.[96] In organizzazioni più articolate, il DPO deve coordinarsi con i responsabili di reparto, con i responsabili IT e con il management per trasformare il registro in uno sistema operativo capace di supportare audit interni, verifiche esterne e decisioni strategiche[97].

Il registro, se utilizzato correttamente, può essere uno strumento di prevenzione dei rischi. Ad esempio, una documentazione accurata dei trattamenti permette di identificare criticità potenziali prima che si verifichino violazioni, rendendo possibile un intervento proattivo. Analogamente, in caso di incidenti o richieste degli interessati ai sensi degli articoli 15-22 GDPR, avere un registro dettagliato e aggiornato consente di rispondere rapidamente e in maniera completa, riducendo esposizione a sanzioni e danni reputazionali[98].

Oltre alla dimensione organizzativa, il registro assume un valore analitico se integrato con le misure di sicurezza. La descrizione delle procedure di backup, crittografia, controlli di accesso e altre tecnologie non deve essere una mera elencazione, ma una valutazione del loro reale impatto sulla protezione dei dati. Questo approccio consente alle aziende di identificare eventuali lacune, confrontare le soluzioni adottate con le *best practice* del settore e pianificare interventi migliorativi. Nei casi in cui vi siano trasferimenti verso paesi terzi, la documentazione delle garanzie adottate, come clausole contrattuali standard o meccanismi equivalenti, assume una funzione di accertamento preventivo essenziale per sopprimere rischi legali e reputazionali.

Il registro delle attività non va interpretato solo come obbligo formale imposto dalla legge, ma può essere considerato un indicatore della maturità organizzativa in materia di privacy e gestione dei dati. Le imprese che adottano un registro dettagliato, dinamico e integrato nei processi decisionali mostrano una capacità superiore di *accountability*, capacità di audit interno e consapevolezza dei rischi. Al contrario, registri compilati superficialmente o aggiornati sporadicamente possono generare un falso senso di sicurezza e, in caso di controlli, tradursi in criticità legali significative.

Il registro delle attività di trattamento è molto più di un adempimento formale, è un sistema operativo e strategico che, se gestito in maniera attenta e analitica, contribuisce non solo alla conformità normativa ma anche all'efficacia della *governance* dei dati, alla

[96] Art. 39 GDPR (compiti del DPO).
[97] Articoli 24, 25, 32 GDPR – Responsabilità del titolare e misure di sicurezza.
[98] Linee guida EDPB (European Data Protection Board) sull'accountability e tenuta del registro.

prevenzione dei rischi e al rafforzamento della cultura organizzativa in materia di privacy. La sua importanza emerge soprattutto nelle aziende complesse e nei contesti ad alto rischio, dove la corretta documentazione rappresenta un fattore critico di successo nella gestione dei dati personali.

2.7 La valutazione d'impatto sulla protezione dei dati (DPIA)

La valutazione d'impatto sulla protezione dei dati personali (DPIA) rappresenta una delle innovazioni più rilevanti introdotte dal Regolamento europeo sulla protezione dei dati (GDPR, Regolamento UE 2016/679). Essa non si limita a un obbligo formale, ma costituisce uno strumento strategico volto a identificare, analizzare e gestire in anticipo i rischi che un trattamento può comportare per i diritti e le libertà degli interessati. La DPIA richiede un approccio proattivo e multidisciplinare, che coinvolge non solo il titolare del trattamento, ma anche il responsabile, *il Data Protection Officer* (DPO) e, idealmente, un campione rappresentativo dei soggetti interessati per comprendere le percezioni e le aspettative riguardo ai rischi[99].

L'idea di valutazione preventiva non nasce nel contesto della privacy, ma trae origine dagli strumenti di valutazione d'impatto ambientale sviluppati negli Stati Uniti alla fine degli anni Sessanta. Questa logica è stata progressivamente estesa al diritto e alla regolazione, fino a diventare centrale nel GDPR, che introduce il principio di *accountability* anche attraverso la DPIA, richiedendo di documentare non solo le decisioni, ma anche la metodologia di analisi dei rischi e le misure adottate per contenere il loro impatto.

Il Regolamento, all'articolo 35, distingue tra un caso generale, in cui la DPIA è raccomandata ogniqualvolta un trattamento presenti rischi elevati, e casi specifici in cui essa diventa obbligatoria. Tra questi si includono: trattamenti basati su tecnologie innovative che producono effetti giuridici significativi; trattamenti su larga scala di categorie particolari di dati o dati relativi a condanne penali; sorveglianza sistematica su larga scala di aree pubbliche[100]. La complessità e l'interpretazione dei criteri rendono

[99] Art. 35 GDPR.
[100] Art. 35(1) GDPR.

necessario un esercizio di giudizio da parte del titolare, che deve documentare le scelte, anche se decide di non effettuare la DPIA pur ricorrendo i presupposti normativi.

Dal punto di vista operativo, la DPIA deve includere una descrizione completa del trattamento, delle finalità e della base giuridica, la valutazione della necessità e proporzionalità delle operazioni rispetto agli obiettivi, l'analisi dei rischi per gli interessati e le misure adottate per ridurre tali rischi[101]. Ciò comporta la stima della probabilità e gravità di eventi indesiderati, la loro origine e gli impatti sui diritti degli interessati, con decisioni mirate a ridurre, trasferire o accettare i rischi residui. Questo approccio consente di integrare la protezione dei dati nella progettazione dei processi aziendali, rispettando il principio di *privacy by design* e *by default*.

Un esempio pratico italiano che rende evidente l'impatto della DPIA riguarda il gruppo *Ferrovie dello Stato Italiane*, che ha introdotto sistemi di controllo avanzato dei flussi di passeggeri e dei dati biometrici per l'accesso a determinate aree delle stazioni[102]. La società ha dovuto condurre una DPIA approfondita, analizzando il rischio derivante dalla raccolta e dall'archiviazione di dati biometrici sensibili, integrando misure tecniche come crittografia e pseudonimizzazione e definendo protocolli operativi per l'accesso ai dati[103]. L'analisi ha permesso di identificare punti critici nei processi interni, come il trattamento dei dati da parte di fornitori terzi, e di adottare procedure preventive per garantire la conformità normativa, riducendo al contempo i rischi per i passeggeri. Questo caso dimostra come la DPIA non sia solo un adempimento formale, ma un reale strumento di gestione strategica dei dati, capace di influire sulle decisioni operative e di sicurezza.

Dal punto di vista temporale, la DPIA deve essere svolta nella fase iniziale della progettazione del trattamento, integrando le misure di tutela fin dall'inizio. Tuttavia, non si tratta di un documento statico. Deve essere aggiornata lungo l'intero ciclo di vita del trattamento, soprattutto in caso di modifiche tecnologiche o evoluzione delle finalità. La DPIA diventa così uno strumento dinamico, utile anche per audit interni ed esterni e per rispondere alle richieste degli interessati, contribuendo a dimostrare la responsabilità attiva del titolare e la compliance dell'organizzazione[104].

---

[101] Considerando 90–92 GDPR.

[102] Gruppo Ferrovie dello Stato Italiane**,** *Rapporto di sostenibilità 2023*, Roma, aprile 2023, 248 pagine, https://www.fsitaliane.it/content/dam/fsitaliane/Documents/sostenibilit%C3%A0/rapporto-di-sostenibilit%C3%A0-2022/rapporto-di-sostenibilit%C3%A0-2022-gruppo-fs.pdf

[103] Art. 35(3) GDPR.

[104] WP29, *Guidelines on DPIA*, WP 248 rev.01, p.6.

La DPIA rappresenta un elemento cardine della *governance* dei dati personali, andando oltre la semplice ricostruzione normativa. Essa richiede capacità analitiche, multidisciplinarità e una visione strategica della gestione dei dati. La sua corretta applicazione consente alle aziende non solo di ridurre i rischi legali, ma anche di ottimizzare i processi, aumentare la trasparenza verso gli stakeholder e rafforzare la fiducia dei cittadini, trasformando il GDPR in una risorsa operativa concreta e non puramente formale.

2.8 Cambiamenti e sfide aziendali introdotti dal GDPR

L'adeguamento delle imprese al GDPR comporta trasformazioni importanti che coinvolgono tutti gli aspetti dell'organizzazione, dalla gestione dei dati alla struttura dei processi interni, fino alla cultura aziendale. Non si tratta di un semplice adeguamento formale, ma di un intervento sistemico che richiede modifiche strutturali, investimenti tecnologici e sviluppo di competenze interne. Il regolamento europeo impone di rivedere in maniera puntuale il modo in cui le aziende raccolgono, conservano, elaborano e proteggono i dati personali, imponendo standard di sicurezza più rigorosi e la necessità di una documentazione continua e dettagliata di tutte le operazioni di trattamento[105].
I cambiamenti coinvolgono innanzitutto la *governance* dei dati. Le imprese devono chiarire ruoli e responsabilità all'interno dell'organizzazione, definendo chi è incaricato di controllare i flussi di dati, chi verifica la sicurezza dei sistemi e chi supervisiona la conformità normativa. La figura del DPO (Data Protection Officer), se presente, diventa centrale non solo per la gestione operativa, ma anche come punto di riferimento strategico, capace di supportare le decisioni aziendali in relazione alla protezione dei dati e alla valutazione dei rischi. Questo richiede un cambiamento culturale, poiché la privacy e la protezione dei dati non sono più solo adempimenti burocratici, ma elementi centrali per la strategia aziendale[106].

[105] GDPR.net, «Cosa devono fare le aziende per adeguarsi al GDPR», GDPR.net, consultato il 19 novembre 2025, https://www.gdpr.net/gdpr-cosa-devono-fare-le-aziende-per-adeguarsi/
[106] Agenda Digitale, «Impatto del GDPR sulle piccole e medie imprese: il buono, brutto e il cattivo», AgendaDigitale.eu, consultato il 19 novembre 2025, https://www.agendadigitale.eu/sicurezza/impatto-del-gdpr-sulle-piccole-e-medie-imprese-il-buono-brutto-e-il-cattivo/

Dal punto di vista operativo, l'adeguamento al GDPR comporta una revisione dei flussi informativi e dei processi interni. Le imprese devono mappare tutti i dati raccolti, identificare le finalità di ciascun trattamento e analizzare come questi dati vengono condivisi all'interno dell'organizzazione e verso soggetti esterni. Devono inoltre garantire che i dati siano trattati nel rispetto dei principi di *privacy by design* e *privacy by default*, adattando le misure di sicurezza in modo proporzionato al livello di rischio e alla sensibilità delle informazioni. L'uso di sistemi informatici sicuri, controlli di accesso, backup regolari e tecnologie di crittografia non è solo una raccomandazione tecnica, ma un obbligo imprescindibile per garantire la conformità.

Per le piccole e medie imprese, queste trasformazioni rappresentano sfide particolarmente complesse. Spesso non dispongono di personale dedicato alla gestione della privacy né di budget significativi da destinare all'adeguamento. Tuttavia, il GDPR impone anche a queste realtà di documentare tutte le attività di trattamento, predisporre audit periodici sulla sicurezza dei dati e notificare tempestivamente eventuali violazioni alle autorità competenti[107]. Questo processo può comportare un impegno organizzativo notevole, richiedendo non solo investimenti economici, ma anche modifiche ai processi decisionali e all'allocazione delle responsabilità interne.

Nonostante le difficoltà, l'adeguamento al GDPR offre opportunità strategiche. Le imprese che affrontano in modo strutturato la revisione dei propri sistemi di gestione dei dati possono ottenere significativi benefici operativi. L'analisi dei dati, la standardizzazione dei processi e la documentazione delle attività di trattamento contribuiscono a ridurre inefficienze e incoerenze interne, migliorando la qualità dei dati e la capacità di analisi aziendale. Inoltre, l'attuazione di misure di sicurezza adeguate riduce il rischio di incidenti e di attacchi informatici, proteggendo il patrimonio informativo e minimizzando le conseguenze economiche e reputazionali di eventuali violazioni.

Il GDPR spinge le imprese a considerare la protezione dei dati come un fattore competitivo, non più solo come un obbligo normativo. La capacità di garantire la sicurezza dei dati, di rispettare i diritti degli interessati e di reagire prontamente in caso di problemi aumenta la fiducia di clienti, partner e fornitori, rafforzando la reputazione

[107] Ibidem.

aziendale. La compliance diventa quindi uno strumento di *governance* e di comunicazione trasparente, capace di valorizzare la credibilità dell'impresa sul mercato.
Un aspetto spesso trascurato riguarda le conseguenze a lungo termine dell'adeguamento. La trasformazione introdotta dal GDPR non si esaurisce con la semplice implementazione delle misure richieste, ma richiede un aggiornamento continuo dei processi, una formazione costante del personale e una valutazione periodica dei rischi. Le aziende devono sviluppare una cultura della responsabilità, in cui la protezione dei dati diventa un elemento integrato nella pianificazione strategica, nella gestione dei progetti e nella definizione delle priorità aziendali.
Il GDPR introduce cambiamenti che vanno ben oltre la compliance formale. Le imprese sono chiamate a ripensare la gestione dei dati, a rafforzare la sicurezza dei sistemi, a sviluppare competenze interne e a consolidare la cultura organizzativa. L'adozione di queste misure, se gestita in maniera coerente e sistematica, non solo garantisce la conformità normativa, ma diventa anche un mezzo per migliorare la reputazione, la competitività e l'efficienza dell'impresa.

2.9 Il ruolo della Cybersecurity nelle imprese

Nel contesto digitale contemporaneo, i dati assumono un ruolo centrale nella gestione e nello sviluppo delle imprese. L'ampia disponibilità di informazioni generate quotidianamente ha modificato profondamente il modo in cui le aziende operano, imponendo una riconsiderazione dei processi interni e delle strategie decisionali. Diversi studi indicano che la maggior parte dei dati attualmente presenti è stata generata negli ultimi due anni, segnalando un'accelerazione senza precedenti nella produzione e circolazione delle informazioni. Questa crescita esponenziale rende necessario per le imprese adottare sistemi avanzati di gestione dei dati, non solo per ottimizzare l'efficienza operativa, ma anche per sostenere processi decisionali più informati e strategici[108].
La centralità dei dati nell'economia moderna ha portato a considerare le informazioni non più come semplici strumenti operativi, ma come veri e propri asset aziendali. La capacità di raccogliere, organizzare e analizzare i dati in modo efficace determina il successo

[108] The European House – Ambrosetti, *InnoTech Report 2023: l'ecosistema dell'innovazione digitale*, InnoTech Community, Milano, maggio 2023, p. 225.

competitivo delle imprese, influenzando la loro capacità di innovare, di comprendere le esigenze dei clienti e di anticipare i trend di mercato. Le imprese che adottano una gestione dei dati organizzata e sicura riescono a ottenere benefici concreti, possono seguire con maggiore precisione l'andamento delle proprie attività, utilizzare le risorse in modo più efficace e sviluppare nuovi modelli di business fondati sulle informazioni disponibili[109].

Parallelamente, l'importanza crescente dei dati ha spinto molte grandi aziende a introdurre figure dedicate alla sicurezza informatica a livello dirigenziale, inserendole all'interno dei Consigli di amministrazione. Questo fenomeno riflette la consapevolezza che la protezione dei dati non può essere considerata un mero adempimento tecnico, ma deve essere parte integrante della strategia aziendale complessiva, con impatti diretti sulla *governance* e sul rischio di credibilità aziendale. La gestione dei dati richiede infatti un equilibrio tra la possibilità di sfruttare le informazioni per generare valore e la necessità di garantire la sicurezza e la protezione delle stesse, in conformità con le normative vigenti.

Tuttavia, la centralità dei dati comporta anche un aumento dei rischi legati alla sicurezza. L'evoluzione costante delle minacce informatiche ha portato allo sviluppo di attacchi sempre più sofisticati, capaci di compromettere le infrastrutture aziendali e di esporre le informazioni sensibili a rischi economici e reputazionali significativi. La frequenza e la complessità di tali attacchi impongono alle imprese di adottare misure di Cybersecurity avanzate, che comprendano la protezione preventiva dei sistemi, osservazione continua e piani di risposta rapida in caso di incidenti. In questo senso, la Cybersecurity assume un ruolo strategico imprescindibile, non solo tutela i dati aziendali, ma garantisce la continuità operativa e il mantenimento della fiducia di clienti e partner.

[109] Beccara, Cirolini Lunelli, Ranise, *Protezione dei dati personali e sicurezza informatica*, Franco Angeli, Milano, 2021, pp. 45-48.

110

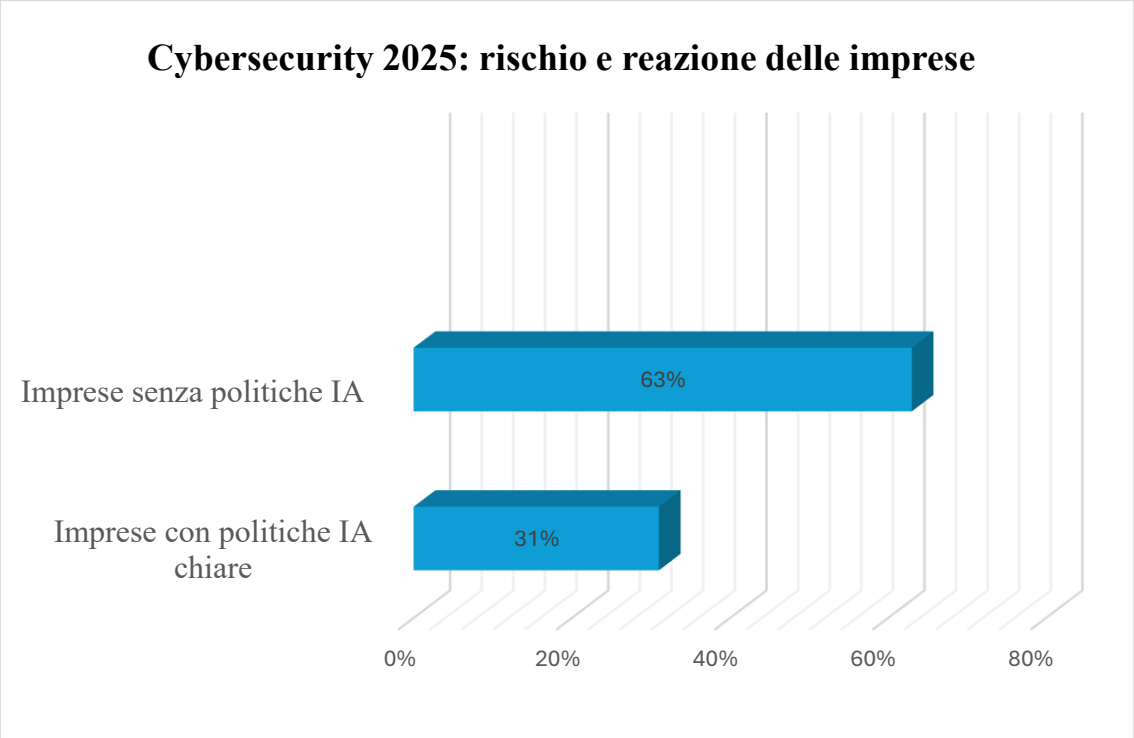

Figura 3: Elaborazione su dati ANSA (2025), Innovation Post (2025) e Clusit (2025). Il dataset comprende informazioni sul tasso di imprese attaccate, sull'aumento della spesa in sicurezza, sull'incremento annuale degli incidenti informatici, nonché il numero di *63% imprese prive di politiche di sicurezza* e *31% imprese dotate di politiche chiare sull'IA*.

Un'osservazione interessante emerge confrontando le imprese italiane con politiche di Cybersecurity avanzate rispetto a quelle prive di strategie definite. Secondo i dati elaborati da *ANSA, Innovation Post* e *Clusit* (2025), il 63% delle aziende italiane non dispone di politiche di sicurezza strutturate, mentre solo il 31% adotta linee guida chiare, spesso integrate con strumenti di intelligenza artificiale per la gestione dei dati. Questo divario evidenzia come la percezione del rischio e la capacità di investimento siano fattori critici. Le aziende più strutturate non solo riducono la probabilità di violazioni, ma

[110] *ANSA*. "Il 73 % delle grandi aziende italiane colpito da hacker". *ANSA*, 27 febbraio 2025, Milano, https://www.ansa.it/canale_tecnologia/notizie/Cybersecurity/2025/02/27/hacker-contro-grandi-aziende-colpito-il-73-delle-italiane_d9e29ef9-9a39-401c-9e27-46361ae21d36.html
Innovation Post, «Spesa per Cybersecurity in aumento del 60%: previsioni 2025», Innovation Post. https://www.innovationpost.it/tecnologie/industrial-security/cyber-security-aumenta-la-spesa-ma-si-perdono-ancora-troppi-dati-ecco-perche-i-sistemi-tradizionali-di-protezione-non-funzionano/
Clusit, «Anteprima Rapporto Clusit 2025: +15% crescita attacchi in Italia», Clusit.it, https://clusit.it/wp content/uploads/area_stampa/2025/Anteprima_Rapporto_Clusit_2025.pdf

riescono anche a utilizzare i dati in modo più strategico, migliorando la qualità delle decisioni e la competitività sul mercato.

Tuttavia, l'adozione di misure avanzate comporta costi significativi e richiede competenze interne specializzate, che risultano spesso carenti nelle PMI. In questa circostanza, emerge una tensione tra la necessità di garantire la sicurezza dei dati e la capacità operativa dell'impresa, indicando che la semplice implementazione di strumenti tecnologici non è sufficiente: serve un approccio integrato che includa *governance*, formazione del personale e supervisione continua dei rischi.

Dal confronto tra le due categorie, si evidenzia anche l'impatto reputazionale. Le imprese con politiche chiare sono percepite come più affidabili dai clienti e dai partner, rafforzando la fiducia e la sostenibilità a lungo termine, mentre le aziende con gestione lacunosa dei dati rischiano danni economici e reputazionali in caso di incidenti. Questo confronto suggerisce che, oltre al rispetto formale del GDPR, la Cybersecurity può diventare un vero vantaggio competitivo per chi sa integrarla in modo strategico nel modello di business.

La crescente esposizione delle imprese alle minacce digitali evidenzia come le organizzazioni stiano sviluppando una maggiore consapevolezza della necessità di investire in misure di protezione adeguate. Una gestione attenta e sicura dei dati consente di ottenere vantaggi competitivi come: informazioni precise e aggiornate permettono previsioni più accurate, una migliore comprensione dei comportamenti e delle preferenze dei clienti e un'ottimizzazione delle esperienze offerte agli utenti. Allo stesso tempo, la protezione dei dati diventa un elemento distintivo della reputazione aziendale, rafforzando la fiducia dei consumatori e dei soggetti coinvolti. In quest'ottica, l'investimento in Cybersecurity e nella gestione dei dati non rappresenta un costo, ma una risorsa strategica che può incidere direttamente sulla crescita e sulla sostenibilità delle imprese nel lungo periodo.

2.10 Protezione dei dati personali nell'era dell'Internet of Things

L'evoluzione tecnologica e la diffusione capillare di dispositivi connessi rendono *l'Internet of Things* un elemento strutturale del paesaggio digitale contemporaneo. In tale contesto, la gestione dei dati personali non può più essere confinata a processi isolati. Il

flusso continuo di informazioni sensoriali, ambientali, comportamentali attraverso sensori, gateway (dispositivo hardware o software che collega due reti diverse), cloud e applicazioni, crea un sistema interconnesso e collegato che comporta rischi nuovi e complessi[111]. I dati raccolti da questi dispositivi possono essere combinati con altre fonti a volte variegate, rendendo possibile la re-identificazione anche di soggetti che avevano ritenuto i propri dati "anonimi", oppure la costruzione di profili approfonditi, stratificati e dinamici, con conseguenze significative sul piano della privacy e dei diritti individuali. Questo fenomeno è oggi oggetto di crescente attenzione nel panorama scientifico internazionale. Uno studio recente: *A survey on privacy and security issues in IoT-based environments: Technologies, protection measures and future directions*, mette in luce come le vulnerabilità emergano a diversi livelli come: firmware, protocolli di comunicazione, gestione del ciclo di vita dei dispositivi, gestione degli accessi e interfaccia con sistemi cloud[112].

In risposta a queste complessità, il Regolamento (UE) 2016/679 (GDPR) propone un quadro normativo fondato su responsabilità attiva (accountability) e misure proporzionate come il registro dei trattamenti (art. 30), misure di sicurezza tecniche e organizzative (art. 32), valutazione d'impatto (DPIA, art. 35), nomina di un responsabile della protezione dati (art. 37) e laddove necessario un rappresentante nell'Unione (art. 27). Tali strumenti, pensati in un contesto generico, devono essere reinterpretati e rafforzati nell'ambito dell'IoT, adattando le garanzie al livello di rischio effettivo, alla natura dei dispositivi, alle risorse hardware/software disponibili e ai flussi reali di dati.

Va considerata la fragilità strutturale dell'ecosistema IoT. Molte soluzioni soprattutto nel mercato consumer o in dispositivi "leggeri" presentano vulnerabilità intrinseche, difficoltà di aggiornamento firmware, assenza di controlli di accesso robusti, uso di protocolli insicuri. Recenti rassegne della letteratura, come *A survey on Cybersecurity in IoT* (2025), mostrano come i dispositivi IoT costituiscano un vettore privilegiato di

[111] G. Malgieri, G. Comandè (a cura di), *Guida al trattamento e alla sicurezza dei dati personali*, Giuffrè Francis Lefebvre, Milano, 2021, p. 142.

[112] Sun P., Wan Y., Wu Z., Fang Z., Li Q., A survey on privacy and security issues in IoT-based environments: Technologies, protection measures and future directions, Computers & Security, vol. 148 (2025) https://www.sciencedirect.com/science/article/abs/pii/S0167404824004024

attacco, con criticità che spaziano dalla privacy degli utenti alla compromissione dell'integrità e disponibilità dei sistemi[113].

Dal punto di vista pratico per un'impresa che decide di adottare soluzioni IoT (*smart-device*, sensori, dispositivi connessi) la sfida di conformità al GDPR si trasforma in un problema di *governance*, ingegneria e gestione del rischio. Occorre applicare misure concrete, come la cifratura dei dati (in transito e a riposo), l'uso di protocolli sicuri, l'aggiornamento continuo dei firmware, il controllo degli accessi, audit regolari, controllo e tracciamento dei trattamenti. Ma queste misure non bastano. La complessità dell'ecosistema richiede anche una politica aziendale coerente, figure responsabili, formazione del personale e una documentazione trasparente.

Da questo punto di vista, le misure previste dal GDPR registro trattamento, DPIA, codici di condotta, certificazioni assumono un valore strategico. Esse non costituiscono un semplice adempimento formale, ma un framework operativo per gestire in maniera consapevole i rischi legati all'IoT. Tuttavia, la letteratura evidenzia che non tutte le contromisure sono ugualmente efficaci; per esempio, la presenza di vulnerabilità firmware, la scarsa manutenzione e la debolezza dei protocolli di rete riducono l'efficacia della cifratura o della pseudonimizzazione, se non accompagnate da una *governance* solida[114].

La protezione dei dati personali nell'era dell'IoT richiede un approccio scientifico e integrato. Non basta conoscere la norma, occorre interpretarla alla luce delle evidenze tecnologiche e dei rischi reali, adottando misure tecniche adeguate, strutturando processi di *governance* efficaci e garantendo trasparenza e responsabilità. Solo in questo modo l'uso dell'IoT può essere compatibile con la tutela dei diritti e con la conformità normativa.

---

[113] *Dritsas E. Trigka M., A Survey on Cybersecurity in IoT, Future Internet 2025, 17(1),30, https://www.mdpi.com/1999-5903/17/1/30*

[114] Ahmed, S. F., Shawon, S. S., Bhuyian, A., Afrin, S., Mehjabin, A., Kuldeep, S. A., Bin Alam, M. S., & Gandomi, A. H. (2025). *Forensics and security issues in the Internet of Things*. Wireless Networks. https://link.springer.com/article/10.1007/s11276-025-03942-2

2.11 Il caso Amazon: la maxi-sanzione del CNPD per profilazione illecita ai fini pubblicitari

Nei paragrafi precedenti ho analizzato il quadro normativo del GDPR, soffermandomi sugli obblighi che le imprese devono rispettare, sui costi connessi all'adeguamento e sulle sanzioni previste in caso di violazioni. Alla luce di questo contesto, il caso Amazon assume particolare rilevanza perché mostra in modo concreto come le autorità europee applichino tali principi nei confronti delle grandi piattaforme digitali. Esso rappresenta un esempio emblematico di come il mancato rispetto delle regole sulla trasparenza, sul consenso e sulla corretta gestione dei dati personali possa tradursi in conseguenze economiche e reputazionali di notevole impatto, fornendo un utile punto di partenza per approfondire le dinamiche pratiche della compliance nel settore digitale.

Nel luglio 2021, il garante per la protezione dei dati del Lussemburgo (CNPD – Commission Nationale pour la Protection des Données) ha inflitto ad Amazon Europe Core S.à r.l. una sanzione amministrativa di 746 milioni di euro, la più elevata mai comminata nell'ambito del GDPR[115]. La vicenda suscitò immediatamente clamore internazionale, non solo per l'entità eccezionale della multa, ma soprattutto per la natura delle contestazioni: a differenza di numerosi casi noti, legati a violazioni della sicurezza o *data breach*, la sanzione contro Amazon derivava da pratiche di profilazione dei dati per finalità pubblicitarie, ritenute illecite e non conformi ai principi fondamentali del GDPR.

Il caso prende avvio nel 2018, quando un'organizzazione europea per la tutela dei consumatori e dei diritti digitali presentò una serie di segnalazioni contro Amazon. Le segnalazioni contestavano il fatto che Amazon raccogliesse ed elaborasse dati personali degli utenti per costruire profili comportamentali estremamente dettagliati e utilizzarli a fini di pubblicità personalizzata, senza una base giuridica valida e senza fornire informazioni chiare e trasparenti agli utenti. In particolare, si sosteneva che gli utenti non fossero pienamente consapevoli dell'ampiezza dei trattamenti, né ricevessero

[115] CNPD, "CNPD imposes fine of EUR 746 million on Amazon Europe Core S.à r.l.", 2021, https://cnpd.public.lu/en/actualites/national/2025/03/amazon-decision.html

un'informativa sufficiente a spiegare come i loro dati venissero combinati, incrociati e utilizzati per modellare le loro preferenze[116].

A seguito di questi esposti, il CNPD avviò un'indagine approfondita per analizzare il funzionamento dei sistemi pubblicitari e di profilazione di Amazon. L'autorità esaminò come fossero raccolti e trattati i dati derivanti dagli acquisti, dalla navigazione e dalle interazioni degli utenti all'interno dell'ecosistema Amazon. Dall'analisi emerse che il trattamento dei dati si basava su un consenso ritenuto non valido, insufficiente e non liberamente espresso dagli utenti. Inoltre, il CNPD osservò che gli utenti non disponevano di strumenti chiari e facilmente accessibili per opporsi alla profilazione o gestire il proprio consenso in modo dettagliato[117].

Un aspetto centrale della vicenda riguardava la profilazione automatizzata, ossia la capacità di Amazon di costruire modelli predittivi molto dettagliati sui comportamenti futuri dei clienti. Il CNPD rilevò che gli utenti non erano informati in maniera trasparente sul funzionamento di tali algoritmi né sull'uso che ne veniva fatto, violando così il principio di limitazione della finalità sancito dall'articolo 5 del GDPR. I dati personali venivano infatti impiegati per scopi ulteriori rispetto a quelli dichiarati, creando profili predittivi dettagliati senza che gli utenti avessero reale consapevolezza o controllo sui trattamenti.

La decisione della CNPD sottolineò tre violazioni principali. La prima riguardava la mancanza di una base giuridica valida ai sensi dell'articolo 6 del GDPR: Amazon trattava dati personali per finalità pubblicitarie senza il consenso valido degli utenti né altra giustificazione giuridica lecita. La seconda violazione riguardava i principi di correttezza e trasparenza (artt. 5, 12 e 13 GDPR), poiché le informazioni fornite agli utenti non erano sufficientemente comprensibili e non permettevano di conoscere l'estensione reale dei trattamenti e dei meccanismi di profilazione. La terza violazione era relativa al principio di limitazione della finalità, dato che i dati venivano impiegati per scopi ulteriori rispetto a quelli originariamente dichiarati e comunicati agli utenti.

L'autorità sottolineò inoltre la gravità delle violazioni considerando la scala del trattamento e il ruolo centrale della profilazione nel modello di business di Amazon, che

[116] Shead, Sam, *"Amazon hit with $887 million fine by European privacy watchdog"*, *CNBC*, 30 luglio 2021, https://www.cnbc.com/2021/07/30/amazon-hit-with-fine-by-eu-privacy-watchdog-.html

[117] Luxtimes, *"Amazon Europe fined €746 mn for data protection breaches"*, Luxtimes.lu, 30 luglio 2021, https://www.luxtimes.lu/businessandfinance/amazon-europe-fined-746-mn-for-data-protection-breaches/50260710.html

gestisce milioni di utenti in tutta l'Unione Europea. Il CNPD notò che il GDPR si applica pienamente anche alle grandi piattaforme digitali e che le logiche economiche non possono giustificare trattamenti poco trasparenti o non negoziabili dei dati personali. La decisione mostrò chiaramente che, indipendentemente dalla potenza economica o dalle dimensioni dell'impresa, la normativa europea tutela il diritto alla trasparenza, alla liceità e all'autodeterminazione digitale degli utenti.

Amazon reagì contestando le accuse, sostenendo che non vi fosse stata alcuna violazione dei dati e che nessun dato personale fosse stato divulgato impropriamente. L'azienda dichiarò che la decisione del CNPD si basava su un'interpretazione soggettiva delle norme e annunciò l'intenzione di presentare ricorso, definendo la sanzione sproporzionata e ingiustificata.

Dal punto di vista del GDPR, questo caso dimostra come il regolamento protegga i diritti degli utenti anche in assenza di incidenti di sicurezza, consentendo alle autorità di verificare la liceità dei trattamenti, la trasparenza, la proporzionalità dei dati e la correttezza dei processi di profilazione. La multa record di 746 milioni di euro rappresenta un chiaro segnale a tutte le imprese: il GDPR impone limiti stringenti all'uso dei dati personali, alla profilazione e all'adozione di algoritmi predittivi, richiedendo il rispetto dei principi di trasparenza, liceità, correttezza e accountability. Anche se la vicenda è tuttora oggetto di ricorsi, il caso Amazon rimane un punto di riferimento fondamentale per comprendere l'impatto reale del GDPR sulle grandi piattaforme digitali e sulle responsabilità associate all'uso dei dati personali.

Inoltre, il caso Amazon evidenzia come il GDPR non sia uno strumento limitato alla sicurezza informatica, ma rappresenti una cornice normativa ampia e vincolante che disciplina il trattamento dei dati personali in tutte le sue forme, compresa la profilazione automatizzata e l'utilizzo di algoritmi predittivi a fini commerciali. La sanzione record comminata dal CNPD dimostra che le autorità europee sono pronte a intervenire anche contro le più grandi piattaforme digitali, qualora vengano compromessi i principi di trasparenza, liceità, correttezza e accountability. Per le imprese, il caso costituisce un monito chiaro: non basta garantire la sicurezza dei sistemi, ma è fondamentale assicurare che tutti i processi di trattamento dei dati rispettino i diritti fondamentali degli utenti, dalla raccolta delle informazioni fino alla profilazione automatizzata. In questo senso, la vicenda Amazon rappresenta un esempio emblematico dell'impatto reale del GDPR sulle

aziende e della crescente responsabilità delle piattaforme digitali nella gestione dei dati personali dei cittadini europei.

CAPITOLO TERZO

L'INTELLIGENZA ARTIFICIALE IN AZIENDA PER PROTEGGERE I DATI

La rapida diffusione dei sistemi di Intelligenza Artificiale rappresenta oggi uno dei principali fattori di trasformazione nella gestione delle informazioni e, in particolare, nella protezione dei dati personali all'interno delle organizzazioni. Dopo aver analizzato nel primo capitolo i fondamenti della Cybersecurity e nel secondo gli obblighi introdotti dal GDPR per le imprese, è possibile osservare come l'IA si inserisca in questo quadro come uno strumento ambivalente. Da un lato una risorsa estremamente potente per migliorare i processi di sicurezza, dall'altro un potenziale elemento di rischio se adottata senza adeguate misure di *governance*, trasparenza e verifica[118]. È proprio questa duplice natura dell'intelligenza artificiale a rendere necessario un approfondimento non meramente tecnologico, ma orientato all'analisi delle strutture di governo, controllo e responsabilizzazione dei sistemi automatizzati, che costituiranno il fulcro dell'analisi sviluppata nel capitolo successivo.

L'IA, infatti, è parte integrante della trasformazione digitale che sta ridefinendo i modelli organizzativi, i flussi informativi e le strategie aziendali. Se utilizzata in modo competente e accompagnata da opportune competenze tecniche e organizzative, essa può rafforzare in modo significativo la capacità delle imprese di prevenire le minacce informatiche, individuare vulnerabilità, gestire grandi quantità di dati e garantire un livello più elevato di protezione. Gli algoritmi di *machine learning* applicati alla sicurezza sono oggi in grado di rilevare anomalie nei sistemi informativi, prevedere possibili attacchi e

[118] Ginevra Cerrina Feroni, *Intelligenza artificiale e ruolo della protezione dei dati personali*, Garante per la protezione dei dati personali (14 febbraio 2023), https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9855742.

automatizzare alcuni processi di risposta agli incidenti, contribuendo così a migliorare la resilienza aziendale.

Tuttavia, l'adozione di sistemi di IA non comporta soltanto vantaggi. Come ogni tecnologia avanzata, essa introduce nuovi margini di rischio, sia sotto il profilo della sicurezza sia sotto quello della protezione dei dati personali. L'utilizzo di algoritmi poco chiari, l'accumulo di enormi quantità di dati per l'addestramento dei modelli, la possibilità di bias decisionali e l'automazione di attività delicate possono generare impatti rilevanti sui diritti degli interessati e sulle responsabilità giuridiche delle organizzazioni.

L'intelligenza artificiale può diventare essa stessa una fonte di vulnerabilità. Un esempio è il *data poisoning,* cioè un attacco in cui i dati utilizzati per addestrare un sistema di IA vengono manipolati inserendo informazioni false o sbagliate. Poiché l'IA basa il proprio funzionamento sull'apprendimento da questi dati, finirà per sviluppare modelli alterati, prendere decisioni errate o generare risultati non affidabili. Allo stesso modo, la manipolazione degli algoritmi o lo sfruttamento delle loro debolezze può compromettere i processi decisionali e mettere a rischio l'integrità delle informazioni.

Nel contesto regolatorio delineato dal GDPR, l'adozione dell'IA richiede dunque un approccio attento e responsabile. Il Regolamento, pur non menzionando espressamente l'IA, impone obblighi che incidono direttamente sul suo utilizzo. Principi come minimizzazione dei dati, trasparenza, *accountability e privacy by design* rappresentano il quadro entro il quale le tecnologie intelligenti devono essere progettate e applicate. Anche le valutazioni d'impatto (DPIA), introdotte nel secondo capitolo, assumono un ruolo cruciale, poiché consentono di identificare i rischi elevati derivanti da sistemi automatizzati e di implementare misure di sicurezza adeguate prima dell'avvio del trattamento.

L'obiettivo di questo capitolo sarà quindi analizzare il ruolo dell'IA come un punto di forza per migliorare la protezione dei dati in azienda, evidenziando i principali benefici che può apportare in termini di prevenzione, rilevazione e risposta agli incidenti di Cybersecurity. Allo stesso tempo, verranno approfonditi i rischi derivanti da un uso non controllato o non conforme delle tecnologie intelligenti, ponendo attenzione agli aspetti etici e giuridici già introdotti nei capitoli precedenti. Saranno inoltre esaminate le politiche e le strategie che le imprese possono adottare per integrare l'IA in maniera sicura, trasparente e rispettosa dei diritti delle persone, trasformando questa tecnologia

non in un fattore di vulnerabilità, ma in un punto di forza di protezione e innovazione responsabile.

3.1 IA, trasparenza e protezione dei dati aziendali

L'impiego di sistemi di intelligenza artificiale all'interno dell'ecosistema aziendale odierno è sempre più diffuso, tanto nei processi produttivi quanto in quelli decisionali e questo determina una crescente esigenza di tutela giuridica di queste tecnologie sotto il profilo della proprietà intellettuale. Sebbene la forma di protezione che risulta preferibile o quantomeno la più adatta in molti casi sia quella del segreto commerciale, emerge la necessità di valutare con attenzione il rapporto tra tale tutela e gli obblighi di trasparenza previsti al fine di garantire diritti fondamentali della persona e della collettività. In questo contributo si propone di analizzare il bilanciamento tra il diritto dell'impresa a mantenere segrete le tecnologie di IA utilizzate nella propria attività e, dall'altro lato, le esigenze di trasparenza e comprensibilità relative ai sistemi stessi.

Oggi appare pacifico che i sistemi di IA, nelle loro molteplici forme e funzionalità, costituiscano spesso una componente fondamentale dell'assetto aziendale moderno. Il ricorso a queste tecnologie in ambito industriale e imprenditoriale è considerato determinante non solo per acquisire o mantenere un vantaggio competitivo (anche in chiave concorrenziale), ma semplicemente per aumentare l'efficienza operativa dell'impresa. L'uso dell'IA è infatti interdisciplinare, in quanto può manifestarsi attraverso l'adozione di sistemi automatizzati finalizzati a migliorare e velocizzare le interazioni con i clienti (anche nei servizi di assistenza), elaborare dati plurimi per facilitare attività analitiche, può essere utilizzata anche in ambito diagnostico o di ricerca, in procedure nella pubblica amministrazione, fino alla robotica industriale integrata con componenti intelligenti. Anche il settore finanziario non è rimasto estraneo. Alcune istituzioni hanno integrato sistemi di IA per finalità quali verifica e analisi dei rischi, rilevamento delle frodi e analisi dati utili a decisioni rapide.

La diffusione di queste tecnologie richiede che lo sviluppo di nuove soluzioni sia accompagnato da strumenti di tutela giuridica, specie in ambito societario. Il patrimonio immateriale di un'impresa, costituito frequentemente da *know-how*, cioè competenze tecniche, esperienze e procedure che permettono di svolgere un'attività in modo efficace,

rappresenta un elemento cruciale per la competitività e l'efficienza. Pertanto, le tecnologie che includono sistemi di IA possono essere considerate conoscenze riservate dell'impresa e configurarsi, da sole o integrate nell'insieme delle informazioni aziendali, come un asset tutelabile mediante segreto commerciale. Le strategie e le metodologie adottate nella produzione o nella gestione sono il risultato di investimenti significativi, che possono riguardare ricerca, sviluppo o acquisizione da fornitori esterni che meritano protezione giuridica[119]. La certezza offerta da tale tutela legale costituisce un incentivo per chi investe in tali attività.

La scelta dello strumento di protezione più adeguato che sia diritto d'autore, brevetto o segreto commerciale, dipende dalle caratteristiche dell'asset da tutelare. Nel caso delle tecnologie di IA, queste sono soggette a continui aggiornamenti e miglioramenti; pertanto, una protezione brevettuale con una durata ventennale potrebbe risultare non perfettamente adatta. Inoltre, la tutela mediante segreto commerciale comporta costi economici che consistono principalmente nel mantenimento di misure di sicurezza per garantire la riservatezza, senza richiedere spese iniziali per la costituzione di un diritto. In definitiva, la decisione di un sistema di tutela dipende specificamente dal tipo di bene da proteggere. Da ricordare però che non tutte le tecnologie sono brevettabili. Il software "in quanto tale" non rientra tra quelle brevettabili né secondo il Codice di proprietà industriale né secondo la Convenzione europea sul brevetto.

Tuttavia, la protezione come segreto commerciale non può estendersi a qualunque informazione. La normativa richiede che le informazioni siano effettivamente segrete (non conosciute o facilmente reperibili), che abbiano valore economico proprio in quanto segrete e che siano protette da misure ragionevoli di sicurezza. Questi criteri sono stati stabiliti dalla Direttiva (UE) 2016/943 (nota come "*Trade Secrets Directive*") e recepiti dal Codice della proprietà industriale (art. 98), si adattano di per sé alla tutela di algoritmi complessi e codici sorgente. La complessità intrinseca dei sistemi di IA è dovuta alla programmazione, alla scelta e validazione dei dati di addestramento, e all'intervento umano che rende peraltro molto improbabile l'ipotesi di scoperta indipendente o di *reverse engineering* da parte di terzi. In questo senso, la segretezza rappresenta uno strumento efficace di protezione, offre una tutela potenzialmente illimitata nel tempo e

[119] Licia Garotti e Giulia Di Biase, Intelligenza artificiale, trasparenza e tutela dei dati aziendali, in Lavoro Diritti Europa, pubblicato il 20 novembre 2024.

immediatamente operativa, compatibile con eventuali modifiche o aggiornamenti del sistema, a patto che l'impresa mantenga misure di sicurezza adeguate.

Al tempo stesso, va riconosciuto che quando un bene tutelato comprende sistemi di IA, emerge l'esigenza di garantire la riservatezza dei processi e delle decisioni che generano l'output. Questa necessità suscita perplessità, poiché la presenza di un controllo umano non annulla la natura "artificiale" della decisione. Con l'adozione del *Artificial Intelligence Act* (AI Act), approvato dal Consiglio dell'UE nel 2024, viene prevista la supervisione umana del funzionamento dei sistemi di IA. Tuttavia, tale supervisione resta parte integrante del sistema e non elimina l'autonomia decisionale dell'IA. In tal modo, da un lato, l'accesso alla tutela del segreto commerciale richiede che le informazioni restino non accessibili; dall'altro, emerge l'esigenza di garantire l'intelligibilità dell'output, dei meccanismi decisionali e dei dati che hanno alimentato il processo (dati di addestramento)[120].

La richiesta di trasparenza rispetto alle decisioni algoritmiche non è solo un'esigenza normativa, nasce anche da un sentimento umano di sfiducia e diffidenza verso processi percepiti come non trasparenti o incontrollabili. Tale percezione è del tutto comprensibile se si considera che le decisioni generate da sistemi di IA possono incidere su un'ampia gamma di interessi e diritti, da considerazioni interne all'impresa su concorrenza e strategia, fino a impatti su consumatori, cittadini, ambiente e diritti fondamentali.

La possibilità di comprendere la logica di un sistema di IA e il processo che porta a un determinato output è preziosa per individuare eventuali bias, discriminazioni o decisioni lesive dei diritti.

Proprio questa esigenza di chiarezza è stata incorporata dal legislatore europeo nella filosofia dell'IA "affidabile" *(so-called Trustworthy AI*), richiamata nell'AI Act. Molto prima dell'adozione del Regolamento, principi etici formulati *dall'High-Level Expert Group on AI* (HLEG), un gruppo di esperti sull'AI[121]. In particolare, nel documento *Ethics Guidelines for Trustworthy AI*, avevano già evidenziato l'importanza di elementi come la supervisione umana, la robustezza tecnica e la sicurezza, ma anche la trasparenza. Al pari, i principi del OECD (Organizzazione per la Cooperazione e lo Sviluppo

[120] Ibidem.

[121] High-Level Expert Group on Artificial Intelligence (AI HLEG), *Ethics Guidelines for Trustworthy AI*, European Commission, 8 Aprile 2019. Documento che presenta i principi etici dell'IA "affidabile" elaborati dal gruppo di esperti istituito dalla Commissione europea.

Economico) in materia di intelligenza artificiale sottolineano trasparenza e accuratezza dei sistemi, intesi come necessità di rendere accessibili in modo semplice e comprensibile le fonti di dati e i processi che portano a un dato risultato.

Tuttavia, non sempre è realisticamente possibile garantire una comprensione totale, soprattutto in presenza di sistemi complessi, i cosiddetti *"black-box"*, per i quali la trasparenza deve essere graduata in funzione del livello di rischio e delle possibili conseguenze dannose. L'AI Act sembra in effetti contemplare questa tensione. Da un lato, promuove la trasparenza e chiarezza dei sistemi; dall'altro, riconosce la legittimità della protezione della proprietà intellettuale e dei segreti commerciali (inclusi codici sorgente e *know-how*). In particolare, l'obbligo di garantire trasparenza non si traduce necessariamente in una divulgazione tecnica dettagliata, ma può consistere in una sintesi pubblica sufficientemente generica delle informazioni utili, così da proteggere gli interessi concorrenti delle imprese senza compromettere i diritti fondamentali[122].

Pertanto, l'apparente contrasto tra il diritto alla segretezza e la necessità di trasparenza non riguarda in realtà la legittimità degli interessi in gioco, entrambi meritevoli di tutela, bensì le modalità con cui tali interessi devono essere soddisfatti. La finalità del segreto commerciale non è creare un monopolio dell'informazione fine a sé stesso, ma tutelare gli investimenti sostenuti dall'impresa per sviluppare tecnologie complesse, incentivando l'innovazione. Dall'altro lato, gli obblighi di trasparenza intendono prevenire e correggere eventuali effetti discriminatori, decisioni ingiuste, bias o violazioni dei diritti fondamentali. La soluzione più coerente consiste dunque nell'individuare misure che consentano di proteggere entrambi gli interessi, calibrando la trasparenza sulle circostanze concrete, sul livello di rischio, sul settore di applicazione, sulla rilevanza delle decisioni rispetto ai diritti delle persone.

Un approccio flessibile, che valuta caso per caso l'equilibrio tra riservatezza e accessibilità, appare il più adatto. Quando l'output di un sistema di IA può avere effetti rilevanti sui diritti dei soggetti coinvolti, con possibili conseguenze discriminatorie o lesive, dovrebbe prevalere l'esigenza di trasparenza, anche se rivolta esclusivamente alle autorità competenti o soggetti istituzionali. Al contrario, nei casi in cui l'impatto è modesto e non rileva un interesse pubblico diretto, può essere giustificata una preferenza per la riservatezza del *know-how*. La decisione su quale interesse privilegiare deve

[122] Ibidem.

fondarsi su una valutazione attenta rispetto alla natura della tecnologia, al contesto di impiego, al livello di rischio e alla prossimità della decisione ai diritti delle persone.

3.2 Il ruolo dell'intelligenza Artificiale in azienda

L'impiego dell'intelligenza artificiale nei contesti aziendali si colloca oggi in una fase di consolidamento, in cui i sistemi automatizzati non svolgono più un ruolo meramente sperimentale, ma incidono in modo diretto sui processi operativi, decisionali e di gestione dei dati. In tale scenario, il ruolo dell'IA non può essere valutato esclusivamente in termini di efficienza o di capacità predittiva, ma deve essere analizzato alla luce delle criticità tecniche e operative che emergono dalla sua integrazione in infrastrutture informatiche complesse e dinamiche. L'adozione di sistemi di intelligenza artificiale, infatti, introduce nuove superfici di rischio che si affiancano – e in alcuni casi si sovrappongono – a quelle già presenti nei tradizionali sistemi informativi aziendali.
Uno dei principali fattori di criticità riguarda la dipendenza strutturale dei sistemi di IA dai dati. A differenza delle applicazioni informatiche tradizionali, i modelli di *machine learning* non operano sulla base di regole predeterminate, ma costruiscono le proprie inferenze a partire da grandi quantità di dati storici. Ciò comporta che eventuali errori, distorsioni o lacune presenti nei *dataset* utilizzati in fase di addestramento possano riflettersi in modo sistematico sul comportamento del sistema. In ambito aziendale, questa dipendenza può tradursi in decisioni imprecise o non coerenti con il contesto operativo attuale, soprattutto nei casi in cui i dati non siano aggiornati o non rappresentativi delle reali dinamiche di business[123].
Un ulteriore profilo di rischio è connesso alla vulnerabilità dei modelli di intelligenza artificiale rispetto a forme di manipolazione intenzionale o accidentale. I sistemi di IA possono essere esposti a interventi che alterano il loro funzionamento senza compromettere direttamente l'infrastruttura informatica sottostante. La modifica dei dati di *input*, l'introduzione di informazioni fuorvianti o l'alterazione dei parametri del modello, possono incidere in modo significativo sugli output generati, rendendo difficile individuare tempestivamente la causa di eventuali anomalie. In contesti aziendali

[123] Cfr. G. Finocchiaro, La protezione dei dati personali in Italia. Regolamento UE 2016/679 e d.lgs. 101/2018, Zanichelli, 2019, pp. 45-67.

caratterizzati da un'elevata automazione dei processi, tali vulnerabilità possono avere effetti amplificati, incidendo su una pluralità di attività e di trattamenti di dati.

La complessità tecnica dei sistemi di intelligenza artificiale rappresenta un'ulteriore fonte di criticità. I modelli avanzati, in particolare quelli basati su modelli informatici, risultano spesso difficilmente interpretabili anche per gli stessi soggetti che li hanno progettati o implementati. Questa opacità tecnica non si traduce soltanto in una difficoltà di comprensione teorica del funzionamento dell'algoritmo, ma incide concretamente sulla capacità dell'impresa di monitorare il sistema, individuare errori e valutare l'affidabilità delle decisioni automatizzate. In assenza di strumenti di monitoraggio adeguati, il rischio è quello di affidarsi a sistemi il cui comportamento risulta sostanzialmente non verificabile.

L'integrazione dell'intelligenza artificiale nei sistemi informativi aziendali solleva inoltre problemi legati alla continuità operativa e alla gestione del cambiamento. I modelli di IA non sono statici, ma possono degradarsi nel tempo a causa del mutamento dei dati di input e del contesto operativo in cui sono inseriti. Questo fenomeno, spesso poco considerato nelle fasi iniziali di realizzazione, comporta la necessità di aggiornamenti costanti, riaddestramento dei modelli e verifiche periodiche delle prestazioni. La mancata gestione di tali aspetti può portare a un progressivo scollamento tra il comportamento del sistema e le esigenze aziendali, con conseguenti rischi sul piano della qualità delle decisioni e della protezione dei dati trattati.

Dal punto di vista operativo, l'adozione dell'intelligenza artificiale richiede inoltre un ripensamento delle modalità di gestione degli incidenti e delle anomalie. Nei sistemi tradizionali, gli errori possono essere ricondotti a malfunzionamenti specifici o a violazioni puntuali delle regole di sistema. Nei sistemi di IA, invece, le anomalie possono emergere in modo graduale e non immediatamente riconducibile a una causa unica. Questa caratteristica rende più complessa l'individuazione di responsabilità operative e richiede l'adozione di procedure di tracciamento continuo, capaci di intercettare deviazioni significative nel comportamento del sistema prima che producano effetti rilevanti.

Il ruolo dell'intelligenza artificiale in azienda deve essere valutato anche in relazione alla sua capacità di interagire con altri sistemi automatizzati e con le infrastrutture di sicurezza esistenti. L'IA non opera in isolamento, ma si inserisce in un ecosistema tecnologico

articolato, la cui interconnessione può comportare aumento dell'impatto di eventuali criticità. Il ruolo dell'IA non può essere ridotto a quello di semplice strumento di supporto, ma deve essere considerato come un elemento centrale dell'architettura tecnologica aziendale, la cui gestione richiede competenze specifiche e un approccio consapevole ai rischi.

Dalle analisi emerge come il ruolo dell'intelligenza artificiale in azienda non possa essere compreso senza una valutazione approfondita delle criticità tecniche e operative che ne caratterizzano l'impiego. L'IA rappresenta una risorsa strategica, ma al tempo stesso introduce nuove forme di vulnerabilità che, se non adeguatamente governate, possono incidere sulla sicurezza dei dati, sull'affidabilità dei processi e sulla capacità dell'impresa di esercitare un controllo effettivo sulle proprie attività. La gestione di tali rischi costituisce, pertanto, una condizione imprescindibile per un utilizzo responsabile dell'intelligenza artificiale in ambito aziendale.

3.3 Criticità organizzative e rischi di governance nell'adozione dell'intelligenza artificiale

L'introduzione dell'intelligenza artificiale nei contesti aziendali non incide esclusivamente sulle modalità operative e sull'efficienza dei processi, ma produce effetti rilevanti sull'organizzazione del lavoro, sulle strutture decisionali e sui meccanismi di responsabilità interna. In questo senso, l'IA rappresenta un fattore di trasformazione che, se non adeguatamente governato, può generare criticità sistemiche difficilmente riconducibili a singoli errori tecnici. Il rischio principale non risiede tanto nell'adozione della tecnologia in sé, quanto nella tendenza a integrarla all'interno di modelli organizzativi che non sono stati progettati per gestire processi decisionali automatizzati complessi[124].

Uno dei profili più delicati riguarda il progressivo spostamento del potere decisionale dai soggetti umani ai sistemi algoritmici. In molte realtà aziendali, l'IA viene impiegata come mezzo di supporto alle decisioni, ma nella pratica finisce per orientare in modo determinante le scelte operative e strategiche. Tale fenomeno, spesso definito come

[124] L. Diaferia, L. M. De Rossi, and G. Salviotti, *AI Management: Strategie e approcci in azienda*, Milano, Egea, 2024, cap. dedicato alla *governance* e alle sfide organizzative.

automation bias, porta gli operatori a fare affidamento sulle decisioni suggerite dal sistema, riducendo la capacità critica e accertamento umano effettivo. Ne deriva una forma di delega implicita che può compromettere la responsabilità individuale e collettiva, soprattutto nei casi in cui le decisioni automatizzate incidano su dati personali o su diritti degli interessati.

Un ulteriore elemento di criticità è rappresentato dalla frammentazione delle responsabilità all'interno dell'organizzazione aziendale. L'adozione di sistemi di intelligenza artificiale coinvolge una pluralità di attori: sviluppatori, fornitori esterni, responsabili IT, management, DPO con competenze e ruoli differenti. In assenza di una chiara definizione delle responsabilità, il rischio è quello di creare aree grigie in cui nessun soggetto risulta pienamente responsabile delle decisioni assunte dal sistema. Questa dispersione della responsabilità rende più complesso individuare eventuali violazioni, adottare misure correttive tempestive e garantire un'effettiva *accountability*, come richiesto dal quadro normativo europeo.

La trasformazione organizzativa indotta dall'IA incide anche sulle competenze richieste al personale. L'utilizzo di sistemi automatizzati avanzati presuppone la presenza di figure professionali in grado di comprendere, monitorare e valutare il funzionamento degli algoritmi. Tuttavia, molte imprese adottano soluzioni di intelligenza artificiale senza investire in modo adeguato nella formazione del personale, generando una dipendenza tecnologica che riduce la capacità dell'organizzazione di intervenire in caso di anomalie o malfunzionamenti. Questo squilibrio tra sofisticazione tecnologica e competenze umane può tradursi in un aumento del rischio operativo e in una ridotta capacità di garantire la conformità ai principi di protezione dei dati.

Sul piano dei processi aziendali, l'integrazione dell'IA può determinare una standardizzazione eccessiva delle decisioni, con il rischio di trascurare le specificità dei singoli casi. L'automazione dei flussi decisionali, se non accompagnata da adeguati meccanismi di supervisione, può portare a una gestione rigida dei dati e delle informazioni, limitando la possibilità di intervento umano nei casi atipici o complessi. In ambito di protezione dei dati, tale rigidità può risultare particolarmente problematica, poiché i trattamenti automatizzati richiedono spesso valutazioni contestuali che difficilmente possono essere completamente codificate in un algoritmo.

Un'ulteriore criticità organizzativa riguarda la cultura aziendale e l'approccio alla *compliance*. In alcune realtà, l'intelligenza artificiale viene percepita come uno strumento neutro e oggettivo, capace di eliminare errori e discrezionalità umana. Questa visione rischia di oscurare il fatto che i sistemi di IA riflettono le scelte progettuali, i dati e gli obiettivi definiti dall'organizzazione. La mancata consapevolezza di tale aspetto può portare a una sottovalutazione dei rischi e a un approccio meramente formale agli obblighi di protezione dei dati, in contrasto con l'impostazione sostanziale richiesta dal *principio di accountability*.

L'adozione dell'intelligenza artificiale solleva interrogativi rilevanti in merito alla capacità delle strutture aziendali di adattarsi nel tempo all'evoluzione dei sistemi. I modelli organizzativi tradizionali, basati su processi statici e gerarchie definite, risultano spesso inadeguati a gestire tecnologie che apprendono, si modificano e richiedono un esame continuo. In questa situazione, il rischio non è solo quello di inefficienze operative, ma anche di una progressiva perdita di controllo sui processi decisionali automatizzati, con potenziali ripercussioni sulla tutela dei dati e sulla legittimità complessiva delle attività aziendali.

Alla luce di tali considerazioni, emerge la necessità di affiancare all'adozione dell'intelligenza artificiale un ripensamento profondo dell'organizzazione del lavoro e dei modelli di *governance* aziendale. La gestione dei rischi connessi all'IA non può essere affidata esclusivamente a soluzioni tecnologiche, ma richiede strutture organizzative flessibili, competenze adeguate e una chiara attribuzione delle responsabilità, al fine di garantire che l'innovazione si sviluppi in modo coerente con i principi di protezione dei dati e con i diritti fondamentali degli interessati.

3.4 I principi fondamentali della protezione dei dati e la loro applicazione ai sistemi di intelligenza artificiale

L'applicazione dei principi fondamentali della protezione dei dati personali ai sistemi di intelligenza artificiale rappresenta una delle sfide più complesse del diritto della privacy contemporaneo. Sebbene il Regolamento (UE) 2016/679 sia stato concepito come un sistema tecnologicamente neutro, la crescente diffusione di sistemi di IA evidenzia una serie di tensioni strutturali tra l'impianto concettuale del GDPR e le caratteristiche

operative dei trattamenti automatizzati avanzati. Tali tensioni non mettono in discussione la validità dei principi, ma ne rivelano i limiti applicativi, soprattutto in contesti aziendali caratterizzati da elevata complessità tecnologica e organizzativa.

Uno dei principali profili critici riguarda il principio di trasparenza. Nei sistemi di intelligenza artificiale, la trasparenza non si esaurisce nella mera informativa all'interessato, ma implica la possibilità di comprendere, almeno in termini generali, le logiche sottese al trattamento e alle decisioni automatizzate. Tuttavia, nella pratica aziendale, la traduzione di tale principio in obblighi concreti risulta problematica. Da un lato, la complessità tecnica degli algoritmi limita la capacità di fornire spiegazioni realmente intelligibili; dall'altro, la necessità di tutelare il segreto commerciale e le conoscenze riservate dell'azienda riduce ulteriormente lo spazio per una comunicazione effettiva. Ne deriva una trasparenza spesso formale, che rischia di svuotare il principio della sua funzione sostanziale di garanzia per l'interessato[125].

Analoga criticità emerge in relazione al principio di limitazione della finalità. I sistemi di IA, soprattutto quelli basati su apprendimento automatico, sono spesso progettati per essere riutilizzati in contesti differenti e per trarre valore dall'analisi incrociata di grandi volumi di dati. In ambito aziendale, questa caratteristica può entrare in conflitto con l'esigenza di determinare finalità specifiche, esplicite e legittime sin dalla fase iniziale del trattamento. Il rischio è quello di una progressiva estensione delle finalità originarie, giustificata da esigenze di efficienza o innovazione, ma non sempre accompagnata da una rivalutazione giuridica della liceità del trattamento.

Il principio di minimizzazione dei dati pone ulteriori problemi applicativi. L'efficacia dei sistemi di intelligenza artificiale è spesso correlata alla disponibilità di grandi quantità di dati, inclusi dati storici. In tale contesto, la selezione preventiva dei dati strettamente necessari può risultare complessa, se non addirittura incompatibile con le logiche di funzionamento di alcuni modelli. Le imprese si trovano così a dover bilanciare esigenze tecniche e obblighi giuridici, con il rischio di adottare soluzioni che privilegiano l'efficienza algoritmica a scapito della minimizzazione, esponendosi a potenziali profili di non conformità.

Particolarmente delicata è la questione dell'*accountability*. Il GDPR impone al titolare del trattamento non solo di rispettare i principi di protezione dei dati, ma anche di essere

[125] Machine, Platform, Crowd: Harnessing Our Digital Future.Brynjolfsson, E., & McAfee, A. (2017).

in grado di dimostrarne l'effettiva applicazione. Nei sistemi di IA, tale obbligo si confronta con la difficoltà di ricostruire e documentare processi decisionali automatizzati complessi, che possono evolvere nel tempo. In ambito aziendale, l'*accountability* rischia di tradursi in un adempimento prevalentemente documentale, fondato su policy e procedure standardizzate, senza che vi sia una reale capacità di controllo sul funzionamento concreto dei sistemi utilizzati.

Ulteriori criticità emergono con riferimento al principio di esattezza e alla gestione degli errori. Nei trattamenti tradizionali, l'inesattezza dei dati può essere individuata e corretta mediante interventi puntuali. Nei sistemi di intelligenza artificiale, invece, l'errore può essere sistemico e derivare dal modello stesso, piuttosto che dal singolo dato. Ciò solleva interrogativi rilevanti in merito all'effettività del diritto di rettifica e alla possibilità per l'interessato di incidere su trattamenti automatizzati che producono effetti giuridici o significativamente analoghi.

Anche il principio di limitazione della conservazione incontra ostacoli applicativi. I sistemi di IA possono richiedere l'archiviazione prolungata dei dati per finalità di riaddestramento, verifica delle prestazioni o audit interni. In tali casi, la determinazione di un periodo di conservazione adeguato risulta complessa e spesso rimessa a valutazioni discrezionali dell'impresa, con il rischio di una conservazione eccessiva non sempre giustificata da esigenze giuridicamente rilevanti.

Nel contesto dei sistemi di intelligenza artificiale, i limiti applicativi dei principi del GDPR evidenziano come la conformità normativa non possa essere raggiunta attraverso un approccio meramente formale. L'adozione di modelli di IA richiede una valutazione sostanziale dei rischi per i diritti e le libertà degli interessati, nonché una capacità di adattare i principi di protezione dei dati alle specificità dei trattamenti automatizzati. In questo senso, il GDPR offre un quadro di riferimento imprescindibile, ma non sempre sufficiente a risolvere le criticità che emergono nella pratica aziendale[126].

Alla luce di tali considerazioni, appare evidente come l'applicazione dei principi fondamentali della protezione dei dati ai sistemi di intelligenza artificiale ponga problemi interpretativi e operativi che richiedono un'evoluzione delle prassi aziendali e un rafforzamento degli strumenti di *governance*. Il rispetto dei principi del GDPR, nell'era

[126] The EU General Data Protection Regulation (GDPR): A Commentary. Oxford University Press.Kuner, C., Bygrave, L., & Docksey, C. (2020).

dell'IA, non può limitarsi a un adempimento statico, ma deve tradursi in un processo continuo di valutazione, supervisione e adattamento, capace di tenere conto della natura dinamica e complessa dei sistemi automatizzati.

3.5 L'intelligenza artificiale come strumento di conformità giuridica e gestione dei rischi

Pur emergendo criticità interpretative ed operative nell'applicazione dei principi fondamentali della protezione dei dati ai sistemi di intelligenza artificiale, è fondamentale affiancare all'analisi delle tensioni anche un approfondimento sulle modalità con cui l'IA può concretamente supportare il rispetto della disciplina della protezione dei dati. In particolare, nella modernizzazione dei processi aziendali, le tecnologie intelligenti non devono essere viste unicamente come fattori di rischio da governare, ma come strumenti abilitanti per una compliance normativa più efficace, dinamica e integrata nelle strutture organizzative.

L'adozione di sistemi di IA può, in primo luogo, favorire un monitoraggio continuo dei flussi di dati personali, facilitando la rilevazione di anomalie, incongruenze o processi non conformi alle policy interne e ai requisiti del GDPR. Algoritmi di *machine learning* e tecniche di *natural language processing* possono essere impiegati per automatizzare la verifica dei contenuti documentali e il controllo di coerenza rispetto agli standard normativi, alleggerendo l'onere delle attività manuali e riducendo il margine di errore umano, particolarmente critico in contesti con grandi volumi di informazioni sensibili. Un esempio di questo approccio è stato sviluppato in ambito pubblico da Basile e altri, che propongono framework di IA per supportare le decisioni in materia di conformità GDPR verificando testi e documenti secondo criteri normativi predefiniti [127].

Un'altra funzione abilitante dell'intelligenza artificiale riguarda la documentazione e la tracciabilità dei processi decisionali automatizzati. Instrumenti di log intelligenti e sistemi di audit basati su IA consentono di mantenere registri automatici e dettagliati delle attività di trattamento, generando report strutturati che facilitano il rispetto del principio di accountability. In questo modo, l'organizzazione non solo rispetta gli obblighi di

[127] Lorè F., Basile P., Appice A., de Gemmis M., Malerba D., Semeraro G., *An AI framework to support decisions on GDPR compliance*, *Journal of Intelligent Information Systems* 61 (2023), pp. 541-568.

trasparenza nei confronti delle autorità di controllo, ma può anche dimostrare in maniera verificabile l'applicazione pratica delle misure di protezione adottate, facilitando verifiche interne ed esterne senza appesantire i processi amministrativi.

Dal punto di vista operativo, l'IA può supportare la gestione delle richieste degli interessati (accesso, rettifica, cancellazione, portabilità), automatizzando la raccolta, la classificazione e la risposta alle istanze degli utenti. Strumenti di intelligenza conversazionale e *chatbot* basati su modelli linguistici avanzati possono guidare gli utenti nella compilazione e nell'esercizio dei diritti, riducendo i tempi di risposta e aumentando la qualità delle interazioni senza gravare sulle risorse interne dell'organizzazione.

Inoltre, l'intelligenza artificiale può contribuire a ottimizzare la *governance* dei dati a livello strategico. Attraverso tecniche predittive e analitiche, le imprese possono identificare pattern di rischio, stimare l'impatto di nuove iniziative sui diritti degli interessati e adattare procedure interne in tempo reale. Queste capacità permettono di affinare le valutazioni d'impatto (DPIA) e di integrare criteri di *privacy by design* e *by default* nei sistemi interconnessi, come suggerito da esperti di gestione dell'IA in azienda, che invocano un approccio integrato tra tecnologia, business process e controllo organizzativo.

Infine, la trasformazione delle attività di compliance in processi dinamici, proattivi e basati su evidenze può rafforzare la cultura aziendale della protezione dei dati, spostandola da una visione puramente formale a una dimensione operativa e strategica. L'IA, integrata in un quadro di *governance* solido, non sostituisce il giudizio umano ma lo potenzia, fornendo strumenti analitici avanzati, capacità di previsione dei rischi e supporto decisionale continuo. Ciò consente alle organizzazioni di non limitarsi a reagire alle violazioni normative, ma di anticipare criticità, pianificare interventi mirati e consolidare fiducia e trasparenza nei rapporti con gli stakeholder e le autorità di controllo.

In conclusione, le potenzialità dell'intelligenza artificiale si estendono ben oltre il mero automatismo: esse abilitano modalità di compliance più efficaci, resilienti e integrate con la *governance* aziendale, creando un percorso di tutela dei dati personali che è tanto normativo quanto operativo. Questo orientamento non solo valorizza il contributo dell'IA al rispetto del GDPR, ma costituisce un elemento strategico per l'evoluzione dell'organizzazione complessiva di impresa in chiave digitale e responsabile.

3.6 IA e la creazione di valore in azienda

Osservando i risultati ottenuti dai principali protagonisti del settore tecnologico e dalle startup che negli ultimi anni hanno sviluppato soluzioni innovative basate sull'intelligenza artificiale, si potrebbe essere portati a pensare che per trarre vantaggio dall'IA sia necessaria una trasformazione radicale dell'intera organizzazione. In realtà, anche interventi mirati, se supportati da una strategia chiara di *governance* dei dati e da un'adeguata integrazione dei principi di protezione delle informazioni, possono generare valore significativo. L'IA non deve essere considerata una tecnologia da applicare senza criterio, ma uno strumento da inserire in un percorso di crescita coerente, progressivo e rispettoso della normativa.

L'esperienza della trasformazione digitale degli ultimi anni lo dimostra chiaramente. Inizialmente si riteneva che solo programmi profondi e radicali potessero portare benefici concreti. Successivamente, è emerso che approcci più graduali, ma pensati in un modo integrato dall'inizio alla fine, potevano risultare altrettanto efficaci. Nel caso dell'IA, questa logica richiede che ogni iniziativa sia progettata con attenzione alla circolazione dei dati, ai rischi derivanti dai trattamenti automatizzati e alla necessità di assicurare trasparenza, sicurezza e rispetto del principio di minimizzazione[128].

Le applicazioni dell'IA in azienda seguono principalmente due logiche: da un lato, la possibilità di integrare nuove funzionalità in prodotti e servizi, dall'altro, l'evoluzione o l'introduzione di processi interni basati su capacità predittive o decisionali avanzate. Entrambe le logiche, tuttavia, si fondano sull'uso intensivo di dati, che devono essere raccolti, conservati, elaborati e protetti secondo criteri rigorosi. Nuovi prodotti basati su IA, come assistenti intelligenti, algoritmi di previsione della domanda, strumenti di analisi comportamentale o sistemi di rilevamento delle frodi, richiedono basi dati ampie e diversificate. È quindi fondamentale integrare meccanismi di *privacy by design*, prevedendo anonimizzazione, pseudonimizzazione e controlli costanti sul ciclo di vita dei dati.

La creazione di valore attraverso i processi interni è altrettanto rilevante. L'IA può migliorare la pianificazione, ottimizzare la logistica, ridurre i costi operativi e identificare

[128] L. Diaferia, L. M. De Rossi, and G. Salviotti, *AI Management: Strategie e approcci in azienda*, Milano, Egea, 2024, pp. 39-40.

inefficienze. Tuttavia, questi benefici possono essere ottenuti solo se il sistema è affidabile, accurato e costantemente monitorato. Ciò implica la definizione di procedure di audit dei modelli, la tracciabilità delle decisioni automatizzate, valutazioni dell'impatto sui diritti degli interessati e verifiche periodiche sulla qualità dei dati utilizzati. In assenza di tali misure, il rischio è quello di introdurre sistemi che generano errori, violano la privacy o si deteriorano nel tempo.

L'IA può essere impiegata anche per analisi più improvvisate, mirate a risolvere problemi specifici o a esplorare scenari di mercato. Anche in questo caso la protezione dei dati deve essere parte integrante della progettazione. Il trattamento dei dati deve essere limitato alla finalità individuata e devono essere adottate misure per evitare che informazioni identificabili vengano conservate più a lungo del necessario o utilizzate in modo incompatibile con gli scopi iniziali.

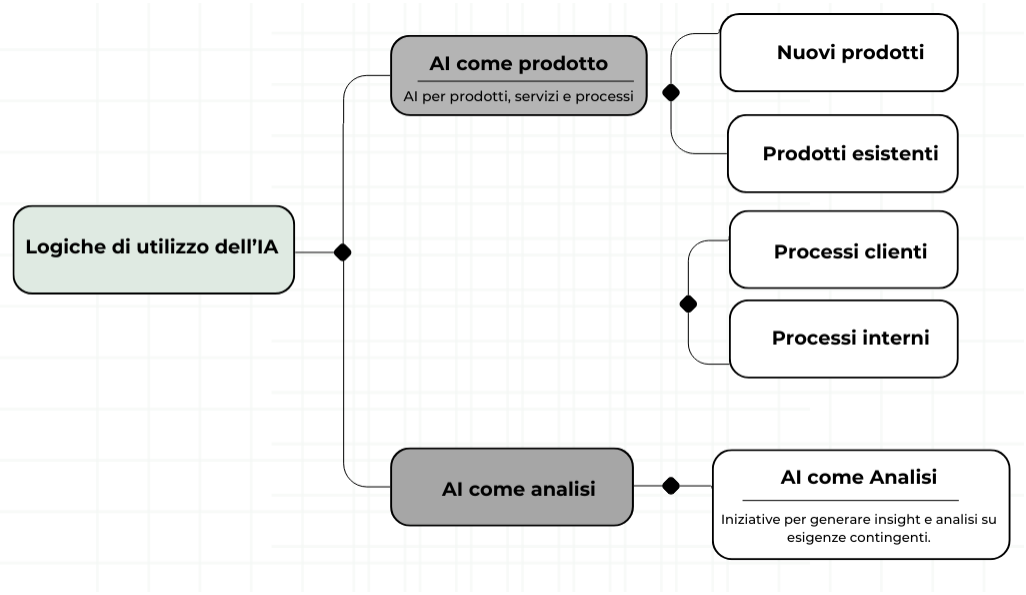

Figura 4: Rappresentazione delle modalità di impiego dell'AI all'interno dell'impresa. IA utilizzata per l'ottimizzazione dei processi interni e AI impiegata per attività analitiche mirate[129].

Un punto fondamentale per generare valore attraverso l'IA riguarda la consapevolezza che i dati rappresentano un *asset* strategico. La protezione delle informazioni, quindi, non costituisce un ostacolo, ma un elemento chiave. Un sistema di IA conforme al GDPR,

[129] L. Diaferia, L. M. De Rossi, and G. Salviotti, op. cit, p.42.

progettato con criteri di sicurezza e trasparenza, garantisce affidabilità, tutela dei diritti degli utenti e maggiore fiducia da parte dei clienti e dei partner commerciali. Ciò si traduce in un vantaggio competitivo significativo, soprattutto in contesti in cui la fiducia nel trattamento dei dati è un requisito essenziale.
L'IA può essere una risorsa determinante per la creazione di valore in azienda, ma solo se inserita in una strategia che integri innovazione, protezione dei dati e *governance* responsabile. L'obiettivo non è replicare i modelli delle grandi aziende tecnologiche, bensì adottare un approccio che consenta all'IA di potenziare prodotti, servizi e processi, garantendo al tempo stesso sicurezza, trasparenza e conformità normativa.

3.7 Il ciclo di vita dei sistemi di IA

L'introduzione di sistemi di intelligenza artificiale nelle organizzazioni richiede una gestione strutturata e continua dell'intero ciclo di vita dei modelli, che va ben oltre la semplice fase di implementazione. La complessità intrinseca degli algoritmi, la variabilità dei dati e l'interazione con processi aziendali dinamici impongono che il ciclo di vita dell'IA venga concepito come un processo ciclico, iterativo e strettamente connesso alla *governance* dei dati. Ogni fase, dalla progettazione alla messa in produzione, deve essere attentamente pianificata per garantire che le decisioni automatizzate siano affidabili, sicure e conformi ai requisiti normativi, con particolare riguardo alla protezione dei dati personali.
In questo contesto si inseriscono i *framework* dedicati alla descrizione del ciclo di vita dei progetti di intelligenza artificiale. Pur esistendo numerosi modelli proposti negli anni, molti di essi convergono su principi comuni che derivano da tradizioni consolidate del *Data mining,* cioè il processo di estrazione di informazioni utili e conoscenza da grandi quantità di dati, in cui l'obiettivo è trasformare dati grezzi in conoscenza utilizzabile per decisioni strategiche. Tra questi, il modello *CRISP-DM* (Cross Industry Standard Process for Data Mining), un modello di riferimento standard per lo sviluppo di progetti di *Data Minin*g e analisi dei dati, ha rappresentato una pietra miliare nel settore, offrendo una struttura metodologica ampia, flessibile e facilmente adattabile a differenti contesti applicativi. Sebbene sia nato negli anni Novanta, questo metodo mantiene ancora oggi

grande rilevanza, poiché fornisce una visione completa del processo di costruzione di soluzioni basate sui dati, dalla definizione del problema fino all'adozione operativa[130].
Il *CRISP-DM* si articola in sei fasi principali, concepite come elementi interdipendenti di un processo ciclico.
La prima fase riguarda la **comprensione del business**. Non si tratta solo di identificare obiettivi generali, ma di tradurre esigenze strategiche in problematiche concretamente risolvibili tramite sistemi di IA. In questa fase è fondamentale individuare le metriche operative che permettano di misurare l'efficacia del modello, definire vincoli e risorse disponibili, e mappare rischi potenziali legati a dati sensibili o flussi informativi critici. La mancanza di un'analisi accurata del contesto può compromettere la progettazione stessa del modello, generando sistemi inadatti, inefficienti o non pienamente integrabili con i processi aziendali esistenti. Il coinvolgimento di team multidisciplinari, che includano esperti di dominio, analisti di dati e responsabili della privacy, è cruciale per costruire una base decisionale solida e allineata alle necessità operative.
Segue la fase di **comprensione dei dati**, che implica non solo l'acquisizione dei dataset disponibili, ma anche una valutazione critica della loro qualità, coerenza e rappresentatività. Analizzare la completezza, la variabilità e l'eventuale presenza di bias nei dati permette di anticipare problemi che potrebbero emergere durante la modellazione. La comprensione dei dati include anche la valutazione dei limiti legali e normativi legati al loro utilizzo, alla sensibilità delle informazioni trattate e ai possibili effetti sui diritti degli interessati. In molte organizzazioni, la disponibilità di dati eterogenei e disomogenei richiede la creazione di pipeline di integrazione, in grado di armonizzare strutture e formati differenti senza compromettere la qualità complessiva del modello.
La fase di **preparazione dei dati** rappresenta un nodo operativo particolarmente complesso. La pulizia dei dataset, la gestione dei valori mancanti, l'integrazione di fonti plurime e l'ingegnerizzazione delle feature costituiscono attività che richiedono competenze tecniche elevate e un'attenta considerazione dei rischi. In questa fase emergono anche le prime decisioni relative alla sicurezza, alla tracciabilità e alla minimizzazione dei dati, che costituiscono elementi chiave per la compliance normativa e la tutela dei diritti dei soggetti coinvolti.

[130] L. Diaferia, L. M. De Rossi, and G. Salviotti, *op. cit,* pp. 71–75.

La **modellazione** rappresenta il cuore tecnico del ciclo di vita. La scelta dell'algoritmo più idoneo deve considerare non solo la capacità predittiva o descrittiva, ma anche l'interpretabilità, la robustezza e la resilienza del modello. Il processo richiede iterazioni continue: testare parametri, confrontare approcci diversi, bilanciare dataset squilibrati e adattare tecniche di preparazione dei dati per migliorare le performance. In questa fase, l'interazione con le fasi precedenti è costante. Eventuali anomalie identificate durante i test richiedono spesso un ritorno alla preparazione dei dati o alla revisione degli obiettivi di business, confermando la natura ciclica e iterativa del processo.

La fase di **valutazione** implica un'analisi approfondita delle prestazioni dei modelli, ma non solo dal punto di vista quantitativo. L'accuratezza statistica deve essere integrata con la verifica della coerenza con le regole aziendali, l'assenza di bias discriminatori e la capacità di rispettare vincoli normativi e di sicurezza. L'affidabilità del modello viene misurata anche sulla base della sua capacità di adattarsi a nuovi scenari e della robustezza rispetto a dati non previsti durante l'addestramento. Le verifiche devono essere documentate in modo completo, creando un registro che consenta di ricostruire le scelte tecniche e le motivazioni strategiche alla base del modello.

Infine, la **messa in produzione** comporta l'integrazione del sistema nell'infrastruttura aziendale e la definizione di protocolli operativi, flussi di lavoro e responsabilità. Questa fase include la definizione di strategie di indagine continua, piani di aggiornamento periodico e procedure per la gestione dei dati in evoluzione. La manutenzione predittiva dei modelli, la rilevazione di drift dei dati e l'aggiornamento dei parametri diventano elementi essenziali per garantire che il sistema mantenga performance elevate nel tempo. La messa in produzione è quindi strettamente legata alla *governance* dei dati, alla sicurezza e alla compliance, richiedendo un approccio multidisciplinare che coinvolga esperti IT, responsabili della privacy e figure manageriali.

L'intero ciclo di vita dei sistemi di IA mette in evidenza come la gestione dei dati e dei modelli non possa essere considerata un'attività isolata. Ogni fase influenza le successive e richiede una continua interazione tra aspetti tecnici, organizzativi e normativi. L'attenzione alla qualità dei dati, alla sicurezza, alla trasparenza e alla responsabilizzazione costituisce un elemento costante, poiché la solidità dell'intero processo dipende dalla capacità dell'organizzazione di monitorare, adattare e aggiornare sistemi complessi in un contesto in continua evoluzione.

3.8 L'uso dell'intelligenza artificiale nella protezione dei dati in Poste Italiane

La crescente digitalizzazione dei servizi ha trasformato il modo in cui le aziende raccolgono e trattano i dati personali. Nelle grandi realtà che operano nei settori finanziario, assicurativo e dei servizi al cittadino, le informazioni gestite non riguardano soltanto l'identità delle persone, ma includono dettagli sensibili della loro vita economica e sociale. La protezione dei dati non può più essere considerata un semplice obbligo normativo; è diventata un elemento strategico, legato alla responsabilità aziendale e alla fiducia tra impresa e utenti.

Poste Italiane rappresenta un esempio concreto di come l'intelligenza artificiale possa essere integrata nei processi aziendali per rafforzare la tutela dei dati personali. L'azienda gestisce quotidianamente informazioni relative a milioni di cittadini attraverso servizi postali, finanziari, assicurativi e digitali. La complessità e la quantità di dati trattati espongono l'organizzazione a rischi rilevanti: accessi non autorizzati, frodi finanziarie e usi impropri delle informazioni sono minacce costanti che richiedono strumenti avanzati di prevenzione[131]. In risposta a queste sfide, Poste Italiane ha inaugurato nel marzo 2023 a Roma il *Fraud Prevention Centre*, una struttura dedicata alla sicurezza delle transazioni, operativa 24 ore su 24 e composta da oltre cento specialisti in sicurezza finanziaria e cybersecurity.

Il centro utilizza tecnologie avanzate, comprese soluzioni basate su intelligenza artificiale, per monitorare e analizzare in tempo reale grandi volumi di dati. L'obiettivo principale è la prevenzione delle frodi, che non rappresentano solo un danno economico, ma anche una violazione della privacy degli individui, poiché implicano l'uso illecito di informazioni personali. I sistemi di intelligenza artificiale permettono di identificare pattern anomali e comportamenti sospetti prima che le operazioni vengano completate, aumentando l'efficacia della protezione rispetto ai metodi tradizionali.

I risultati ottenuti confermano l'impatto positivo di questa strategia. Nel solo anno 2022, il centro ha gestito oltre un milione di segnalazioni di rischio, sventando tentativi di frode per un valore complessivo di circa 50 milioni di euro. Nel settore delle carte di pagamento, l'azione preventiva ha ridotto del 50% l'incidenza degli eventi fraudolenti sui clienti, con

[131] Poste Italiane S.p.A., Bilancio di sostenibilità e relazione sulla gestione dei dati, disponibile su: https://www.posteitaliane.it

una percentuale di frodi pari allo 0,0015% sul totale delle transazioni, in netto contrasto con l'aumento del 90% registrato nello stesso periodo a livello mondiale. Nel ramo assicurativo, i primi mesi del 2023 hanno visto la gestione con successo di 6.200 casi di frode, impedendo perdite rilevanti. Questi dati evidenziano come l'IA non sia soltanto uno strumento di automazione, ma un fattore decisivo nella tutela concreta dei dati personali[132].

La portata dei dati gestiti da Poste Italiane è impressionante: circa 35 milioni di clienti, di cui oltre 20 milioni attivi tramite web e app, e 2,5 miliardi di transazioni annue per un valore complessivo di circa 200 miliardi di euro. Il 10% del mercato dei pagamenti elettronici in Italia viene gestito attraverso quasi 5 milioni di POS fisici e virtuali.

Nel quadro attuale, l'intelligenza artificiale consente di analizzare immediatamente enormi flussi di operazioni, individuando anomalie e riducendo il rischio di violazioni, senza rallentare i servizi.

Accanto alla prevenzione delle frodi, l'IA rafforza anche la sicurezza degli accessi ai sistemi informatici. Monitorando il modo in cui gli utenti interagiscono con i servizi digitali, il sistema può rilevare comportamenti anomali e intervenire tempestivamente, senza rendere l'esperienza dell'utente complessa o invasiva. Questo approccio bilancia sicurezza e usabilità, proteggendo le informazioni senza imporre controlli rigidi e fastidiosi.

Tuttavia, l'impiego dell'IA comporta anche criticità. La progettazione dei sistemi deve garantire chiarezza e comprensibilità. Se gli utenti percepiscono la tecnologia come opaca, la fiducia nei servizi rischia di diminuire. Inoltre, esiste il pericolo di dipendenza eccessiva dalla tecnologia. Se l'intervento umano venisse ridotto oltre misura, errori o distorsioni nei sistemi automatici potrebbero passare inosservati. La gestione efficace richiede quindi supervisione costante, aggiornamenti regolari e una chiara attribuzione delle responsabilità[133].

Nonostante questi limiti, l'esperienza di Poste Italiane dimostra che l'intelligenza artificiale può essere un mezzo potente per la protezione dei dati personali, aumentando la sicurezza senza compromettere la qualità dei servizi. La tecnologia, se progettata e

[132] Commissione Europea, Regolamento generale sulla protezione dei dati (GDPR), disponibile su: https://eur-lex.europa.eu/eli/reg/2016/679/oj

[133] Garante per la protezione dei dati personali, Intelligenza artificiale e protezione dei dati personali, disponibile su: https://www.garanteprivacy.it (consultato dicembre 2025).

governata con attenzione, non sostituisce le regole, ma le rafforza, contribuendo a creare un ambiente digitale affidabile e a consolidare la reputazione aziendale. L'adozione di sistemi automatizzati per la tutela dei dati diventa così un fattore strategico, capace di trasformare una necessità normativa in un'opportunità di valore per l'azienda e per gli utenti.

3.9 L'Intelligenza Artificiale come nuovo paradigma nella tutela dei dati aziendali

L'intelligenza artificiale sta ridefinendo la protezione dei dati aziendali non solo come insieme di strumenti tecnici, ma come parte integrante della cultura organizzativa. Questo cambiamento va oltre l'utilizzo di algoritmi avanzati, implica la creazione di un approccio sistemico in cui le decisioni, la gestione dei rischi e la responsabilità condivisa diventano centrali. La protezione dei dati smette di essere un obbligo formale per diventare un processo dinamico, capace di adattarsi alle esigenze in continua evoluzione dell'azienda e degli utenti.

Un elemento distintivo del nuovo paradigma riguarda la capacità di anticipare scenari complessi e inattesi. L'intelligenza artificiale non si limita a segnalare eventi noti, ma individua *pattern* nascosti nei dati che possono prefigurare rischi futuri. In questo senso, le aziende non reagiscono più esclusivamente a incidenti già accaduti, ma sviluppano una visione predittiva della sicurezza. Tale approccio richiede una gestione accurata delle fonti dati e della loro qualità. L'efficacia dell'IA dipende dalla precisione delle informazioni di input e dalla capacità di contestualizzare ogni segnale rilevato. Il risultato è un controllo più raffinato e tempestivo, che consente di prevenire danni potenziali senza bloccare le attività operative quotidiane[134].

Accanto alla proattività, il paradigma basato sull'IA enfatizza la resilienza dei processi aziendali. La protezione dei dati non riguarda solo l'identificazione delle minacce, ma anche la capacità di adattare le strategie di difesa in risposta a contesti mutevoli. Sistemi intelligenti possono aggiornare continuamente i propri criteri di analisi in base all'evoluzione delle minacce, alle nuove modalità di interazione dei clienti e alle innovazioni tecnologiche. Questo implica una gestione costante, in cui gli strumenti

[134] ENISA, Artificial Intelligence Cybersecurity Challenges, European Union Agency for Cybersecurity, 2023, https://www.enisa.europa.eu/publications/artificial-intelligence-Cybersecurity-challenges

automatizzati e l'esperienza umana si integrano. La tecnologia suggerisce azioni e segnala anomalie, mentre il giudizio dei professionisti decide la risposta più appropriata. In questo modo, la protezione dei dati diventa un processo vivo, capace di crescere insieme all'azienda.

Tuttavia, l'adozione di un paradigma di questo tipo non è priva di criticità. La trasparenza delle decisioni automatizzate rappresenta un nodo centrale. La complessità degli algoritmi può rendere difficile comprendere come e perché determinate operazioni vengano bloccate o modificate. Per le aziende, ciò comporta la necessità di progettare sistemi intelligibili, che consentano di spiegare le scelte a utenti e stakeholder, e di sviluppare procedure interne di verifica. La sfida non è soltanto tecnica, ma riguarda la fiducia, un'IA percepita come opaca può suscitare diffidenza, riducendo l'efficacia degli strumenti di protezione e compromettendo il rapporto tra azienda e clienti.

Un ulteriore aspetto critico riguarda la gestione dei confini tra automazione e responsabilità umana. L'intelligenza artificiale non deve sostituire il giudizio delle persone, ma supportarlo in modo mirato. Un'eccessiva delega ai sistemi digitali può generare rischi di errore non rilevato o di interpretazioni errate dei dati. Per questo motivo, le aziende devono definire chiaramente le responsabilità interne, aumentare controlli periodici e assicurare che gli operatori possano intervenire in modo efficace. La combinazione di automazione e supervisione umana costituisce il vero nucleo del nuovo paradigma. L'IA diventa un elemento chiave che amplifica la capacità decisionale, ma non ne sostituisce la componente etica e strategica.

Un altro elemento distintivo di questo approccio è la personalizzazione della sicurezza. Sistemi intelligenti possono modulare le misure di protezione in base al profilo e al comportamento dei singoli utenti, senza introdurre rigidità inutili. Questo consente di bilanciare due esigenze spesso percepite come in contrasto. La tutela dei dati e la fluidità dell'esperienza digitale. Ad esempio, controlli più rigorosi possono essere applicati a transazioni o attività ritenute a rischio, mentre operazioni abituali e regolari possono procedere senza frizioni. In questo modo, la tecnologia rafforza la protezione senza compromettere la soddisfazione dell'utente, dimostrando che sicurezza e fruibilità non sono necessariamente opposti, ma possono essere integrati in maniera armoniosa.

Infine, il paradigma dell'IA apre la strada a una gestione strategica dei rischi reputazionali e normativi. Proteggere i dati non è più solo un obbligo di legge, ma un fattore

competitivo. La capacità di dimostrare trasparenza, controllo e adattabilità rafforza la credibilità dell'azienda e consolida la fiducia degli utenti. Allo stesso tempo, richiede un approccio strutturato alla *governance*, in cui le politiche aziendali, le procedure operative e le verifiche periodiche si coordinano per garantire la conformità legale e la sostenibilità a lungo termine. L'intelligenza artificiale diventa uno strumento di governo dei dati, capace di supportare decisioni strategiche senza sostituire la responsabilità umana, ma amplificandone l'efficacia[135].

Il nuovo paradigma introdotto dall'IA nella tutela dei dati aziendali non è un semplice aggiornamento tecnologico, ma una trasformazione culturale e organizzativa. Esso implica un equilibrio tra automazione e supervisione, proattività e resilienza, sicurezza e usabilità. L'adozione consapevole di questi strumenti consente alle aziende di affrontare un contesto digitale sempre più complesso, proteggere i dati in modo efficace e consolidare un modello di fiducia con clienti.

[135] Politecnico di Milano – Osservatorio Cybersecurity & Data Protection, *Rapporto sulla sicurezza ICT in Italia*, 2023.

CAPITOLO QUARTO

L'INTELLIGENZA ARTIFICIALE COME FATTORE DI COMPLESSITA' NELL'APPLICAZIONE DELLA DISCIPLINA DELLA PROTEZIONE DEI DATI PERSONALI

Nel capitolo precedente l'intelligenza artificiale è stata analizzata come possibile strumento di supporto all'attuazione della disciplina della protezione dei dati personali, evidenziandone il potenziale contributo in termini di monitoraggio, gestione del rischio, responsabilità e automazione dei processi di compliance. Tale analisi ha mostrato come, se correttamente integrata nei processi organizzativi, l'IA possa rafforzare la capacità delle imprese di conformarsi agli obblighi previsti dal GDPR, rendendo più efficienti attività complesse e ad alto contenuto informativo.

Tuttavia, l'adozione di sistemi di intelligenza artificiale nei processi di trattamento dei dati personali non si traduce automaticamente in un rafforzamento della tutela dei diritti degli interessati. Al contrario, proprio le caratteristiche che rendono l'IA uno strumento potenzialmente utile alla compliance – l'automazione, la capacità predittiva, l'elaborazione di grandi volumi di dati e la riduzione dell'intervento umano diretto – possono trasformarsi in fattori di criticità sotto il profilo dell'applicazione concreta della disciplina della protezione dei dati personali.

Il presente capitolo si propone dunque di analizzare l'intelligenza artificiale non come fenomeno tecnologico astratto, né come mera innovazione organizzativa, ma come elemento che incide direttamente sulle modalità di attuazione del GDPR all'interno delle imprese. L'attenzione è rivolta alle condizioni organizzative, decisionali e di *governance* che possono rendere più complesso garantire il rispetto dei principi fondamentali della protezione dei dati, quali liceità, trasparenza, minimizzazione, sicurezza e accountability. In questa prospettiva, l'IA non viene considerata in termini di "rischio tecnologico" in senso generico, bensì come fattore che può aumentare la fragilità dei meccanismi di conformità, incidendo sulla capacità dell'organizzazione di controllare i trattamenti, attribuire correttamente le responsabilità, documentare le scelte effettuate e assicurare

l'effettivo esercizio dei diritti degli interessati. L'analisi non si concentra sull'evento negativo in sé, ma sui presupposti strutturali che rendono più o meno probabile il verificarsi di situazioni di non conformità.

Il capitolo si articola, pertanto, in un'analisi progressiva dei principali profili di criticità legati all'uso dell'intelligenza artificiale nei trattamenti di dati personali, dalle fragilità organizzative e decisionali, ai limiti di trasparenza degli algoritmi, alle problematiche di sicurezza, fino all'esame di un caso concreto di applicazione industriale. In questo modo, l'IA viene esaminata come componente che influisce sulla resilienza complessiva dell'organizzazione rispetto agli obblighi di protezione dei dati personali, mettendo in luce le tensioni tra automazione, efficienza e tutela dei diritti fondamentali.

4.1 Fragilità organizzative e responsabilità nel trattamento dei dati personali

L'introduzione di sistemi di intelligenza artificiale nei processi aziendali comporta una trasformazione profonda delle modalità di trattamento dei dati personali, incidendo in maniera significativa sull'assetto organizzativo previsto dalla disciplina della protezione dei dati. Uno dei profili più critici riguarda la complessità nell'attribuzione delle responsabilità e nella concreta applicazione del principio di accountability sancito dal GDPR.

Come illustrato nel primo capitolo, il regolamento europeo impone al titolare del trattamento l'obbligo non solo di rispettare i principi di protezione dei dati, ma anche di essere in grado di dimostrarne l'osservanza. In presenza di sistemi di IA, tale obbligo assume una dimensione particolarmente problematica. L'automazione decisionale, l'uso di modelli complessi e l'interazione tra diversi attori tecnologici rendono infatti più difficile individuare chi sia effettivamente responsabile delle scelte che incidono sul trattamento dei dati personali.

In contesti tradizionali, il processo decisionale relativo al trattamento dei dati è riconducibile a soggetti chiaramente identificabili all'interno dell'organizzazione. Al contrario, l'adozione di sistemi di intelligenza artificiale tende a distribuire le decisioni lungo una catena articolata che coinvolge sviluppatori, fornitori di soluzioni tecnologiche, *data scientist*, responsabili IT e figure manageriali. Questa frammentazione decisionale

può indebolire la capacità del titolare del trattamento di esercitare un controllo effettivo sui trattamenti e di dimostrare il rispetto delle prescrizioni normative[136].

Dal punto di vista della protezione dei dati personali, tale situazione genera una fragilità strutturale. Il rischio non è soltanto quello di un trattamento illecito, ma quello di un'organizzazione che non è in grado di ricostruire e giustificare le scelte effettuate in relazione ai dati personali. L'IA, in questo senso, non elimina la responsabilità del titolare, ma ne rende più complessa l'attuazione concreta, richiedendo un rafforzamento dei meccanismi interni di gestione organizzativa e documentazione.

Un ulteriore elemento di criticità riguarda il rapporto tra automazione e controllo umano. L'affidamento crescente a sistemi intelligenti può generare una riduzione dell'intervento umano diretto nelle fasi decisionali, con il rischio che le decisioni automatizzate vengano percepite come "neutrali" o "oggettive". Tale percezione può condurre a un indebolimento delle attività di supervisione, in contrasto con l'impostazione del GDPR, che richiede una valutazione costante dei rischi e delle conseguenze dei trattamenti sui diritti degli interessati.

In questo contesto, l'IA può favorire una sorta di delega implicita della responsabilità decisionale al sistema tecnologico, rendendo più difficile individuare le cause di eventuali violazioni e adottare misure correttive tempestive. La fragilità non risiede tanto nella tecnologia in sé, quanto nella capacità dell'organizzazione di mantenere il controllo sostanziale sui trattamenti, evitando che l'automazione si traduca in una perdita di consapevolezza giuridica.

La complessità organizzativa si riflette anche sul ruolo del *Data Protection Officer*, chiamato a operare in un contesto in cui le scelte rilevanti per la protezione dei dati sono incorporate in sistemi tecnici altamente specializzati. L'effettività del suo intervento dipende dalla possibilità di comprendere, monitorare e valutare i sistemi di IA utilizzati, nonché dalla collaborazione delle funzioni aziendali coinvolte. In assenza di un adeguato coordinamento interno, il rischio è che la protezione dei dati venga relegata a un livello formale, privo di reale incidenza sulle decisioni operative.

Da ultimo, l'uso dell'intelligenza artificiale può accentuare le fragilità organizzative anche sotto il profilo della gestione del rischio. L'evoluzione dinamica dei modelli,

[136] Brynjolfsson, E., & McAfee, A. (2017). *Machine, Platform, Crowd: Harnessing Our Digital Future*. New York: W. W. Norton & Company.

l'apprendimento continuo e l'adattamento automatico dei sistemi rendono necessario un aggiornamento costante delle valutazioni di impatto e delle misure di protezione adottate. Se tali attività non vengono integrate stabilmente nei processi decisionali dell'impresa, l'IA può trasformarsi da strumento di supporto alla compliance a fattore strutturale di esposizione a rischi di non conformità[137].

L'intelligenza artificiale ha un impatto rilevante sull'assetto organizzativo richiesto dal GDPR, rendendo più complessa l'attuazione del principio di accountability e la gestione delle responsabilità nel trattamento dei dati personali. La sfida non consiste nel limitare l'adozione dell'IA, ma nel costruire modelli organizzativi in grado di governarne l'uso in modo consapevole, trasparente e giuridicamente resiliente.

4.2 Opacità algoritmica, bias decisionali e tutela dei diritti degli interessati

L'impiego di sistemi di intelligenza artificiale nei processi di trattamento dei dati personali solleva questioni particolarmente rilevanti in relazione ai principi di trasparenza, correttezza e tutela dei diritti degli interessati, che costituiscono il nucleo della disciplina della protezione dei dati personali. A differenza delle fragilità organizzative analizzate nel paragrafo precedente, le criticità che emergono in questo ambito riguardano direttamente l'impatto delle decisioni algoritmiche sugli individui e sulla loro capacità di comprendere, controllare e contestare i trattamenti che li riguardano.

Uno dei principali elementi di complessità è rappresentato dalla cosiddetta opacità algoritmica. Molti sistemi di intelligenza artificiale, in particolare quelli basati su modelli di *machine learning* avanzato, operano attraverso meccanismi decisionali difficilmente intelligibili anche per gli stessi soggetti che li sviluppano o li utilizzano. Questa caratteristica entra in tensione con il principio di trasparenza sancito dal GDPR, che richiede che gli interessati siano informati in modo chiaro e comprensibile circa le modalità di trattamento dei loro dati personali.

Dal punto di vista della protezione dei dati, la difficoltà non risiede esclusivamente nella complessità tecnica dei modelli, ma nella traduzione di tale complessità in informazioni giuridicamente rilevanti per l'interessato. Il GDPR non impone la divulgazione del codice

[137] Harvard Business Review Italia, L'intelligenza artificiale generativa, eBook, 2023. Disponibile online: https://www.hbritalia.it/userUpload/ebook_LIA_generativa.pdf

sorgente o dei dettagli tecnici dell'algoritmo, ma richiede che l'interessato possa comprendere le logiche di base del trattamento e le sue possibili conseguenze. In presenza di sistemi di IA opachi, garantire tale comprensione diventa un obiettivo particolarmente difficile da raggiungere, soprattutto quando il trattamento incide in modo significativo sulla sfera giuridica o personale dell'individuo.

A questa problematica si affianca il tema dei bias algoritmici, ossia delle decisioni soggette ad errori che possono emergere a causa della qualità dei dati di addestramento, delle scelte progettuali o delle modalità di utilizzo dei sistemi di intelligenza artificiale.

I bias assumono una rilevanza specifica in ambito di protezione dei dati personali quando producono effetti discriminatori o ingiustificatamente penalizzanti per determinati gruppi di interessati. In tali casi, il rischio non è soltanto etico o sociale, ma giuridico, poiché vengono messi in discussione i principi di correttezza e liceità del trattamento[138].

Il trattamento automatizzato basato su dati storici può infatti riprodurre o amplificare disuguaglianze preesistenti, incidendo sulla valutazione di comportamenti, profili o caratteristiche personali degli individui. Questo aspetto assume particolare rilievo nei contesti in cui l'IA viene utilizzata per attività di profilazione, valutazione del rischio o monitoraggio dei comportamenti, ambiti nei quali il GDPR riconosce una protezione rafforzata dei diritti degli interessati. In tali situazioni, l'uso dell'intelligenza artificiale rende più complesso garantire che le decisioni siano fondate su criteri equi, pertinenti e proporzionati.

La presenza di bias e l'opacità dei modelli decisionali incidono direttamente sulla possibilità per l'interessato di esercitare i diritti riconosciuti dal regolamento, quali il diritto di accesso, di rettifica e di opposizione. Se il funzionamento del sistema non è sufficientemente comprensibile, l'interessato si trova in una posizione di debolezza informativa che limita la sua capacità di contestare il trattamento o di richiedere interventi correttivi. In questo senso, l'intelligenza artificiale può contribuire a un'asimmetria di potere tra titolare del trattamento e interessato, in contrasto con la finalità di riequilibrio che caratterizza la disciplina della protezione dei dati personali.

Un ulteriore profilo di criticità riguarda le decisioni basate unicamente su trattamenti automatizzati, disciplinate dall'articolo 22 del GDPR. Sebbene il regolamento non vieti

[138] Davenport, T. H., Guha, A., Grewal, D., & Bressgott, T. (2020). *How artificial intelligence will change the future of marketing*. *Journal of the Academy of Marketing Science*, 48, 24–42.

in modo assoluto tali decisioni, esso prevede condizioni stringenti e specifiche garanzie per gli interessati. L'utilizzo di sistemi di intelligenza artificiale in questo ambito rende particolarmente complesso assicurare il rispetto di tali garanzie, soprattutto quando l'intervento umano risulta limitato o meramente formale. La difficoltà di comprendere e spiegare le decisioni algoritmiche può svuotare di contenuto il diritto dell'interessato a ottenere un intervento umano significativo.

Dal punto di vista organizzativo, queste criticità impongono alle imprese un ripensamento delle modalità con cui vengono progettati, implementati e monitorati i sistemi di intelligenza artificiale. La protezione dei dati personali non può essere considerata un elemento accessorio, ma deve essere integrata nelle fasi di progettazione e valutazione dei sistemi, secondo i principi di privacy by design e by default. In assenza di tali accorgimenti, l'IA rischia di compromettere l'effettività delle tutele previste dal GDPR, trasformando la complessità tecnologica in un ostacolo all'esercizio dei diritti fondamentali.

L'opacità algoritmica e la presenza di bias decisionali rappresentano uno dei principali fattori attraverso cui l'intelligenza artificiale rende più fragile l'applicazione concreta della disciplina della protezione dei dati personali. La sfida per le organizzazioni non consiste nell'eliminare l'uso dell'IA, ma nel garantire che i sistemi adottati siano compatibili con i principi di trasparenza, correttezza e tutela dei diritti degli interessati, evitando che l'automazione decisionale si traduca in una riduzione delle garanzie riconosciute dal GDPR.

4.3 Intelligenza artificiale, sicurezza dei dati e responsabilità del titolare del trattamento

L'impiego dell'intelligenza artificiale nei contesti aziendali incide in modo significativo sulle modalità di gestione della sicurezza dei dati personali, rendendo più articolata l'applicazione degli obblighi previsti dal GDPR in capo al titolare del trattamento. A differenza dei sistemi informatici tradizionali, l'IA non si limita a conservare o trasmettere dati, ma li utilizza in modo dinamico per generare inferenze, previsioni e modelli decisionali, ampliando il perimetro del trattamento e aumentando il potenziale impatto di eventuali violazioni.

Dal punto di vista della disciplina della protezione dei dati personali, la sicurezza non è un obiettivo meramente tecnico, ma un obbligo giuridico funzionale alla tutela dei diritti e delle libertà fondamentali degli interessati. L'articolo 32 del GDPR impone al titolare e al responsabile del trattamento di adottare misure tecniche e organizzative adeguate al rischio. Tuttavia, l'introduzione di sistemi di intelligenza artificiale rende particolarmente complessa la valutazione di tale rischio, poiché i trattamenti diventano meno prevedibili e più difficili da circoscrivere.

Uno degli elementi di maggiore criticità riguarda la moltiplicazione dei flussi di dati personali. I sistemi di IA operano spesso integrando informazioni provenienti da fonti diverse, talvolta originariamente raccolte per finalità differenti. Questa interconnessione rende più difficile garantire il rispetto dei principi di limitazione della finalità e di minimizzazione dei dati. Anche quando il singolo trattamento appare conforme, l'uso combinato dei dati all'interno di modelli intelligenti può generare nuove informazioni personali, ampliando il contenuto informativo senza che l'interessato ne sia pienamente consapevole[139].

La sicurezza dei dati personali assume inoltre una dimensione ulteriore quando si considerano i modelli di intelligenza artificiale come possibili vettori di rischio. I modelli addestrati su dati personali possono, in alcuni casi, incorporare informazioni sensibili nei propri parametri interni. Questo fenomeno rende più difficile garantire che, anche in caso di accesso non autorizzato al modello, i dati personali non siano indirettamente esposti. In tali situazioni, il confine tra violazione del dato e violazione del modello diventa sfumato, ponendo nuove sfide all'applicazione delle regole tradizionali in materia di *data breach.*

Un ulteriore profilo di complessità riguarda la gestione degli incidenti di sicurezza. Nel contesto dell'intelligenza artificiale, una violazione non si esaurisce necessariamente nell'evento iniziale, ma può produrre effetti prolungati nel tempo. Un modello addestrato su dati compromessi o alterati può continuare a influenzare le decisioni future, incidendo sulla correttezza dei trattamenti anche dopo il ripristino dei sistemi. Questo aspetto rende particolarmente delicata l'applicazione degli obblighi di notifica delle violazioni dei dati personali previsti dagli articoli 33 e 34 del GDPR.

---

[139] V. Dignum, *Responsible Artificial Intelligence: How to Develop and Use AI in a Responsible Way*, Springer, (2019), pp.47-68.

La responsabilità del titolare del trattamento assume, in questo scenario, un ruolo centrale. Il GDPR attribuisce al titolare il compito di dimostrare la conformità del trattamento ai principi del regolamento (accountability). Tuttavia, l'utilizzo di sistemi di IA sviluppati o gestiti da fornitori esterni può rendere più difficile esercitare un controllo effettivo sui trattamenti. La dipendenza da soluzioni tecnologiche complesse rischia di tradursi in una delega di fatto delle decisioni rilevanti, in contrasto con il principio secondo cui la responsabilità non può essere trasferita.

In questo contesto, l'intelligenza artificiale può rappresentare sia un fattore di rischio sia un possibile strumento di supporto alla disciplina della protezione dei dati personali. Da un lato, essa amplia la superficie di attacco e rende più complessa la gestione della sicurezza; dall'altro, può essere utilizzata per individuare anomalie, prevenire violazioni e rafforzare i meccanismi di controllo. Tuttavia, affinché l'IA possa effettivamente "aiutare" la protezione dei dati, è necessario che il suo utilizzo sia guidato da una chiara strategia di *governance*, orientata alla tutela dei diritti degli interessati e non esclusivamente all'efficienza operativa.

4.3 L'intelligenza artificiale come fattore di complessità e fragilità nell'applicazione concreta del GDPR

L'impiego dell'intelligenza artificiale nei processi di trattamento dei dati personali non si limita ad ampliare il perimetro dei rischi già noti in materia di *data protection*, ma incide in modo più profondo sulla possibilità stessa di applicare in maniera effettiva, coerente e verificabile i principi sanciti dal Regolamento generale sulla protezione dei dati. Il GDPR è costruito su una struttura normativa che presuppone un elevato grado di controllo umano sul trattamento; il titolare è chiamato a determinare preventivamente finalità, basi giuridiche, modalità operative e misure di tutela, assumendosene la piena responsabilità. L'introduzione di sistemi di intelligenza artificiale tende, tuttavia, a mettere sotto tensione questa architettura, rendendo più complesso il passaggio dalla conformità formale alla tutela sostanziale dei diritti degli interessati.

Una prima area di criticità riguarda la capacità del titolare del trattamento di mantenere un controllo effettivo sulle finalità del trattamento. Nei sistemi tradizionali, la relazione tra dato personale e scopo perseguito è generalmente lineare e circoscrivibile; nei sistemi

di IA, invece, il dato assume un valore dinamico, poiché viene utilizzato non solo per produrre un risultato immediato, ma anche per alimentare processi di apprendimento e ottimizzazione continua. In questo contesto, anche quando le finalità dichiarate restano formalmente invariate, il modo in cui i dati contribuiscono alla generazione degli output può evolvere nel tempo, rendendo più difficile dimostrare che il trattamento resti effettivamente confinato entro i limiti originariamente comunicati agli interessati. Ne deriva una fragilità applicativa del principio di limitazione della finalità, che rischia di perdere la sua funzione di presidio sostanziale a favore di una lettura meramente dichiarativa.

L'intelligenza artificiale incide in modo significativo anche sulla concreta applicazione del principio di minimizzazione dei dati. Il GDPR richiede che i dati personali siano adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità del trattamento. Tuttavia, nei sistemi basati su modelli predittivi o di apprendimento automatico, la determinazione di ciò che è "necessario" non è sempre immediatamente verificabile. Il contributo del singolo dato al risultato finale è spesso indiretto e difficilmente isolabile, e l'efficacia del sistema può dipendere dalla disponibilità di ampi set informativi. Questa caratteristica non implica automaticamente un trattamento illecito, ma rende più oneroso per il titolare dimostrare, in sede di accountability, che le scelte operate siano effettivamente conformi al principio di minimizzazione, trasformando un obbligo giuridico chiaro in un requisito di difficile attuazione pratica.

Un ulteriore elemento di complessità emerge con riferimento alla trasparenza del trattamento e alla comprensibilità delle decisioni automatizzate. Il GDPR attribuisce un ruolo centrale alla possibilità per l'interessato di comprendere come e perché i propri dati vengano utilizzati, soprattutto quando il trattamento incide in modo significativo sulla sua sfera giuridica. L'impiego di sistemi di intelligenza artificiale, caratterizzati da processi decisionali complessi e talvolta opachi, rende più difficile tradurre le logiche algoritmiche in informazioni accessibili e comprensibili. Anche in assenza di una vera e propria "black box" tecnologica, la distanza tra il funzionamento del sistema e la capacità dell'interessato di comprenderne gli effetti può compromettere l'effettività dei diritti informativi,

trasformando la trasparenza in un adempimento formale privo di reale incidenza sulla posizione dell'individuo[140].

Questa difficoltà si riflette direttamente sull'esercizio dei diritti riconosciuti agli interessati dal GDPR. Diritti come l'accesso, la rettifica, la cancellazione o la limitazione del trattamento presuppongono la possibilità di individuare il dato personale e di intervenire su di esso in modo puntuale. Nei sistemi di intelligenza artificiale, tuttavia, i dati possono essere integrati nei parametri del modello, contribuendo in modo diffuso alla generazione degli output. In tali contesti, l'attuazione concreta dei diritti rischia di scontrarsi con limiti tecnici che, pur non esonerando il titolare dalle proprie responsabilità, rendono la tutela meno immediata e più fragile sul piano operativo.

La presenza di sistemi di IA incide inoltre sulla portata del principio di accountability, che costituisce uno dei pilastri del GDPR. La responsabilizzazione del titolare non si esaurisce nell'adozione di misure adeguate, ma richiede la capacità di dimostrare in modo continuo la conformità del trattamento. Nei contesti automatizzati, la conformità non può essere considerata uno stato statico. Il comportamento del sistema può mutare nel tempo in funzione dei dati utilizzati, delle condizioni operative e delle interazioni con altri sistemi. Questo rende necessario un monitoraggio costante e una revisione periodica delle scelte effettuate, aumentando il carico organizzativo e documentale richiesto per garantire una protezione effettiva dei dati personali.

Un ulteriore profilo di fragilità riguarda il rapporto tra automazione e responsabilità umana. Sebbene il GDPR attribuisca sempre al titolare del trattamento la responsabilità ultima delle decisioni, l'affidamento crescente a sistemi intelligenti può ridurre, nella pratica, la capacità di intervento consapevole da parte degli operatori umani. Il rischio non è soltanto quello di una delega eccessiva alla tecnologia, ma quello di una progressiva difficoltà nel ricostruire le scelte effettuate dal sistema e nel giustificarle sotto il profilo giuridico. Ciò incide direttamente sulla possibilità di garantire una tutela effettiva in caso di contestazioni o verifiche da parte delle autorità di controllo.

In questa prospettiva, l'intelligenza artificiale non rappresenta semplicemente una nuova tipologia di trattamento dei dati personali, ma un fattore che mette sotto pressione l'impianto complessivo della protezione dei dati. Il GDPR continua a fornire i principi di

[140] Regolamento (UE) 2016/679, art. 5, Principi applicabili al trattamento dei dati personali.

riferimento, ma la loro applicazione concreta diventa più complessa, più onerosa e meno lineare quando i trattamenti sono mediati da sistemi intelligenti. L'IA agisce così come un moltiplicatore delle criticità operative, rendendo evidente come la tutela dei dati personali non possa essere affidata esclusivamente a soluzioni tecniche o a un rispetto formale delle regole, ma richieda un approccio integrato, consapevole e dinamico alla *governance* dei processi automatizzati.

4.5 Caso concreto di utilizzo dell'intelligenza artificiale e criticità applicative del GDPR: i sistemi algoritmici di Amazon nella gestione dei lavoratori

A differenza del caso Amazon analizzato nel Capitolo II, utilizzato come esempio di applicazione sanzionatoria del GDPR in materia di profilazione pubblicitaria, il presente paragrafo considera Amazon come caso emblematico per indagare le sfide strutturali dell'uso diffuso dell'intelligenza artificiale nell'applicazione concreta della normativa sulla protezione dei dati personali. In questa sede, l'attenzione non si concentra sul singolo procedimento sanzionatorio, bensì sulle dinamiche organizzative, tecnologiche e decisionali che, nei contesti aziendali complessi, rendono più difficile l'effettiva attuazione dei principi di trasparenza, accountability e tutela dei diritti degli interessati previsti dal GDPR.

L'utilizzo dell'intelligenza artificiale nei contesti aziendali non riguarda esclusivamente l'ottimizzazione dei processi produttivi o l'analisi dei mercati, ma investe sempre più frequentemente la gestione delle risorse umane e l'organizzazione del lavoro. Un caso particolarmente significativo, anche alla luce delle problematiche connesse alla protezione dei dati personali, è rappresentato dall'esperienza di Amazon, che ha introdotto su larga scala sistemi algoritmici e strumenti di intelligenza artificiale per il monitoraggio, la valutazione e la gestione delle attività dei propri dipendenti, in particolare nei centri logistici.

In questo contesto, l'intelligenza artificiale viene impiegata per raccogliere e analizzare una molteplicità di dati relativi ai lavoratori; tempi di esecuzione delle mansioni, ritmi di lavoro, produttività individuale, pause, spostamenti all'interno del magazzino e, in alcuni casi, indicatori comportamentali. Tali informazioni, pur essendo strettamente collegate all'attività lavorativa, costituiscono a tutti gli effetti dati personali ai sensi del GDPR,

poiché riferibili a persone fisiche identificate o identificabili e idonee a incidere in modo significativo sulla loro sfera professionale e personale[141].

L'elemento di maggiore criticità non risiede tanto nella raccolta dei dati in sé, quanto nel modo in cui tali informazioni vengono elaborate attraverso sistemi algoritmici che contribuiscono a orientare decisioni rilevanti, come l'assegnazione dei compiti, la valutazione delle performance, l'individuazione di comportamenti ritenuti non conformi agli standard aziendali e, in alcuni casi, l'avvio di procedimenti disciplinari o la cessazione del rapporto di lavoro. In questo scenario, l'uso dell'intelligenza artificiale rende l'applicazione concreta del GDPR più complessa e fragile, poiché introduce una distanza crescente tra il dato raccolto, il processo decisionale e la possibilità per l'interessato di comprendere e contestare le modalità del trattamento.

Uno dei principi maggiormente messi alla prova è quello della trasparenza. Il GDPR impone che gli interessati siano informati in modo chiaro e comprensibile circa le finalità del trattamento, le logiche utilizzate e le conseguenze previste. Tuttavia, nel caso dei sistemi algoritmici adottati da Amazon, le decisioni non derivano da regole semplici e predeterminate, ma da modelli complessi che operano su grandi quantità di dati e che risultano difficilmente interpretabili anche per gli stessi operatori aziendali. Questa opacità rende problematico fornire informative realmente efficaci, trasformando spesso l'obbligo di trasparenza in un adempimento formale che non consente al lavoratore di comprendere come e perché determinate valutazioni vengano effettuate.

Un ulteriore profilo critico riguarda il principio di limitazione delle finalità e di minimizzazione dei dati. L'utilizzo di sistemi di intelligenza artificiale incentiva una raccolta estesa e continua di informazioni, spesso giustificata dall'esigenza di migliorare l'efficienza e l'accuratezza dei modelli. Tuttavia, questa logica entra in tensione con il GDPR, che richiede che i dati siano adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità dichiarate. Nel caso Amazon, il confine tra monitoraggio funzionale all'organizzazione del lavoro e controllo invasivo dell'attività dei dipendenti appare particolarmente sottile, evidenziando come l'adozione dell'IA possa spingere le imprese verso trattamenti eccedenti rispetto a quanto strettamente necessario.

[141] Gaudio, G., *Le discriminazioni algoritmiche*, LavoroDirittiEuropa.it. (29 gennaio 2024,), https://www.lavorodirittieuropa.it/dottrina/principi-e-fonti/1524-le-discriminazioni-algoritmiche

La difficoltà di applicazione del GDPR emerge con forza anche in relazione al principio di accountability. Il regolamento attribuisce al titolare del trattamento la responsabilità di dimostrare la conformità alle norme, ma quando le decisioni sono fortemente mediate da sistemi automatizzati, diventa complesso individuare con chiarezza le responsabilità effettive. Nel caso in esame, il processo decisionale risulta distribuito tra progettisti degli algoritmi, responsabili delle risorse umane, sistemi informatici e management aziendale. Questa frammentazione rende più difficile non solo attribuire la responsabilità in caso di violazione, ma anche intervenire tempestivamente per correggere eventuali distorsioni o errori del sistema.

Particolarmente rilevante è inoltre il tema delle decisioni automatizzate e del diritto all'intervento umano, previsto dall'art. 22 del GDPR. Sebbene Amazon sostenga che le decisioni finali non siano completamente automatizzate, il peso attribuito alle valutazioni algoritmiche è tale da influenzare in modo determinante l'esito dei processi decisionali. In questi casi, la possibilità per il lavoratore di ottenere una revisione effettiva da parte di una persona fisica rischia di rimanere teorica, soprattutto in contesti caratterizzati da elevati volumi di dati e da processi standardizzati.

Il caso Amazon mette inoltre in luce una criticità più ampia: la difficoltà di esercizio dei diritti degli interessati in presenza di sistemi di intelligenza artificiale. Diritti come l'accesso ai dati, la rettifica o la contestazione delle decisioni presuppongono una comprensione del trattamento e delle logiche sottostanti. Tuttavia, quando il trattamento è basato su modelli complessi e in continua evoluzione, l'effettività di tali diritti risulta ridotta, contribuendo a creare un divario tra la tutela prevista dalla normativa e la sua applicazione concreta.

In questa prospettiva, l'esperienza di Amazon evidenzia come l'intelligenza artificiale non renda automaticamente incompatibile il GDPR, ma ne metta in luce i limiti operativi e interpretativi. Il regolamento è costruito su principi flessibili, pensati per adattarsi a contesti tecnologici diversi, ma l'uso estensivo dell'IA accentua la necessità di tradurre tali principi in pratiche organizzative, procedure di controllo e forme di governance più robuste. In assenza di questi strumenti, il rischio è che la protezione dei dati personali perda efficacia proprio nei contesti in cui l'impatto sulle persone è più significativo.

Il caso analizzato dimostra quindi che l'intelligenza artificiale, soprattutto quando applicata alla gestione dei lavoratori, rende l'applicazione del GDPR più complessa e

fragile non tanto per una carenza normativa, quanto per la difficoltà delle organizzazioni di governare processi decisionali opachi, automatizzati e ad alto impatto. Questo rafforza l'idea che la protezione dei dati personali non possa essere considerata un aspetto accessorio dell'innovazione tecnologica, ma debba essere integrata fin dalla progettazione dei sistemi di intelligenza artificiale, attraverso un approccio che tenga insieme efficienza, responsabilità e tutela dei diritti fondamentali.

4.6 Intelligenza artificiale, governance del rischio e prospettive di integrazione con la disciplina della protezione dei dati personali

Le criticità analizzate nei paragrafi precedenti mostrano come l'adozione dell'intelligenza artificiale non incida soltanto sulle modalità operative delle imprese, ma investa direttamente la capacità dell'organizzazione di applicare in modo effettivo e continuativo la disciplina della protezione dei dati personali. Quando l'IA viene integrata nei processi aziendali, il trattamento dei dati non rappresenta più una fase circoscritta e facilmente delimitabile, ma diventa parte integrante di meccanismi decisionali complessi, dinamici e spesso non pienamente prevedibili. In questa prospettiva, la questione centrale non è se l'intelligenza artificiale sia compatibile con il GDPR in astratto, ma in che modo il suo utilizzo renda più difficile, più fragile e più onerosa l'attuazione concreta dei principi di protezione dei dati personali.

A differenza dei sistemi tradizionali, nei quali il trattamento dei dati è definito ex ante attraverso regole e finalità relativamente stabili, l'intelligenza artificiale introduce una logica adattiva che tende a modificare nel tempo le modalità di utilizzo delle informazioni. I dati personali non vengono soltanto raccolti e conservati, ma diventano materia prima per processi di apprendimento, correlazione e inferenza che possono generare risultati ulteriori rispetto alle finalità originarie. Questo aspetto pone una sfida significativa per il titolare del trattamento, chiamato dal GDPR non solo a rispettare i principi di liceità, correttezza e trasparenza, ma anche a dimostrare, in modo continuativo, la conformità delle proprie scelte organizzative e tecnologiche.

L'uso dell'intelligenza artificiale tende, inoltre, ad amplificare il divario tra progettazione formale dei trattamenti e loro funzionamento effettivo. Anche quando un sistema è inizialmente configurato in modo conforme alla normativa, il suo comportamento può

evolvere nel tempo sulla base dei dati utilizzati e delle interazioni con l'ambiente operativo. Questo fenomeno rende più complessa l'applicazione di principi fondamentali del GDPR, come la limitazione della finalità e la minimizzazione dei dati, poiché il valore informativo non risiede più nel singolo dato, ma nelle relazioni che il sistema è in grado di costruire tra informazioni diverse. Di conseguenza, il rischio non riguarda soltanto l'uso improprio del dato personale, ma la progressiva perdita di controllo sul significato e sugli effetti del trattamento.

In questo contesto, il principio di accountability assume una rilevanza strategica. L'intelligenza artificiale non consente al titolare del trattamento di limitarsi a un approccio formale alla conformità normativa. Al contrario, richiede una capacità rafforzata di governare processi complessi, di monitorarne l'evoluzione e di intervenire tempestivamente in caso di scostamenti rispetto agli obiettivi di tutela dei diritti degli interessati. La difficoltà non risiede solo nella prevenzione delle violazioni, ma nella possibilità di ricostruire ex post il percorso decisionale che ha condotto a un determinato risultato, soprattutto quando questo incide in modo significativo sulla sfera giuridica delle persone.

È proprio in risposta a queste criticità che il legislatore europeo ha adottato, accanto al GDPR, un quadro normativo specifico per l'intelligenza artificiale basato su una logica di gestione del rischio. *L'Artificial Intelligence Act* non si limita a introdurre nuove regole settoriali, ma propone un modello di regolazione che riconosce la diversa incidenza dei sistemi di IA sui diritti fondamentali, inclusa la protezione dei dati personali. La classificazione dei sistemi in base al livello di rischio rappresenta un tentativo di rendere governabile una tecnologia che, per sua natura, tende a sfuggire a schemi rigidi e uniformi.

Questo approccio risulta particolarmente significativo se letto in chiave di protezione dei dati personali, poiché consente di calibrare gli obblighi giuridici in relazione all'impatto potenziale sui diritti fondamentali degli individui. La logica del rischio, già centrale nel GDPR, viene così estesa e rafforzata con riferimento alle tecnologie di intelligenza artificiale, creando un quadro normativo integrato orientato alla prevenzione delle violazioni e alla tutela sostanziale degli interessati.

Tuttavia, l'estensione della logica del rischio ai sistemi di intelligenza artificiale non comporta un rafforzamento automatico della tutela dei dati personali. Al contrario, l'uso

dell'IA tende a rendere più complessa l'applicazione concreta del GDPR, poiché aumenta il grado di scarsa chiarezza dei trattamenti, moltiplica le variabili rilevanti e rende meno immediata l'individuazione dei momenti decisionali in cui il dato personale viene effettivamente utilizzato. Nei sistemi automatizzati, il trattamento non si esaurisce in un singolo atto, ma si sviluppa come processo continuo, rendendo più difficile per il titolare mantenere un controllo sostanziale e dimostrabile.

In tale prospettiva, il rischio assume una dimensione strutturale. Non si tratta più soltanto del rischio di una violazione materiale dei dati, ma della possibilità che l'organizzazione perda progressivamente la capacità di comprendere, spiegare e giustificare i propri trattamenti automatizzati. L'intelligenza artificiale introduce quindi una forma di fragilità sistemica nell'applicazione del GDPR, che richiede un ripensamento delle strategie aziendali in termini di *governance*, supervisione umana e integrazione tra competenze tecniche, giuridiche e organizzative.

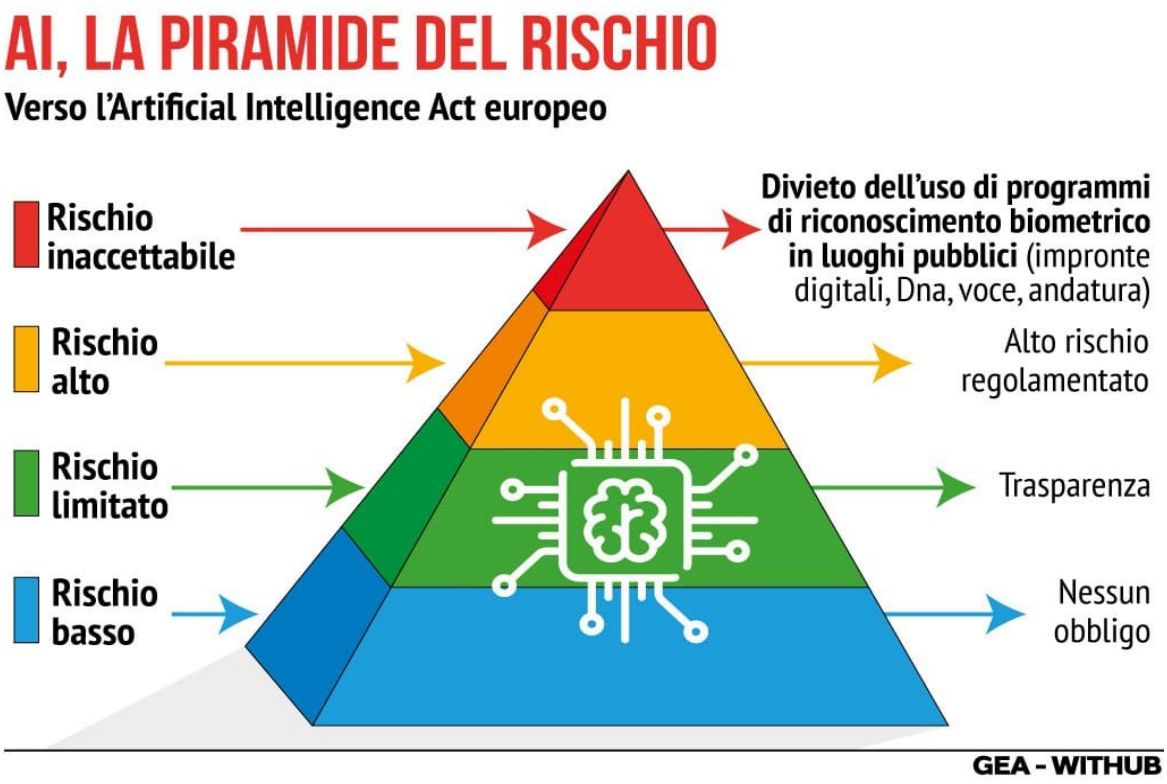

Figura 5: Piramide dei sistemi di IA secondo il rischio – classificazione Atto UE 2024 (fonte: UE News, 2024)[142].

[142] EU News, Atto UE sull'Intelligenza Artificiale: in vigore dal 2024, 1° agosto 2024. Disponibile online: https://www.eunews.it/2024/08/01/atto-ue-intelligenza-artificiale-vigore/

La rappresentazione a piramide consente di visualizzare con immediatezza come solo una parte delle applicazioni di intelligenza artificiale rientri nelle categorie di rischio più elevato, ma anche come proprio tali applicazioni richiedano il maggiore sforzo in termini di *governance* e protezione dei dati personali. I sistemi ad alto rischio sono spesso caratterizzati da trattamenti su larga scala, utilizzo di dati sensibili o capacità di incidere significativamente sulle persone, rendendo più difficile garantire trasparenza, controllo e rispetto dei diritti degli interessati. In questi casi, l'applicazione del GDPR diventa particolarmente complessa e richiede strumenti organizzativi e tecnici avanzati.

La classificazione del rischio non deve essere intesa come un semplice schema normativo, ma come una guida operativa per le imprese. Essa impone una riflessione preventiva sulle modalità di utilizzo dell'IA e sulle conseguenze che tali sistemi possono produrre sul piano della protezione dei dati. In questo senso, l'intelligenza artificiale può diventare anche uno strumento di supporto alla disciplina del GDPR, contribuendo a migliorare il monitoraggio dei trattamenti, la gestione delle violazioni e la documentazione delle decisioni, purché sia inserita all'interno di un quadro di *governance* chiaro e strutturato.

Affinché l'IA possa effettivamente "aiutare" la disciplina della protezione dei dati personali, è necessario che l'organizzazione mantenga un controllo effettivo sui sistemi automatizzati. Ciò implica la definizione di ruoli e responsabilità chiare, la supervisione umana dei processi decisionali e la capacità di intervenire in caso di risultati inattesi o distorti. L'assenza di tali presidi rischia di trasformare l'intelligenza artificiale in un fattore di ambiguità, compromettendo l'accountability richiesta dal GDPR e rendendo difficile dimostrare la conformità alle autorità di controllo.

Un ulteriore elemento critico riguarda la sostenibilità nel tempo delle scelte tecnologiche. L'adozione dell'IA non è un evento isolato, ma un processo che evolve insieme ai dati, ai modelli e ai contesti organizzativi. In questa prospettiva, la protezione dei dati personali deve essere integrata nei meccanismi di apprendimento organizzativo, evitando che le decisioni vengano progressivamente "incorporate" nei sistemi senza un adeguato riesame critico. Il rischio, altrimenti, è quello di una delega tecnologica che riduce la capacità dell'impresa di comprendere e governare i propri processi di trattamento.

Le analisi condotte evidenziano come l'intelligenza artificiale rende più complessa l'applicazione del GDPR, ma al tempo stesso ne conferma la centralità come strumento di gestione del rischio e di tutela dei diritti fondamentali. Il rapporto tra IA e protezione

dei dati personali non è di contrapposizione, ma di interdipendenza. La capacità delle imprese di integrare l'IA in modo coerente con i principi del GDPR rappresenta una condizione essenziale per un'innovazione tecnologica duratura, responsabile e giuridicamente solida.

CONCLUSIONI

La trasformazione digitale ha ridefinito il ruolo delle imprese, ponendo la gestione sicura dei dati e la protezione delle informazioni al centro delle strategie aziendali. Quanto emerso nei diversi capitoli della tesi conferma che Cybersecurity e protezione dei dati non sono ambiti isolati, ma componenti integrate del funzionamento dell'impresa moderna. La loro interazione incide non solo sul livello di sicurezza tecnica dei sistemi, ma anche sulla qualità delle relazioni con i consumatori, sulla trasparenza della comunicazione e sulla credibilità dell'organizzazione in un contesto caratterizzato da crescente complessità.

La prima considerazione da trarre riguarda il ruolo del GDPR, che ha segnato un cambiamento strutturale nel rapporto tra imprese e dati personali. Con l'introduzione del principio di accountability, il regolamento ha superato la logica delle misure minime e delle prescrizioni standardizzate, imponendo un modello più maturo e dinamico, fondato sulla responsabilità del titolare nel valutare i rischi e adottare misure adeguate. Questo approccio ha spinto le organizzazioni a ripensare i propri processi, la struttura interna e le modalità di gestione delle informazioni. La protezione dei dati non è più un compito circoscritto agli specialisti IT, ma un impegno trasversale che coinvolge tutte le funzioni aziendali.

Dall'analisi emergono anche le difficoltà che molte imprese, soprattutto le piccole e medie realtà, incontrano nel tradurre in pratica i principi del GDPR. La complessità tecnica, la carenza di competenze specialistiche interne, la frammentazione dei sistemi informativi e la resistenza culturale al cambiamento rappresentano barriere concrete che possono rallentare il processo di adeguamento. In diversi casi, la *compliance* tende a ridursi a un insieme di adempimenti formali che non garantiscono una tutela effettiva degli interessati, evidenziando un divario tra rispetto apparente delle norme e protezione reale dei dati. Questa distanza sottolinea la necessità di investire nella formazione continua, nella sensibilizzazione del personale e nell'adozione di strumenti organizzativi e tecnologici adeguati.

Un altro elemento centrale riguarda la dimensione comunicativa. La protezione dei dati non è soltanto un obbligo normativo, ma una condizione indispensabile per costruire e mantenere la fiducia. Consumatori e utenti sono sempre più consapevoli del valore delle

informazioni che li riguardano e mostrano maggiore attenzione nei confronti delle organizzazioni con cui interagiscono. In questo contesto, la trasparenza diventa un fattore competitivo cioè: comunicare in modo chiaro le finalità del trattamento, le misure di sicurezza adottate e i diritti riconosciuti agli interessati contribuisce a rafforzare la reputazione dell'impresa e a differenziarla sul mercato. La fiducia digitale assume quindi un ruolo strutturale nell'identità aziendale.

La tesi ha inoltre mostrato come la Cybersecurity abbia assunto un ruolo di crescente importanza nella prevenzione dei rischi e nella gestione delle vulnerabilità. La natura sempre più sofisticata degli attacchi informatici, la diffusione capillare dei dispositivi connessi e l'aumento della superficie di esposizione ai rischi richiedono strategie integrate che non si limitino all'adozione di tecnologie avanzate, ma includano anche piani di risposta agli incidenti, test periodici e una valutazione costante delle minacce. La sicurezza informatica non può essere considerata un investimento accessorio, ma rappresenta una condizione essenziale per garantire la continuità operativa e proteggere il patrimonio informativo.

Particolarmente rilevante è, infine, il ruolo dell'Intelligenza Artificiale. Le tecnologie basate sull'IA offrono nuove possibilità per migliorare la protezione dei dati, rilevare anomalie, anticipare minacce e ottimizzare i processi aziendali. Allo stesso tempo, il loro utilizzo solleva nuove sfide etiche e normative, legate alla trasparenza degli algoritmi, alla minimizzazione dei dati e al rischio di trattamenti automatizzati potenzialmente invasivi. Lo sviluppo dell'AI Act e la crescente attenzione europea verso le tecnologie emergenti evidenziano la necessità di integrare sicurezza, etica e progettazione tecnologica all'interno di un approccio orientato alla responsabilità. L'Intelligenza Artificiale non rappresenta soltanto uno strumento operativo, ma un elemento trasformativo del sistema di gestione dei dati.

L'analisi svolta consente di affermare che la sicurezza digitale rappresenta oggi una delle sfide più rilevanti per le imprese, ma anche una delle opportunità più significative. Proteggere i dati significa tutelare le persone, i processi e la reputazione dell'organizzazione, incidendo direttamente sulla sua capacità di competere e innovare.

La Cybersecurity e la protezione dei dati devono quindi essere considerate parte integrante della strategia aziendale, attraversando i processi organizzativi e le modalità di comunicazione. In un contesto in cui il valore dell'informazione cresce costantemente, la

capacità dell'impresa di gestire i dati in modo sicuro, trasparente e responsabile diventa un elemento decisivo non solo ai fini della conformità normativa, ma anche per la costruzione della fiducia digitale, condizione essenziale per uno sviluppo a lungo termine. L'analisi dei casi concreti conferma che l'efficacia delle soluzioni di Intelligenza Artificiale dipende dalla capacità di inserirle all'interno di un quadro di *governance* chiaro e coerente.

Nel complesso, ciò che emerge da questo lavoro è l'esigenza di superare una visione settoriale della Cybersecurity e della protezione dei dati. La sicurezza digitale si configura come una dimensione trasversale, che attraversa strategia, organizzazione e comunicazione d'impresa. Non si tratta di aggiungere un ulteriore livello di controllo, ma di ripensare il modo in cui le imprese gestiscono il valore informativo e costruiscono relazioni di fiducia nel contesto digitale.

La Cybersecurity e la tutela dei dati personali non rappresentano un limite allo sviluppo tecnologico, ma una condizione essenziale per una trasformazione digitale solida. Solo le imprese capaci di integrare sicurezza, responsabilità e comunicazione in un disegno coerente potranno affrontare in modo consapevole le sfide future, rafforzando la propria legittimità e competitività in un ambiente digitale in continua evoluzione.

BIBLIOGRAFIA

- Ahmad, H. M., & Fahmy, H. M. (2023). *Wireless Sensor Networks: Concepts, Applications, Experimentation and Analysis*. Cham: Springer.
- Andress, J. (2019). The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice (3rd ed.). Syngress, Burlington.
- Bagnoli, C., Bravin, A., & Massaro, M. (2018). Business Model 4.0. Pratiche e strumenti per la trasformazione digitale. Franco Angeli, Milano.
- Bamberger, K., & Mulligan, D. (2015). Privacy on the Ground. MIT Press.
- Brynjolfsson, E., & McAfee, A. (2017). Machine, Platform, Crowd: Harnessing Our Digital Future. Norton, New York.
- Cocolos, E., Mandico, M., & Miceli, G. (2024). Trattamento dei dati personali per imprese, professionisti e amministrazioni (2ª ed.). Maggioli Editore, Santarcangelo di Romagna.
- Custers, B. (2022). Data Protection and Privacy. Springer, Berlin.
- Davenport, T. H., Guha, A., Grewal, D., & Bressgott, T. *How artificial intelligence will change the future of marketing*. *Journal of the Academy of Marketing Science*, 48, (2020).
- Diaferia, L., De Rossi, L. M., & Salviotti, G. (2024). AI Management: Strategie e approcci in azienda. Egea, Milano.
- Dritsas, E., & Trigka, M. (2025). *A Survey on Cybersecurity in IoT*. *Future Internet*, 17(1), Article 30.
- EDPB, Guidelines 1/2020 on the processing operations subject to the requirement of a Data Protection Impact Assessment (DPIA) and accountability principles – Register of processing activities, Version 2.0, 18 Febbraio 2020.
- Finocchiaro, G. (2017). Il nuovo diritto europeo della protezione dei dati personali. Zanichelli, Bologna.
- Garante per la Protezione dei Dati Personali, *Linee guida in materia di applicazione delle sanzioni amministrative pecuniarie ai sensi del GDPR*, 2022.
- Guarda, P. (2019). La trasparenza nel trattamento dei dati. Rivista italiana di informatica e diritto.

- Guarda, P., & Bincoletto, G. (2020). Diritto comparato della privacy e della protezione dei dati personali. Giappichelli, Torino.
- Harvard Business Review Italia [Rivista / eBook]. Harvard Business Publishing Italia.
- Junker, J.-C. (2017). Discorso sullo Stato dell'Unione. Commissione Europea, Bruxelles.
- Kuner, C., Bygrave, L., & Docksey, C. (2020). The EU General Data Protection Regulation (GDPR): A Commentary. Oxford University Press, Oxford.
- Lorè, F., Basile, P., Appice, A., de Gemmis, M., Malerba, D., & Semeraro, G. (2023). *An AI framework to support decisions on GDPR compliance*. *Journal of Intelligent Information Systems*. Springer.
- Malgieri, G., & Comandè, G. (a cura di). (2021). Guida al trattamento e alla sicurezza dei dati personali. Giuffrè Francis Lefebvre, Milano.
- Mandico, M. (2021). Privacy e GDPR. Manuale applicativo con esempi e casistiche settoriali. Maggioli Editore, Santarcangelo di Romagna.
- Moerel, L., & Timmers, P. (2021). GDPR and Cybersecurity: A strategic approach. Computer Law & Security Review.
- Montessoro, P. L. (2019). Cybersecurity: conoscenza e consapevolezza come prerequisiti per l'amministrazione digitale. Maggioli Editore, Rimini.
- Negroponte, N. (1995). Essere digitali. Sperling & Kupfer, Milano.
- NIST (2019). Glossary of Key Information Security Terms. NISTIR 7298 Rev. 3.
- Piccolo, V. S. (2021). Principi e pratiche della Cybersecurity. Apogeo, Milano.
- Pizzetti, G. (2016). Privacy e il diritto europeo alla protezione dei dati personali. Giappichelli, Torino.
- Politecnico di Milano, Osservatorio Cybersecurity & Data Protection. (2023). Rapporto sulla sicurezza ICT in Italia 2023. Politecnico di Milano, School of Management.
- Rivista italiana di informatica e diritto, (2025), **7**(2). Le due facce della rivoluzione digitale, tra emergenze e tecnologie dual-use.
- SEAC (2025). GDPR e Codice Privacy. SEAC, Trento.
- Sun, L. (2021). *Data security governance in the era of big data: Status, challenges, and prospects*. *Computers & Security*.

- Taddeo, M., & Floridi, L. (2018). How AI changes Cybersecurity. Philosophy & Technology, Springer.
- V. Dignum, Responsible Artificial Intelligence: How to Develop and Use AI in a Responsible Way, Springer, (2019).
- Working Party Article 29 Data Protection (WP29), Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation (EU) 2016/679, WP 248 rev. 01, adottate il 4 Aprile 2017.

SITOGRAFIA

- Agenda Digitale, *Cybersecurity e competenze digitali*, https://www.agendadigitale.eu/, consultato nel 2026.

- Agenda digitale, *Impatto del GDPR sulle PMI*, https://www.agendadigitale.eu/tag/cyber-security/, consultato nel 2026.

- Altalex, *Art. 4 GDPR – Definizioni*, https://www.altalex.com/documents/news/2018/04/12/articolo-4-gdpr-definizioni, consultato nel 2026.

- ANSA, *1.411 attacchi cyber nel 2023 in Italia (+29%)*, https://www.ansa.it/canale_tecnologia/notizie/cybersecurity/2024/04/24/1.411-attacchi-cyber-nel-2023-in-italia-aumento-del-29_435a7b61-7006-4054-aea5-15fd6923e8cd.html, consultato nel 2026.

- ANSA, *Il 73% delle grandi aziende italiane colpito da hacker*, https://www.ansa.it/canale_tecnologia/notizie/cybersecurity/2025/02/27/hacker-contro-grandi-aziende-colpito-il-73-delle-italiane_d9e29ef9-9a39-401c-9e27-46361ae21d36.html, consultato nel 2026.

- ANSA, *Raddoppiati gli incidenti cyber in Italia nel 2024*, https://www.ansa.it/sito/notizie/cronaca/2025/05/13/raddoppiati-gli-incidenti-cyber-in-italia-nel-2024_9fc238b1-3537-44d3-9f92-3ea0121d17eb.html, consultato nel 2026.

- ASSO DPO, *Il Data Protection Officer nello sviluppo delle organizzazioni aziendali*, 2 ottobre 2020, https://www.assodpo.it/2020/10/02/il-data-protection-officer-nello-sviluppo-delle-organizzazioni-aziendali/, consultato nel 2026.

- AziendaBanca, *GDPR: calo del 33% delle sanzioni in Europa*, *https://www.aziendabanca.it/notizie/banche/report-dla-piper-gdpr-in-italia-sanzioni-per-237-milioni*, consultato nel 2026.

- Carmignani Consulenza, *Sanzione del Garante privacy per trattamento illecito di dati a fini di marketing*, 18 aprile 2023, https://carmignaniconsulenza.com/2023/04/18/il-garante-privacy-ha-sanzionato-una-societa-che-offre-servizi-di-digital-marketing-con-una-multa-di-300mila-euro-per-aver-trattato-in-modo-illecito-dati-personali-a-fini-di-marketing-garante-della/, consultato nel 2026.

- Clusit, *Anteprima Rapporto Clusit 2025*, https://clusit.it/wpcontent/uploads/area_stampa/2025/Anteprima_Rapporto_Clusit_2025.pdf, consultato nel 2026.

- Clusit, *Rapporto sulla sicurezza ICT in Italia 2025*, https://clusit.it/rapporto-clusit/, consultato nel 2026.

- CMS Law, *GDPR Enforcement Tracker Report – Italy*, 2024, https://www.enforcementtracker.com/, consultato nel 2026.

- CNPD, *CNPD imposes fine of EUR 746 million on Amazon Europe*, https://cnpd.public.lu/en/actualites/national/2025/03/amazon-decision.html, 2025.

- CookieHub, *Che cos'è la CNIL*, https://www.cookiehub.com/it/blog/che-cose-la-cnil, consultato nel 2026.

- Cybersecurity360, *Investimenti cyber e benefici del GDPR*, https://www.cybersecurity360.it/news/investimenti-cyber-e-benefici-del-gdpr-uneconomia-che-fa-bene-alle-aziende/, consultato nel 2026.

- Cybersecurity Italia, *Attacchi cyber in Italia nel primo semestre 2025*, https://www.cybersecitalia.it/attacchi-cyber-in-italia-53-gli-eventi-nel-primo-semestre-2025-tra-i-settori-piu-colpiti-pa-telco-ed-energia/49790/, consultato nel 2026.

- ECC Net Italia, *Violazione del GDPR e diritto al risarcimento*, https://ecc-netitalia.it/it/news/violazione-del-regolamento-privacy-la-corte-di-giustizia-ue-chiarisce-quando-e-possibile-ottenere-un-risarcimento/, consultato nel 2026.

- EU News, *Atto UE sull'intelligenza artificiale: entrata in vigore*, https://www.eunews.it/2024/08/01/atto-ue-intelligenza-artificiale-vigore/, 2024.

- EY – Brand News, *La metà delle imprese italiane non è pronta per la nuova normativa privacy*, https://brand-news.it/intelligence/normative/privacy-ricerche-ey/, consultato nel 2026.

- Garante per la protezione dei dati personali, *Approccio basato sul rischio e misure di accountability di titolari e responsabili*, https://www.garanteprivacy.it/regolamentoue/approccio-basato-sul-rischio-e-misure-di-accountability-responsabilizzazione-di-titolari-e-responsabili, consultato il 10 dicembre 2025.

- Gruppo Ferrovie dello Stato Italiane, *Rapporto di sostenibilità 2023*, Roma, 2023, https://www.fsitaliane.it/content/dam/fsitaliane/Documents/sostenibilit%C3%A0/rapporto-di-sostenibilit%C3%A0-2023/rapporto-di-sostenibilita-2023-gruppo-fs.pdf

- IBM Security – Ponemon Institute, *Cost of a Data Breach Report 2025*, https://www.ibm.com/it-it/reports/data-breach, 2025.

- Innovation Post, *Quanto costano le intrusioni informatiche in Italia*, https://www.innovationpost.it/tecnologie/industrial-security/quanto-costano-le-intrusioni-informatiche-in-italia-ben-437-milioni-di-euro-in-media-oltre-5-milioni-per-le-aziende-industriali/, consultato nel 2026.

- Innovation Post, *Spesa per cybersecurity in aumento del 60%: previsioni 2025*, https://www.innovationpost.it/tecnologie/industrial-security/cyber-security-aumenta-la-spesa-ma-si-perdono-ancora-troppi-dati-ecco-perche-i-sistemi-tradizionali-di-protezione-non-funzionano/, consultato nel 2026.

- Key4Biz, *Sanzioni GDPR dal 2018 ad oggi*, https://www.key4biz.it/gpdr-dal-2018-ad-oggi-sanzioni-per-61-miliardi-di-euro-italia-al-secondo-posto-per-numero-di-multe/532356/, consultato nel 2026.

- LavoroDirittiEuropa.it, *Le discriminazioni algoritmiche,* https://www.lavorodirittieuropa.it/dottrina/principi-e-fonti/1524-le-discriminazioni-algoritmiche, consultato nel 2026.

- Lavoro Diritti Europa, *Intelligenza artificiale, trasparenza e tutela dei dati aziendali*, https://www.lavorodirittieuropa.it/dottrina/principi-e-fonti/1693-intelligenza-artificiale-trasparenza-e-tutela-dei-dati-aziendali, consultato nel 2026.

- Luxtimes, *Amazon Europe fined €746 million for data protection breaches*, https://www.luxtimes.lu/businessandfinance/amazon-europe-fined-746-mn-for-data-protection-breaches/50260710.html, consultato nel 2026.

- Poste Italiane S.p.A., *Bilancio di sostenibilità e gestione dei dati*, https://www.posteitaliane.it/it/bilanci-e-relazioni.html#/, consultato nel 2026.

- Punto Impresa Digitale – Unioncamere, *Zero-LAI: l'intelligenza artificiale che trasforma i dati in decisioni in tempo reale*, 2024, https://www.puntoimpresadigitale.camcom.it/.

- The European House – Ambrosetti, *InnoTech Report 2023*, https://www.ambrosetti.eu/innotech-hub/technology-forum-2023/, 2023.

FONTI NORMATIVE

Normative europee

- Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali e alla libera circolazione di tali dati (Regolamento generale sulla protezione dei dati – GDPR).

- Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA e alla certificazione della cibersicurezza delle tecnologie dell'informazione e della comunicazione (Cybersecurity Act).

- Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali e alla libera circolazione di tali dati.

- Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva ePrivacy).

- Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione (direttiva NIS 2).

- Commissione europea, Proposta di regolamento del Parlamento europeo e del Consiglio relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali (Cyber Resilience Act), COM (2022) 454 final, Bruxelles.

- Parlamento europeo e Consiglio dell'Unione europea. (2016). *Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali e alla libera circolazione di tali dati (Regolamento generale sulla protezione dei dati)*. *Gazzetta Ufficiale dell'Unione europea* L 119. EUR-Lex.

Linee guida

- European Data Protection Board (EDPB), *Guidelines 1/2020 on processing operations subject to the requirement of a Data Protection Impact Assessment (DPIA)*, versione 2.0, 18 Febbraio 2020.

- Article 29 Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk"*, WP 248 rev. 01, 4 Aprile 2017.

- Garante per la protezione dei dati personali, *Linee guida in materia di applicazione delle sanzioni amministrative pecuniarie ai sensi del Regolamento (UE) 2016/679*, 2022.

- Unione europea. (2016). *EUR-Lex – Regolamento generale sulla protezione dei dati (GDPR), testo consolidato e definizioni*. EUR-Lex.

- European Data Protection Board. (2020). *Guidelines 07/2020 on the concepts of controller and processor in the GDPR* (Version 2.0). European Data Protection Board.

- European Data Protection Board. (2023). *Guidelines 01/2022 on data subject rights (Version 2.1)*. EDPB.

- ENISA – European Union Agency for Cybersecurity. (2024). *Technical implementation guidance on cybersecurity risk management measures (Version 1.0)*.

Normative nazionali

- Decreto legislativo 30 giugno 2003, n. 196, *Codice in materia di protezione dei dati personali*, come modificato dal decreto legislativo 10 agosto 2018, n. 101.

- Legge 25 ottobre 2017, n. 163, *Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea* (legge di delegazione europea 2016–2017).
- Costituzione della Repubblica italiana, art. 2.

Standard tecnici e testi di supporto

- National Institute of Standards and Technology (NIST), *Glossary of Key Information Security Terms*, NISTIR 7298 Rev. 3, 2019.

- SEAC, *GDPR e Codice Privacy*, Trento, 2025.

Interventi istituzionali

- Juncker J.-C., *Discorso sullo Stato dell'Unione*, Commissione europea, Bruxelles, 2017.