UNIVERSITA' DEGLI STUDI DI ROMA TOR VERGATA

***European Digital Law of the Person, of the Contract and of the Technological Marketplace* - EUDILA**
Cattedra Jean Monnet del Progetto ERASMUS +

IL DATA BREACH TRA OBBLIGHI NORMATIVI E STRUMENTI DI ACCOUNTABILITY

Un equilibrio tra tutela e responsabilità nel diritto privato digitale

Riccardo Ceoldo

0359982

Anno accademico 2024/2025

Indice

1. Introduzione

Nell'era dell'informazione e della digitalizzazione spinta, la protezione dei dati personali è diventata una delle principali preoccupazioni delle istituzioni, delle imprese e dei cittadini. Le violazioni della sicurezza informatica, meglio note come "data breach", rappresentano oggi un rischio trasversale, in grado di compromettere diritti fondamentali, relazioni contrattuali e la fiducia nei servizi digitali.

Questa tesina intende esaminare in modo esteso e critico il fenomeno dei data breach attraverso una lente multidisciplinare che coniuga diritto digitale, ingegneria gestionale e responsabilità civile. Verrà approfondito il quadro normativo europeo e nazionale, con particolare attenzione al Regolamento (UE) 2016/679 (GDPR), agli obblighi di notifica e alle misure preventive previste. Saranno inoltre esaminati i dati sanitari e il nuovo assetto regolatorio europeo disegnato dal progetto EHDS (European Health Data Space), nonché gli strumenti privatistici di controllo e tutela.

Il fine è proporre una visione organica della responsabilità da data breach nel diritto privato digitale, valorizzando i concetti di accountability, trasparenza e prevenzione.

2. Il fenomeno del data breach: definizione, tipologie e contesto digitale

Il concetto di "data breach" rappresenta uno dei nodi critici nella riflessione giuridica e organizzativa sul trattamento dei dati personali. In un'epoca dominata dalla digitalizzazione e dall'interconnessione, le violazioni della sicurezza dei dati costituiscono eventi sempre più frequenti, con conseguenze gravi tanto per i soggetti interessati quanto per le organizzazioni responsabili. Analizzarne natura, classificazione e diffusione è fondamentale per comprenderne l'impatto sistemico e per progettare misure efficaci di prevenzione e gestione.

2.1 Definizione e classificazione delle violazioni di dati personali

Il Regolamento (UE) 2016/679, noto come GDPR, definisce il data breach all'art. 4, n. 12 come:

"la violazione di sicurezza che comporta, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati".

Questa definizione evidenzia la pluralità di scenari in cui si può configurare un data breach. Non si tratta solo di attacchi esterni (come il cybercrime), ma anche di errori umani, malfunzionamenti tecnici o mancanza di misure adeguate.

Classificazione principale:

- Violazione della confidenzialità: accesso o divulgazione non autorizzata dei dati personali.
- Violazione dell'integrità: alterazione non autorizzata dei dati.
- Violazione della disponibilità: perdita di accesso ai dati o loro distruzione.

Esempi tipici includono:

- Furto di dati tramite ransomware.
- Smarrimento di dispositivi contenenti dati personali.
- Email inviate per errore a destinatari sbagliati.
- Accessi non autorizzati da parte di dipendenti.

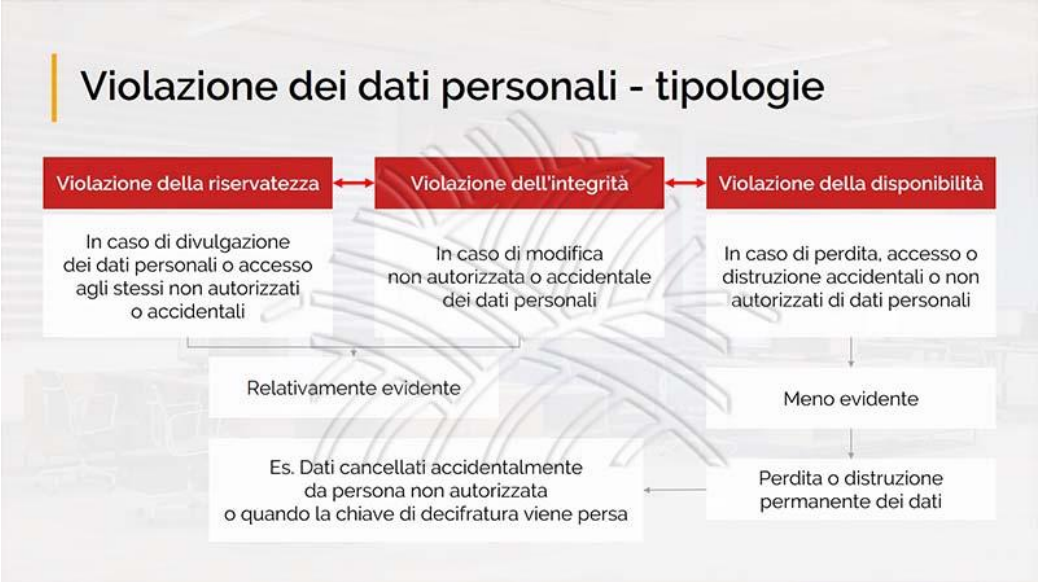

Figura 1 - Tipologie violazione dei dati personali

2.2 Fattori di rischio e ambiti maggiormente esposti

I fattori che aumentano il rischio di data breach possono essere distinti in tecnologici, organizzativi, umani e giuridici. Tra i più rilevanti si segnalano:

- Infrastrutture obsolete o non aggiornate.
- Scarsa formazione del personale.
- Assenza di protocolli di sicurezza o gestione delle crisi.
- Elevata esposizione online dei sistemi (es. cloud, API, IoT).
- Trattamento di dati ad alta sensibilità, come quelli sanitari, biometrici o bancari.

Settori più colpiti:

- Sanità: gestione di dati sensibili e sistemi interconnessi.
- Finanza e assicurazioni: dati patrimoniali, transazioni.
- Pubblica amministrazione: banche dati personali e identità digitale.

- E-commerce e social media: abitudini di consumo e dati di localizzazione.

VOLUME DEI DATI VIOLATI	
Numero di record di identificazione completi	*Punteggio attribuito*
Meno di 100	1
Tra 100 e 1.000	2
Tra 1.000 e 100.000	3
Tra 100.000 e 1.000.000	4
Oltre 1.000.000	5

TIPOLOGIA DI DATI VIOLATI	
Tipologia di dato personale	*Punteggio attribuito*
Dato personale comune	1
Dato sensibile/particolare	2

IMPATTO DELLA VIOLAZIONE	
Grado di divulgazione	*Punteggio attribuito*
Nessuna divulgazione	2
Interna all'organizzazione, controllata	4
Esterna all'organizzazione	6
Pubblica (es. divulgazione su Internet)	8
Sconosciuta	10

Figura 2 - Valutazione del rischio di un data breach

2.3 Analisi statistica del fenomeno: incidenza e conseguenze

L'aumento esponenziale dei data breach è stato documentato da numerosi report, tra cui quelli dell'ENISA (European Union Agency for Cybersecurity) e del Comitato Europeo per la Protezione dei Dati (EDPB).

Trend recenti:

- Nel 2023, sono stati notificati oltre 130.000 data breach in UE dal 2018, con una crescita media del 20% annuo.
- I tempi medi di risposta delle organizzazioni sono ancora critici: solo il 60% rispetta il termine di 72 ore imposto dal GDPR.
- Il costo medio di un data breach, secondo IBM, è di 4,45 milioni di dollari a livello globale, con valori maggiori nel settore sanitario.

Conseguenze principali per le organizzazioni:

- Sanzioni amministrative (fino al 4% del fatturato).
- Perdita di reputazione e fiducia da parte dei clienti.

- Danni contrattuali e azioni di responsabilità civile.
- Interruzioni operative e perdite economiche.

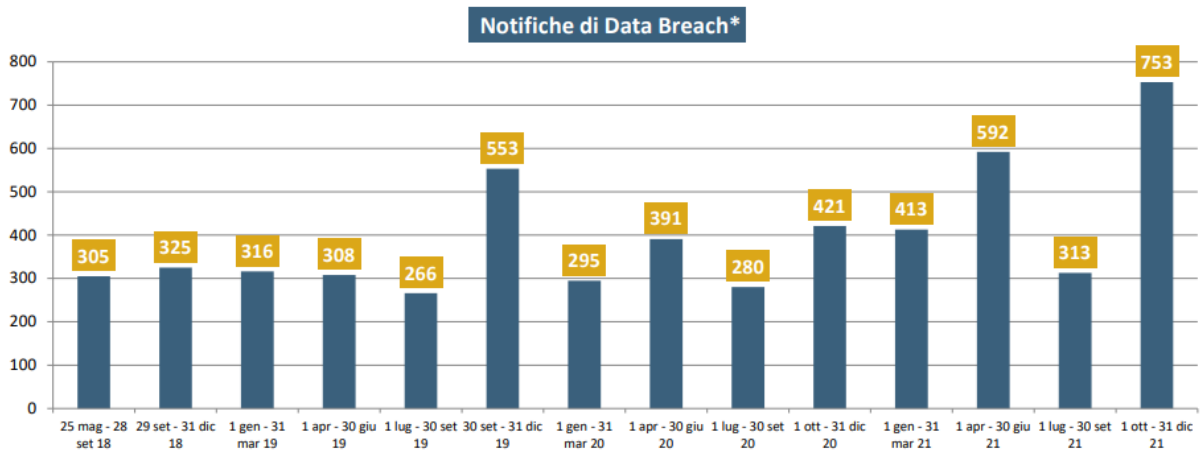

Figura 3 - Notifiche di data breach in vari periodi temporali - bilancio GDPR

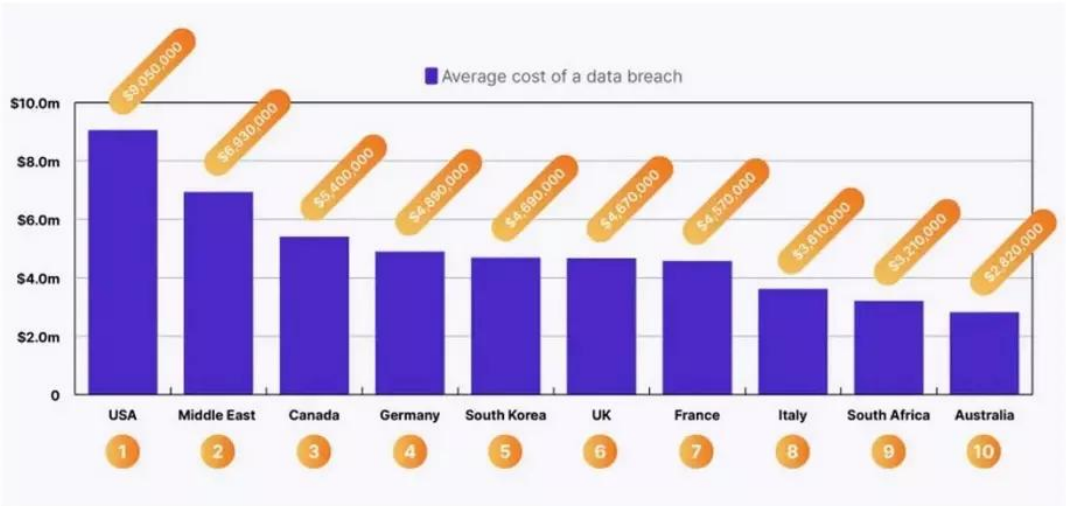

Figura 4 - Costo medio per ciascun data breach

3. Obblighi normativi e strumenti di accountability: quadro regolatorio e implementazione pratica

Il sistema di protezione dei dati personali introdotto dal GDPR si fonda su un equilibrio tra obblighi normativi rigorosi e una chiara attribuzione di responsabilità (accountability) ai soggetti che trattano i dati. In questo capitolo analizzeremo le principali disposizioni in materia di data breach e gli strumenti pratici che permettono di adempiere in modo efficace ai doveri imposti, valorizzando la responsabilizzazione attiva degli operatori del trattamento.

3.1 Il GDPR e la gestione dei data breach

Il GDPR rappresenta un punto di svolta nella regolamentazione della protezione dei dati in Europa, ponendo grande enfasi sulla gestione delle violazioni. Le norme fondamentali in materia di data breach sono contenute negli articoli 33 e 34 del Regolamento.

- **Art. 33 GDPR – Notifica all'autorità di controllo:**

Impone al titolare del trattamento l'obbligo di notificare la violazione all'autorità competente (in Italia: il Garante per la protezione dei dati personali) entro 72 ore, salvo che sia improbabile che il data breach comporti un rischio per i diritti e le libertà delle persone fisiche.

- **Art. 34 GDPR – Comunicazione all'interessato:**

Se la violazione è tale da comportare un rischio elevato per i diritti e le libertà dell'interessato, il titolare deve informarlo senza ingiustificato ritardo, indicando le conseguenze probabili e le misure adottate o proposte per porvi rimedio.

Il rispetto di tali obblighi non è solo una misura formale, ma incide anche sulla valutazione del comportamento diligente del titolare in caso di contenzioso o sanzione.

3.2 Il principio di responsabilizzazione e le misure tecniche-organizzative

Uno dei principi cardine del GDPR è quello della responsabilizzazione (art. 5, par. 2 – Accountability), secondo cui il titolare non solo deve rispettare i principi di protezione dei dati, ma

deve anche essere in grado di dimostrarne il rispetto.

Questo implica un cambio culturale: non bastano misure minime, ma è necessario adottare un approccio proattivo e documentato alla sicurezza dei dati.

Misure richieste:

- Cifratura e pseudonimizzazione dei dati.
- Controlli di accesso basati sui ruoli.
- Backup frequenti e ridondanze.
- Procedure di audit periodico.
- Piani di risposta agli incidenti (incident response plans).

Figura 5 - Ciclo di gestione del rischio

Queste misure devono essere commisurate al rischio e alla natura del trattamento, secondo il principio di privacy by design e by default (art. 25 GDPR).

3.3 DPIA, DPO e registro dei trattamenti come strumenti operativi

Il GDPR introduce strumenti operativi concreti per dare attuazione alla responsabilizzazione.

- DPIA (Data Protection Impact Assessment) – Valutazione d'impatto sulla protezione dei dati (art. 35):

Obbligatoria nei casi di trattamenti ad alto rischio, come quelli che coinvolgono dati sensibili su larga scala, profilazione automatizzata o monitoraggio sistematico. La DPIA consente di valutare in anticipo i rischi e le misure per mitigarli.

- DPO – Data Protection Officer (art. 37-39):

Figura obbligatoria per enti pubblici e soggetti che trattano dati su larga scala. Il DPO ha il compito di vigilare sulla conformità normativa, fornire consulenza e fungere da punto di contatto con l'autorità di controllo.

- Registro dei trattamenti (art. 30):

Obbligatorio per tutte le organizzazioni con più di 250 dipendenti o per trattamenti non occasionali. Consente una mappatura chiara dei flussi di dati e delle responsabilità interne.

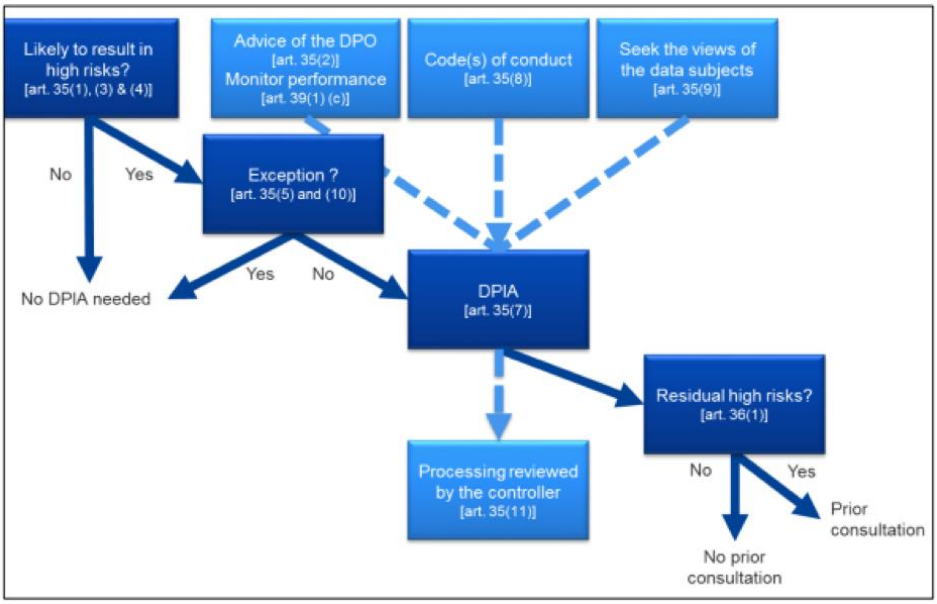

Figura 6 - DPIA flowchart

3.4 Obblighi di notifica e comunicazione: casi studio e prassi applicativa

Nella prassi, la corretta gestione di un data breach comporta la necessità di adottare una procedura interna efficace e verificabile. Gli studi di caso mostrano come il rispetto degli obblighi di notifica sia un elemento centrale nella valutazione della responsabilità del titolare.

Esempio 1: Ente sanitario regionale italiano (2022)

Un attacco ransomware ha colpito il sistema informativo di un'ASL, bloccando l'accesso ai referti dei pazienti. L'ente ha notificato entro 72 ore il Garante e ha successivamente informato tutti gli interessati. La gestione tempestiva ha evitato sanzioni.

Esempio 2: Azienda tech europea (2023)

Data breach per errata configurazione di un database cloud. Nessuna notifica effettuata. Il Garante ha accertato grave negligenza e ha comminato una sanzione da 2 milioni di euro.

4. Il trattamento dei dati sanitari e la governance europea del dato: tra tutela e innovazione

La gestione dei dati sanitari rappresenta una delle aree più sensibili e complesse della protezione dei dati personali, in quanto tali dati rientrano tra le categorie particolari previste dall'art. 9 del GDPR e sono fortemente tutelati per la loro potenziale incidenza sulla dignità, la riservatezza e la libertà personale degli individui. In questo contesto, si inserisce il progetto europeo EHDS (European Health Data Space), che mira a creare un ecosistema armonizzato per il trattamento dei dati sanitari primari e secondari, incentivando ricerca, innovazione e governance etica.

4.1 La natura dei dati sanitari: definizione e criticità

Secondo l'art. 4, par. 15 del GDPR, per "dati relativi alla salute" si intendono i dati personali attinenti alla salute fisica o mentale di una persona, incluse informazioni sulla prestazione di servizi sanitari che rivelano informazioni sullo stato di salute.

Tali dati sono soggetti a una tutela rafforzata e il loro trattamento è vietato in linea generale, salvo il ricorrere di specifiche condizioni indicate all'art. 9, come il consenso esplicito, motivi di interesse pubblico o finalità mediche legittime.

Criticità principali:

- Elevata sensibilità e rischio di discriminazione (es. condizioni patologiche, disabilità, dati genetici).
- Necessità di interoperabilità tra sistemi sanitari.
- Difficoltà nel garantire l'anonimizzazione efficace dei dati.
- Ampia platea di soggetti coinvolti (medici, ospedali, software provider, laboratori, PA).

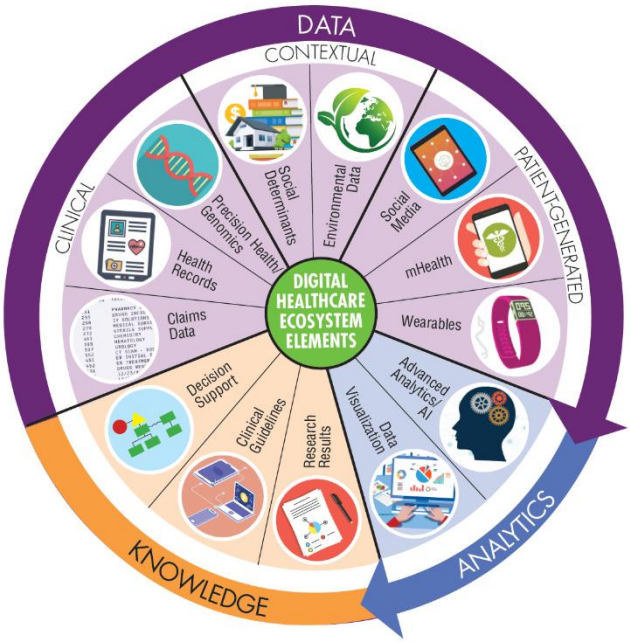

Figura 7 - Ecosistema sanitario digitale

4.2 EHDS (European Health Data Space): obiettivi, struttura e implicazioni giuridiche

Il **Regolamento sull'EHDS**, proposto dalla Commissione Europea nel 2022, è un'iniziativa cardine per la creazione di un vero e proprio spazio europeo dei dati sanitari. Esso si inserisce nel quadro più ampio della European Strategy for Data e mira a:

- Facilitare **l'accesso transfrontaliero** ai dati sanitari elettronici per i cittadini dell'UE.
- Promuovere l'utilizzo secondario dei dati sanitari per scopi di **ricerca scientifica, innovazione, politiche sanitarie e sicurezza dei medicinali**.
- Creare infrastrutture sicure e interoperabili tra Stati membri (es. HealthData@EU).
- Rafforzare il controllo individuale attraverso diritti digitali specifici (accesso, rettifica, restrizione, tracciabilità degli accessi).

Implicazioni giuridiche:

- Introduzione di **obblighi per i fornitori di EHR (cartelle cliniche elettroniche)**.
- Nuovi diritti informatici in ambito sanitario (opt-out, gestione granularità dati).

- Interazione e coordinamento con le norme GDPR: l'EHDS specifica ma non sostituisce le tutele generali.

Figura 8 - European Health Data Space

4.3 Etica, interoperabilità e sicurezza: un nuovo equilibrio tra ricerca e privacy

La complessa sfida dell'EHDS è trovare un bilanciamento tra **utilità pubblica dei dati** e **tutela dei diritti individuali**. A tal fine, il regolamento prevede:

- **Condizioni stringenti per l'accesso secondario ai dati**, attraverso organismi autorizzati e previa richiesta motivata.
- **Pseudonimizzazione obbligatoria** per i dati utilizzati a fini di ricerca.
- **Tracciabilità degli accessi e audit periodici** da parte delle autorità nazionali.
- **Linee guida etiche europee** per evitare discriminazioni e abusi.

In termini di interoperabilità, l'adozione di **formati comuni europei (EHDSI)** e l'obbligo per i sistemi sanitari digitali di garantire la portabilità dei dati rappresentano un avanzamento significativo.

Opportunità emergenti:

- Promozione di progetti di intelligenza artificiale in ambito diagnostico.
- Condivisione sicura dei dati per studi epidemiologici e politiche sanitarie.
- Sviluppo di gemelli digitali per simulazioni terapeutiche personalizzate.

Tabella 1 - Confronto GDPR - EHDS

	GDPR	EHDS
Finalità	Protezione dei dati personali in tutti i settori; garantisce diritti come trasparenza, minimizzazione, sicurezza, controllo individuale.	Garantire accesso immediato e interoperabile ai dati sanitari elettronici; favorire il riutilizzo per ricerca, sanità pubblica, innovazione.
Ambito di Applicazione	Tutti i trattamenti di dati personali all'interno o collegati all'UE, in ogni settore.	Solo dati sanitari elettronici, con due usi distinti: primario (assistenza) e secondario (ricerca, policy).
Titolarità del Trattamento	Titolari e responsabili del trattamento secondo scopi e mezzi determinati.	Introdotti nuovi ruoli: data holder, Health Data Access Body (HDAB), trusted data user, ognuno con compiti specifici.
Diritti degli Interessati	Accesso, rettifica, cancellazione, portabilità, opposizione, limitazione.	Accesso immediato, restrizioni accesso ai professionisti, portabilità transfrontaliera, opt-out per uso secondario.
Strumenti di Garanzia	DPIA, misure tecniche e organizzative, certificazioni, sanzioni fino al 4% del fatturato.	HDAB, ambienti sicuri di trattamento (SPE), standard interoperabilità (EHR).
Sanzioni	Fino al 4% del fatturato globale annuo o 20 milioni di euro.	Idem, con focus aggiuntivo su obblighi specifici per enti sanitari e organismi designati.

5. Tutela civilistica e responsabilità nel diritto privato digitale

La violazione dei dati personali non comporta solo un illecito amministrativo o penale, ma può anche costituire una fonte di responsabilità civilistica. Il diritto privato digitale si confronta con nuove categorie di danno e forme di responsabilità legate alla gestione impropria dei dati, richiedendo un adattamento continuo degli strumenti giuridici tradizionali. In questo capitolo verranno esaminate le principali implicazioni civilistiche derivanti da un data breach, con riferimento alla responsabilità contrattuale, extracontrattuale, alla prova del danno e agli strumenti di prevenzione e gestione.

5.1 Il danno da data breach tra responsabilità contrattuale ed extracontrattuale

Il danno da data breach può configurare sia una **responsabilità contrattuale** che una **responsabilità aquiliana** (ex art. 2043 c.c.). Il discrimine principale è costituito dall'esistenza di un rapporto contrattuale tra l'interessato e il titolare del trattamento.

- In presenza di contratto (es. cliente di una banca, paziente di una clinica privata), l'inadempimento agli obblighi di protezione dei dati personali può configurare una **violazione contrattuale** (art. 1218 c.c.).
- In assenza di rapporto diretto, il danno può essere azionato in via **extracontrattuale** (art. 2043 c.c.), se sussiste un comportamento illecito e un nesso causale con il danno subito.

5.2 La prova del danno e il ruolo della giurisprudenza

Uno degli aspetti più complessi nei giudizi di risarcimento danni per violazione dei dati è la **prova del danno**. Il GDPR (art. 82) riconosce il diritto al risarcimento per "qualsiasi danno subito", compresi quelli **non patrimoniali**, come stress, ansia, perdita della reputazione o senso di insicurezza.

La Corte di Giustizia UE, nella sentenza C-300/21, ha chiarito che:

- Non è necessaria la gravità del danno per poter ottenere un risarcimento.

- Il danno può essere anche minimo, purché effettivo e dimostrato.
- L'onere della prova incombe sull'interessato, ma i giudici nazionali devono applicare principi di effettività e proporzionalità.

Giurisprudenza italiana:

- Cass. civ. 1282/2020 ha riconosciuto un danno da violazione della riservatezza anche in assenza di danno patrimoniale.
- Trib. Roma, sent. 6013/2022: riconosciuto danno morale a favore di un paziente per accesso abusivo a cartella clinica.

Tabella 2 - confronto tra responsabilità contrattuale ed extracontrattuale in ambito data breach

	Responsabilità Contrattuale	**Responsabilità Extracontrattuale**
Oneri Probatori	Il creditore deve provare l'inadempimento contrattuale e il danno. Il debitore deve dimostrare che l'inadempimento non è a lui imputabile (art. 1218 c.c.).	Il danneggiato deve provare il fatto illecito, il danno subito e il nesso causale tra illecito e danno (art. 2043 c.c.).
Danni Risarcibili	Danni patrimoniali e non patrimoniali se prevedibili al momento della stipula del contratto (art. 1223-1225 c.c.).	Danni patrimoniali e non patrimoniali, anche se imprevedibili, se derivanti da fatto illecito (art. 2059 c.c.).
Termini di Prescrizione	10 anni dalla data in cui si verifica l'inadempimento o si ha conoscenza del danno.	5 anni dalla data in cui si verifica il fatto illecito o si ha conoscenza del danno (art. 2947 c.c.).

5.3 Gli strumenti privatistici di prevenzione: assicurazioni, accordi, clausole

Accanto agli obblighi legali, le aziende e i titolari del trattamento possono adottare strumenti di **autotutela contrattuale** per limitare i rischi derivanti da data breach.

Principali strumenti:

- **Data Processing Agreements (DPA)**: accordi tra titolare e responsabile che disciplinano le misure di sicurezza, audit, diritti degli interessati.
- **Clausole di manleva e limitazione di responsabilità** nei contratti con fornitori IT e cloud.
- **Polizze assicurative contro rischi informatici (cyber risk insurance)**: coprono spese legali, notifiche, danni patrimoniali, assistenza tecnica.

L'utilizzo consapevole di tali strumenti è parte integrante della strategia di accountability e risk management aziendale.

5.4 Esempi e best practices di gestione responsabile

Per favorire una cultura della responsabilità digitale, è utile analizzare alcune **best practices** e casi virtuosi di gestione dei data breach:

- **Azienda farmaceutica multinazionale**: implementazione di un sistema di alert in tempo reale, team interno di incident response, audit semestrali. Nessun data breach negli ultimi 3 anni.
- **Ospedale pubblico italiano**: attivazione protocollo DPIA e formazione obbligatoria per tutti i medici sull'accesso lecito ai dati. Riduzione del 60% degli incidenti rispetto al 2020.

5.5 Case Study - Data Breach Regione Lazio 2021:

Nel mese di agosto 2021, la Regione Lazio è stata vittima di uno dei più gravi attacchi informatici in ambito sanitario italiano, con un impatto diretto su dati sensibili e infrastrutture critiche. L'attacco, di tipo ransomware, ha compromesso i sistemi informatici centrali del Centro Elaborazione Dati (CED) regionale, bloccando l'accesso a numerosi servizi, tra cui il portale di prenotazione per le vaccinazioni anti-COVID-19, la consultazione dei referti digitali e altri servizi sanitari e amministrativi.

L'accesso illecito è avvenuto attraverso un account di amministratore VPN privo di autenticazione multifattoriale (MFA), consentendo agli attaccanti di cifrare gran parte dei dati e rendere inoperativi

i servizi online. L'interruzione ha generato gravi disagi per migliaia di cittadini, oltre a sollevare preoccupazioni per la possibile esfiltrazione di dati sanitari, anche se tale circostanza non è stata ufficialmente confermata.

Le indagini sono state condotte con il supporto della Polizia Postale, del CERT-PA e dell'Agenzia per la Cybersicurezza Nazionale, in collaborazione con fornitori di servizi IT. L'attacco ha messo in evidenza diverse carenze in termini di sicurezza, tra cui la mancata implementazione di adeguate misure tecniche e organizzative previste dall'articolo 32 del GDPR.

Sul piano giuridico, la Regione Lazio, quale titolare del trattamento, è stata tenuta a rispettare gli obblighi di notifica al Garante per la protezione dei dati personali (art. 33 GDPR) e, ove necessario, agli interessati (art. 34 GDPR). Il trattamento di dati sanitari, appartenenti a categorie particolari ai sensi dell'art. 9 GDPR, impone una maggiore attenzione nella valutazione e gestione del rischio, anche tramite strumenti come la DPIA (Data Protection Impact Assessment).

In risposta all'incidente, sono state adottate misure correttive tra cui l'introduzione dell'autenticazione a due fattori, il rafforzamento dei piani di continuità operativa e disaster recovery, la crittografia dei dati, nonché campagne di sensibilizzazione e formazione del personale. L'attacco alla Regione Lazio ha rappresentato un caso emblematico della vulnerabilità del settore sanitario e ha spinto molte altre pubbliche amministrazioni italiane a rivedere i propri standard di sicurezza informatica.

6. Conclusioni: verso una cultura della protezione e responsabilità digitale

La presente analisi ha evidenziato la crescente centralità del fenomeno del data breach nel contesto della società digitale, in particolare per quanto riguarda l'interazione tra obblighi normativi, strumenti di accountability e tutele privatistiche. La trasformazione digitale, se da un lato ha offerto nuove opportunità in termini di efficienza, interoperabilità e accessibilità dei dati, dall'altro ha aumentato esponenzialmente i rischi legati alla sicurezza e alla protezione delle informazioni personali.

In tale contesto, il Regolamento Generale sulla Protezione dei Dati (GDPR) si configura come il pilastro normativo su cui si fonda la responsabilità dei soggetti che trattano dati, imponendo obblighi puntuali e promuovendo il principio di accountability. La responsabilizzazione del titolare del trattamento non è meramente formale, ma sostanziale: implica l'adozione di un approccio proattivo, fondato sulla prevenzione, la documentazione e l'analisi del rischio.

Particolare attenzione è stata dedicata alla gestione dei dati sanitari, che richiedono tutele rafforzate per la loro natura altamente sensibile. L'introduzione dell'EHDS (European Health Data Space) rappresenta un ulteriore sviluppo significativo, volto a costruire un ecosistema europeo sicuro e interoperabile per la condivisione dei dati sanitari, senza compromettere la privacy degli individui. Questo processo, tuttavia, solleva nuove sfide di natura tecnica, etica e giuridica che richiederanno una costante vigilanza e aggiornamento normativo.

La responsabilità derivante da un data breach non si esaurisce nel perimetro del diritto pubblico. Come emerso nell'analisi civilistica, la violazione dei dati può comportare danni patrimoniali e non patrimoniali, attivando meccanismi di risarcimento in sede giudiziaria, sia contrattuale che extracontrattuale. L'evoluzione giurisprudenziale mostra un crescente riconoscimento della rilevanza del danno immateriale e della necessità di tutelare la dimensione digitale dell'identità personale.

Accanto agli strumenti normativi, le aziende devono adottare buone pratiche di gestione del rischio, tra cui la stipula di contratti specifici, l'adozione di polizze assicurative informatiche e la promozione di una cultura aziendale fondata sulla sicurezza digitale. La formazione del personale, i test di penetrazione periodici, i piani di continuità operativa e la trasparenza nei confronti degli utenti sono tutti elementi essenziali di un modello di accountability maturo.

Infine, la sfida della protezione dei dati deve essere affrontata in chiave sistemica, attraverso la collaborazione tra autorità, imprese, professionisti e cittadini. Solo una governance distribuita, etica e tecnologicamente avanzata potrà garantire un equilibrio duraturo tra innovazione digitale e tutela dei diritti fondamentali.

Con questa conclusione si chiude la trattazione, che ha cercato di coniugare un approccio normativo, tecnico e applicativo alla problematica del data breach. La direzione futura sarà quella di rafforzare ulteriormente la resilienza digitale delle organizzazioni e la consapevolezza degli individui, in una prospettiva integrata di tutela e responsabilità.

7. BIBLIOGRAFIA

- Clarich, M. (2021). La responsabilità civile nel trattamento dei dati personali. Rivista di diritto civile, Giuffrè.

- Corte di Giustizia dell'Unione Europea. (2023). UI v Österreichische Post AG, C-300/21.

- Deloitte. (2022). Cyber risk in healthcare: a growing concern. Deloitte Insights.

- ENISA. (2024). Threat Landscape Report 2023. European Union Agency for Cybersecurity.

- European Commission. (2022). Proposal for a Regulation on the European Health Data Space (EHDS). COM(2022) 197 final.

- Finocchiaro, G. (2023). Manuale di diritto privato digitale. Giuffrè Editore.

- Garante per la protezione dei dati personali. (2023). Documenti e Linee guida sul trattamento dei dati personali.

- IBM Security. (2023). Cost of a Data Breach Report.

- Malgieri, G. (2022). Dalla privacy alla governance dei dati: il principio di accountability nel GDPR. Diritto dell'informazione e dell'informatica.

- Pizzetti, F. (2019). Privacy e il nuovo diritto europeo della protezione dei dati. Giappichelli.

- Unione Europea. (2016). Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016. Gazzetta ufficiale dell'Unione europea.