

IPSOA In **Pratica**



**PRIVACY
E DATA
PROTECTION**

2022



**PRIVACY
E DATA
PROTECTION**

2022

Copyright 2022 Wolters Kluwer Italia S.r.l.
Via dei Missaglia n. 97 - Edificio B3 - 20142 Milano

I diritti di traduzione, di memorizzazione elettronica, di riproduzione e di adattamento totale o parziale, con qualsiasi mezzo (compresi i microfilm e le copie fotostatiche), sono riservati per tutti i Paesi.

Le fotocopie per uso personale del lettore possono essere effettuate nei limiti del 15% di ciascun volume/fascicolo di periodico dietro pagamento alla SIAE del compenso previsto dall'art. 68, commi 4 e 5, della legge 22 aprile 1941, n. 633. Le riproduzioni diverse da quelle sopra indicate (per uso non personale - cioè, a titolo esemplificativo, commerciale, economico o professionale - e/o oltre il limite del 15%) potranno avvenire solo a seguito di specifica autorizzazione rilasciata da EDISER Srl, società di servizi dell'Associazione Italiana Editori, attraverso il marchio CLEARedi Centro Licenze e Autorizzazioni Riproduzioni Editoriali. Informazioni: www.clearedi.org

L'elaborazione dei testi, anche se curata con scrupolosa attenzione, non può comportare specifiche responsabilità per eventuali involontari errori o inesattezze.

Finito di stampare nel mese di giugno 2022
da L.E.G.O. S.p.A
Viale dell'industria, 2 - 36100 VICENZA

PRIVACY BY DESIGN E BY DEFAULT 10.

- | | |
|--|--|
| 10.1. PREMESSA | 10.4.1. Cos'è il <i>privacy engineering</i> ? |
| 10.1.1. Inquadramento | 10.4.2. Le strategie di <i>privacy design</i> |
| 10.1.2. Rapporto con gli altri principi del GDPR | 10.5. DATA MONETIZATION E PRIVACY: COME SBLOCCARE IL VALORE DEI DATI |
| 10.2. IL PRINCIPIO DI PRIVACY BY DEFAULT | 10.5.1. Come superare i fattori bloccanti della <i>data monetization</i> |
| 10.2.1. Come attuare il principio di <i>privacy by default</i> in concreto | 10.5.2. I rischi nei trasferimenti di dati e gli strumenti giuridici di protezione disponibili |
| 10.2.2. Come valutare la necessità dei dati per le finalità del trattamento | 10.5.3. Strumenti contrattuali per la riutilizzo sicuro dei dati: la <i>privacy</i> come fattore abilitante |
| 10.3. IL PRINCIPIO DI PRIVACY BY DESIGN | 10.5.4. Il dilemma della re-identificazione |
| 10.3.1. I sette principi fondazionali della <i>privacy by design</i> : esempi di applicazione | 10.5.5. Anonimizzazione VS. Pseudonimizzazione |
| 10.3.2. Garantire la <i>privacy</i> nella selezione dei fornitori | 10.5.6. Indicazioni per anonimizzare i dati in sicurezza |
| 10.4. PRIVACY ENGINEERING: LE STRATEGIE PER INCORPORARE LA PRIVACY NEL DESIGN DEI TRATTAMENTI | 10.5.7. Quale base legale per l'anonimizzazione |

PREMESSA

Il fine del Regolamento generale sulla protezione dei dati (UE) 2016/679 (il "GDPR"), è di garantire il diritto fondamentale (sancito dall'art. 8 della Carta dei diritti fondamentali dell'Unione europea e ribadito dall'art. 16 del Trattato sul funzionamento dell'Unione europea) concernente la **protezione delle persone fisiche con riguardo al trattamento dei dati** di carattere personale.

Ma non solo.

Il GDPR è stato adottato per **aggiornare la disciplina della precedente** Dir. 95/46/CE all'avvento della società digitale, in modo così da sbloccare il potenziale delle nuove tecnologie, fornendo dei principi solidi e chiari per indirizzare lo **sviluppo dell'economia digitale**. Un approccio innovativo, con l'intento di sfuggire all'inevitabile obsolescenza dei testi normativi, per riuscire a stare al passo con la dirompente tecnologia, favorendo la possibilità di trarre valore dai dati e garantendo al contempo il diritto individuale alla protezione dei dati personali.

Ma non solo.

Per comprendere appieno la portata innovativa del GDPR è necessario soffermarsi su due **principi cardine** in esso contenuti:

- il principio di protezione dei dati fin dalla progettazione (**privacy by design**);
- il principio di protezione per impostazione predefinita (**privacy by default**).

Tali principi sono forieri di un approccio olistico alla *privacy*, dove l'industria e i consumatori, i tecnici ed i legali, scoprono insieme cosa funziona e cosa no, lasciando

10.1.

spazio all'innovazione "dal basso", a differenza di un approccio puramente regolamentato "dall'alto", che lascerebbe spazio solo alla conformità.

10.1.1. Inquadramento

L'art. 25 GDPR introduce i principi di privacy by design e privacy by default. Sebbene i concetti alla base di questi principi siano in realtà risalenti, è proprio grazie al GDPR che tali paradigmi hanno finalmente trovato una stigmatizzazione nell'ambito di una cornice normativa di rango primario.

I principi introdotti dall'art. 25 GDPR pongono a carico dei titolari del trattamento (di tutte le dimensioni, sia piccole aziende che multinazionali) l'obbligo di adottare misure tecniche ed organizzative adeguate volte ad incorporare i principi di protezione dei dati sin dalla fase di progettazione e sviluppo di ogni prodotto, servizio o attività che preveda il trattamento di dati personali (privacy by design), e volte a garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento (privacy by default).

Ratio della norma - La *ratio* della norma trova fondamento nella consapevolezza della necessità di un **approccio più robusto per affrontare l'evoluzione delle tecnologie** dell'informazione e della comunicazione (ICT), e delle infrastrutture di rete su larga scala. In tal senso viene riconosciuto che l'incorporazione della privacy come impostazione predefinita nella progettazione, nel funzionamento e nella gestione delle ICT e dei sistemi, lungo l'intero ciclo di vita delle informazioni, è necessaria per garantire una protezione completa e costante dei dati degli individui.

10.1.2. Rapporto con gli altri principi del GDPR

I principi di privacy by design e privacy by default sono **complementari** e si rafforzano vicendevolmente: gli individui trarranno maggior beneficio dalla privacy by design, se il principio di privacy by default è correttamente implementato.

Allo stesso tempo tali principi sono strettamente **connessi** agli altri principi previsti dall'art. 5 GDPR ed **in particolare al principio di minimizzazione e di accountability**. Da un lato, infatti, il rispetto di tali principi presuppone che i dati raccolti siano adeguati, pertinenti e limitati a quanto necessario per le finalità per le quali sono raccolti. Dall'altro l'adozione delle misure necessarie a garantire la protezione dei dati, sia all'atto del trattamento sia al momento di determinare i mezzi dello stesso, rappresenta una modalità di dimostrare il rispetto degli obblighi di responsabilizzazione previsti ai sensi dell'art. 24 GDPR. Per decidere quali misure adottare in concreto, il titolare del trattamento deve tenere conto dello stato dell'arte, dei costi di attuazione, della natura, dell'oggetto e delle finalità del trattamento di dati personali che intende svolgere. Deve inoltre procedere a selezionare le misure adeguate, ponderando i rischi del trattamento sia sul versante della probabilità del verificarsi dei medesimi, sia con riferimento alla gravità della lesione dei diritti e delle libertà delle persone fisiche, in caso di realizzazione delle ipotesi di rischio contemplate.

Meccanismi di certificazione - La norma che introduce i due principi in analisi, ha inoltre un interessante collegamento con l'art. 42 GDPR, secondo il quale è auspicabile che le Autorità pubbliche incoraggino l'istituzione di meccanismi di certificazione della protezione dei dati, nonché di **sigilli e marchi di protezione** dei dati (attualmente, non ancora affermatasi nella prassi) allo scopo di dimostrare la conformità al GDPR dei trattamenti effettuati dai titolari. In ogni caso, la certificazione non riduce la responsabilità del titolare, ma può essere in grado di influire sulla gravità delle sanzioni in ossequio al principio dell'accountability.

IL PRINCIPIO DI PRIVACY BY DEFAULT

10.2.

Come attuare il principio di privacy by default in concreto

10.2.1.

L'obiettivo del principio di privacy by default è quello di garantire la salvaguardia delle informazioni relative alle persone interessate dal trattamento nel modo più ampio possibile, ovvero di far sì che **la protezione dei dati personali sia adottata quale impostazione predefinita**. Il rispetto di questo principio impone pertanto ai titolari di **trattare** - per impostazione predefinita - **solo i dati personali strettamente necessari** al perseguimento delle finalità specifiche del trattamento.

Per attuare tale principio il titolare deve adottare una serie di **misure tecniche e organizzative adeguate** (art. 25, comma 2), volte a fare in modo che le applicazioni, i programmi, i prodotti o i servizi che comportano il trattamento di dati personali, offrano le massime garanzie possibili di rispetto della privacy. Il Comitato europeo per la protezione dei dati nelle Linee Guida 4/2019 sull'art. 25 GDPR - Data Protection by Design and by Default (v. 2.0), del 20/10/2020, ha precisato che le opportune misure tecniche e organizzative devono essere concepite, avendo riguardo alla effettiva attuazione di ciascuno dei principi dell'art. 5 GDPR e la conseguente tutela dei diritti. Questo vuol dire innanzitutto che l'art. 25 non impone l'adozione di misure specifiche, ma la scelta dipenderà dalle circostanze dei trattamenti svolti in concreto. Le citate linee guida contengono una dettagliata elencazione dei principali elementi degli elementi di privacy by design e by default da prendere in considerazione per implementare ciascuno dei principi previsti dall'art. 5 GDPR.

In generale, per implementare l'obbligo di adozione delle misure tecniche ed organizzative adeguate, occorre tenere presente che esso vale sia per la quantità dei dati personali raccolti, che per la portata del trattamento, il periodo di conservazione e l'accessibilità.

1. **Volume dei dati personali raccolti:** i dati personali possono essere raccolti **solo se strettamente necessari per il raggiungimento dello scopo** per cui sono stati raccolti. In altre parole, se nella progettazione di un determinato trattamento dovesse risultare astrattamente possibile raccogliere più dati di quelli che sono effettivamente necessari, ad esempio per garantirsi una possibilità futura di utilizzo, tale raccolta non potrà essere svolta in quanto non è predeterminata al perseguimento di una finalità concretamente determinata, ma puramente eventuale. Oltretutto se una finalità del trattamento può essere perseguita trattando indifferentemente diverse categorie di dati personali, occorre scegliere quelle meno invasive, ad esempio limitando il trattamento di dati appartenenti alle categorie particolari di cui all'art. 9 GDPR (es. dati sullo stato di salute o le preferenze sessuali) alle sole ipotesi strettamente necessarie.
2. **Portata del trattamento:** i dati personali possono essere **trattati solo per gli scopi legittimi** per i quali sono stati raccolti e non possono essere utilizzati per altri scopi. Il titolare del trattamento deve stabilire le procedure necessarie per garantire che i soggetti incaricati del trattamento (sia interni che esterni) siano consapevoli dei limiti del trattamento dei dati personali degli interessati e per evitare che i dati siano utilizzati per ulteriori finalità.
3. **Periodo di conservazione:** i dati personali possono essere trattati **solo per il tempo strettamente necessario**. Il titolare del trattamento deve prevedere adeguati protocolli per garantire la cancellazione dei dati una volta raggiunto lo scopo per il quale sono stati raccolti.
4. **Accessibilità:** i dati personali devono essere **accessibili solo ai soggetti le cui funzioni richiedono necessariamente il trattamento di queste informazioni**, impedendo l'accesso ai dati in ogni altro caso. Ad esempio i profili di autorizzazione degli applicativi aziendali devono essere individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati

necessari all'esecuzione delle mansioni assegnate. Inoltre è possibile configurare gli accessi tenendo conto della necessità effettiva, ad esempio qualora un utente o un reparto possa svolgere le proprie funzioni senza conoscere i dati personali degli interessati, l'accesso alle informazioni dovrà avvenire senza la possibilità di visualizzare o trattare questo tipo di dati. In ogni caso il titolare dovrebbe consentire agli interessati di intervenire prima che i propri dati siano divulgati o resi accessibili ad un numero indefinito di soggetti.

Nel determinare le misure adeguate, il titolare deve tenere conto di alcuni elementi specifici previsti dall'art. 25, comma 1.

| | |
|--|---|
| Stato dell'arte | È un concetto dinamico che impone un obbligo ai titolari, nella determinazione delle opportune misure tecniche e organizzative, di tener conto degli attuali progressi tecnologici, volta per volta disponibili sul mercato (cioè tenendo conto anche di modifiche ed aggiornamenti). Eventuali framework, norme, certificazioni, codici di condotta, ecc. esistenti e riconosciuti possono essere utili per individuare lo stato dell'arte in un certo momento nel settore di riferimento. |
| Costi di attuazione | Non è richiesto che il titolare spenda una quantità sproporzionata di risorse quando esistono misure alternative, meno dispendiose, ma comunque efficaci. In ogni caso, indipendentemente dal costo, le misure devono garantire che il rispetto dei principi e dei diritti degli individui sia garantito in maniera effettiva. |
| Natura, ambito di applicazione, contesto e finalità del trattamento | Questi fattori dovrebbero essere interpretati in modo coerente con il loro ruolo in altre disposizioni del GDPR, come gli artt. 24, 32 e 35, allo scopo di definire i principi di protezione dei dati nel trattamento. In breve, il concetto di natura può essere inteso come le caratteristiche intrinseche del trattamento. L'ambito di applicazione si riferisce alle dimensioni e alla portata del trattamento. Il contesto si riferisce alle circostanze di il trattamento, che può influenzare le aspettative dell'interessato, mentre la finalità riguarda alle finalità del trattamento. |
| Rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento | Il titolare deve effettuare un'analisi per identificare i rischi di una violazione dei suddetti principi per i diritti degli interessati, e determinare la loro probabilità e gravità al fine di attuare misure per mitigare efficacemente i rischi individuati. Una valutazione sistematica e approfondita del trattamento è fondamentale per svolgere tale valutazione dei rischi. Tale analisi può essere effettuata ad esempio prendendo in considerazione la metodologia di analisi dei rischi illustrata dal Gruppo di Lavoro ex Art. 29 nelle Linee Guida in materia di valutazione d'impatto sulla protezione dei dati, WP 248 rev.01, di ottobre 2017. |

L'attuazione del principio di privacy by default deve pertanto essere presa in considerazione sin dalla **fase di progettazione** del trattamento, tuttavia è bene rammentare che non è limitata alla sola fase prodromica, ma si estende per tutto il ciclo del trattamento. A tal fine è possibile ad esempio **determinare degli indicatori di per-**

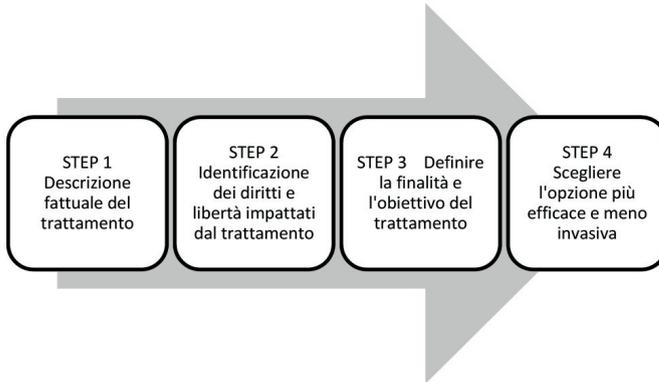
formance (*key performance indicators* o *KPI*) per dimostrare l'effettività delle misure implementate o **programmare delle verifiche volte ad accertare la corretta attuazione di tale principio nei vari ambiti di applicazione**. Con riferimento all'accessibilità, ad esempio, è opportuno prevedere che i profili di accesso stabiliti siano oggetto di controlli periodici finalizzati alla verifica della sussistenza delle condizioni per la conservazione dei profili attribuiti in relazioni alle aree di operatività/mansioni specificamente attribuite.

Come valutare la necessità dei dati per le finalità del trattamento

10.2.2.

È obbligo del titolare del trattamento fare sì che i **dati raccolti siano adeguati, pertinenti e limitati a quanto necessario per le finalità per le quali sono raccolti**. Per valutare la necessità dei dati in relazione ad un determinato trattamento che si intende porre in essere, e per garantire cioè il rispetto del principio di *privacy by default*, allo stato attuale, non esiste una singola metodologia specifica approvata dalle autorità competenti in materia di protezione dei dati personali a livello italiano, né tantomeno a livello europeo. In tal senso, tuttavia, può essere opportuno prendere in considerazione il processo di valutazione suggerito all'interno del *Necessity Toolkit* (disponibile qui: https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en.pdf) realizzato dal Garante europeo della protezione dei dati personali (il c.d. European Data Protection Supervisor, o EDPS). Questo strumento, seppure concepito per rispondere ad una richiesta di chiarimenti delle istituzioni europee sulle particolari condizioni previste dall'art. 52 (1) della Carta dei diritti fondamentali dell'unione europea, contiene un iter di valutazione che può essere utilizzato - con i dovuti adeguamenti al contesto specifico di riferimento - per guidare i titolari nella valutazione della necessità dei dati che intendono trattare, alla luce delle circostanze del trattamento e delle finalità specifiche.

Il processo per la verifica della necessità consiste in quattro step consecutivi. Ad ogni step corrisponde un set di domande che facilitano la valutazione della necessità.



VALUTAZIONE E GESTIONE DEL RISCHIO

STEP 1: è il passaggio preliminare e prevede una descrizione dettagliata dell'attività di trattamento in modo da fornire un quadro chiaro e trasparente con riferimento ad una serie di fattori, tra cui:

- l'obiettivo di interesse generale o particolare perseguito dal trattamento;

- l'esatta finalità del trattamento dei dati personali, spiegata con maggiore dettaglio rispetto all'obiettivo;
- le categorie di dati oggetto del trattamento;
- le categorie di interessati (ad esempio, dipendenti, migranti, minorenni);
- i soggetti che tratteranno ed avranno accesso ai dati (ad esempio, un'azienda privata, un'organizzazione pubblica);
- le operazioni di trattamento previste (ad esempio, raccolta, arricchimento, accesso, trasferimento);
- ogni altra disposizione pertinente, come la durata del trattamento.

STEP 2: il secondo passaggio contribuisce a stabilire se l'attività di trattamento proposta rappresenti una limitazione dei diritti o delle libertà degli interessati. In base alla natura e agli utilizzi dei dati raccolti, alcuni trattamenti possono rappresentare una limitazione del diritto alla riservatezza. Ad esempio, la circostanza che l'esercizio di alcuni diritti possa essere impedito (es. diniego di cancellazione perché i dati sono necessari al titolare per fornire il proprio servizio o per difendere i propri diritti in giudizio) o che i dati possano essere resi noti a terzi (es. autorità o altre società del gruppo) può rappresentare una limitazione del diritto alla protezione dei dati personali. La necessità del trattamento dovrà essere tanto maggiore quanto maggiore è il potenziale impatto sui diritti e le libertà degli interessati.

STEP 3: il terzo passaggio considera la finalità del trattamento, rispetto alla quale la necessità di utilizzo dei dati personali dovrebbe essere valutata. In particolare questo step prevede una analisi dell'obiettivo del trattamento (es. aumentare la riconoscibilità nel mercato del proprio brand) e della finalità perseguita (es. inviare comunicazioni di direct marketing ai clienti). Il titolare dovrà svolgere una analisi precisa ed al contempo trasparente, ad esempio assicurandosi che:

- la finalità del trattamento e l'obiettivo specifico del titolare siano sufficientemente e chiaramente descritti; e
- la finalità del trattamento sia effettivamente finalizzata a conseguire l'obiettivo e che sia legittima e non futile.

STEP 4: il passaggio finale fornisce indicazioni sugli aspetti specifici da considerare durante l'esecuzione del test di necessità, al fine di garantire che il trattamento sia efficace limitandone il più possibile l'invasività. In particolare occorre verificare che:

- i dati oggetto del trattamento siano appropriati e pertinenti rispetto all'obiettivo e alla finalità perseguita (es. per aumentare la riconoscibilità del brand attraverso direct marketing può essere necessario conoscere l'indirizzo email dell'interessato, ma potrebbe non esserlo conoscere il suo stato di salute); non tutto ciò che "potrebbe rivelarsi utile" per un certo obiettivo è appropriato, o può essere considerato un trattamento necessario, la mera convenienza o il favorevole rapporto costi/benefici non sono sufficienti;
- la finalità e l'obiettivo perseguiti siano una diretta conseguenza logica del trattamento dei dati personali raccolti;
- il trattamento di dati diversi (es. meno invasivi, quali quelli anagrafici rispetto ai dati sulla salute, o quelli pseudonimizzati rispetto a quelli direttamente identificabili) o non personali (es. dati anonimizzati) deve essere concretamente preso in considerazione e l'eventuale impossibilità di conseguire la finalità attraverso tali dati deve essere dimostrata.

10.3. IL PRINCIPIO DI PRIVACY BY DESIGN

Il concetto di privacy by design fu coniato per la prima volta negli anni Novanta dalla Dottoressa Ann Cavoukian, *Information and Privacy Commissioner* dell'Ontario (Canada), che fu tra i promotori della risoluzione adottata nel 2010 nel corso della trentaduesima Conferenza mondiale dei Garanti privacy tenutasi a Gerusalemme dal 27 al 29/10/2010, che, riconoscendo il principio come una componente

essenziale della fondamentale protezione della privacy, ne incoraggiava l'adozione come modus operandi standard delle organizzazioni.

Questo approccio concettuale innovativo impone quindi ai titolari un'**attenzione orientata alla gestione del rischio e alla responsabilità**, per stabilire strategie che incorporino la protezione della privacy durante tutto il ciclo di vita di un progetto (sia esso un sistema, un prodotto hardware o software, un servizio o un processo). In base all'art. 25, comma 1, GDPR, nell'elaborazione di tali strategie, il titolare deve tenere conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, procedendo a selezionare le **misure tecniche ed organizzative adatte a ponderare i rischi del trattamento** sia sul versante della **probabilità**, che della **gravità** della lesione dei diritti e delle libertà delle persone fisiche.

Il titolare, infine, deve essere in grado di dimostrare - in sostanza - lo svolgimento di tutte le attività appena descritte, tenendo conto che, come per il principio di privacy by default, queste attività non si esauriscono alla fase prodromica del trattamento, e richiedono pertanto un monitoraggio costante lungo tutto il ciclo di vita del progetto.

I sette principi fondazionali della privacy by design: esempi di applicazione 10.3.1.

La privacy by design si basa sulla concezione che la protezione dei dati sia il modus operandi predefinito all'interno dei modelli di business delle organizzazioni, estendendosi ai sistemi informatici che supportano il trattamento dei dati, ai relativi processi, alle pratiche di business e alla progettazione fisica e logica dei canali di comunicazione utilizzati. Tale paradigma può essere garantito mettendo in pratica i sette "principi fondazionali" definiti da Ann Cavoukian.

| Principio | Esempio di applicazione |
|--|--|
| 1. Proattivo non reattivo , cioè i problemi vanno valutati nella fase di progettazione anticipando gli eventi che influiscono sulla privacy prima che si verifichino. | Sviluppare una cultura condivisa improntata all'impegno e al miglioramento continuo da parte di tutti i dipendenti, definendo ed assegnando responsabilità concrete in modo che ogni membro dell'organizzazione sia chiaramente consapevole dei propri compiti in materia di privacy. |
| 2. Privacy come impostazione di default , quindi massimizzare la privacy assicurando che i dati personali siano automaticamente protetti e che la privacy sia sempre garantita in quanto integrata nel sistema, lasciando al soggetto interessato la possibilità di intervenire sulle impostazioni. | Definire dei termini di conservazione dei dati, prevedere meccanismi per garantire che siano rispettati e creare barriere tecnologiche e procedurali per prevenire il collegamento non autorizzato di fonti di dati indipendenti. Fare in modo che all'utente non sia richiesta nessuna azione per tutelare la sua privacy, ma che sia inclusa nel sistema/app/servizio/ecc., di default. |

| Principio | Esempio di applicazione |
|---|---|
| <p>3. Privacy incorporata nella progettazione, deve essere cioè parte integrante e inscindibile dei sistemi, delle applicazioni, dei prodotti e dei servizi, nonché delle pratiche e dei processi aziendali di un'organizzazione. Non si tratta di un livello o modulo aggiuntivo rispetto ad un'entità preesistente, ma deve essere integrato nel gruppo di requisiti di base a partire dalle fasi di sviluppo e progettazione del concetto stesso.</p> | <p>Documentare tutte le decisioni che vengono adottate all'interno dell'organizzazione dalla fase di progettazione al processo di messa in produzione, in una prospettiva di "privacy design thinking". Adottare una procedura di privacy by design per fare in modo che i framework di gestione dei progetti aziendali prevedano degli adeguati step di controllo circa la conformità con i principi di privacy by design, prima dell'inizio di qualsiasi nuova attività di trattamento di dati personali.</p> |
| <p>4. Massima funzionalità, valore positivo non valore zero: la privacy by design mira a conciliare tutti gli interessi legittimi e gli obiettivi di business, dimostrando che non si escludono tra di loro (<i>win-win situation</i>) rifiutando le false dicotomie quali: più privacy = meno sicurezza, o meno benefici economici.</p> | <p>Applicare il pensiero laterale per trovare soluzioni innovative e stabilire canali di comunicazione per la collaborazione e la consultazione delle varie parti in gioco al fine di comprendere e riunire molteplici interessi che, a prima vista, possono sembrare divergenti. Prevedere dei tavoli di lavoro trasversali in cui le funzioni legal e compliance (es. DPO) si confrontino con i referenti delle funzioni di business e di sicurezza (es. CISO) per mettere insieme le proprie competenze nello sviluppo dei nuovi progetti.</p> |
| <p>5. Sicurezza durante tutto il ciclo del prodotto o servizio: la privacy by design deve essere incorporata prioritariamente rispetto alla acquisizione del primo elemento di informazione, garantendo che si estenda in modo sicuro attraverso l'intero ciclo vitale dei dati, senza diminuirne il valore.</p> | <p>Per integrare la privacy in tutte le fasi del trattamento dei dati, è necessario analizzare in modo approfondito le diverse attività di trattamento coinvolte (es. raccolta, classificazione, conservazione, consultazione, diffusione, ecc.) per fare in modo che vengano adottate le misure di sicurezza più adeguate a seconda del caso specifico. Ciò garantisce che tutti i dati siano conservati in modo sicuro e poi distrutti alla fine del processo, in modo tempestivo.</p> |
| <p>6. Visibilità e trasparenza - mantenere la trasparenza: un aspetto chiave per garantire la privacy è poterla dimostrare, dando prova di diligenza nei confronti delle autorità di controllo, e di fiducia nei confronti degli interessati.</p> | <p>Elaborare e pubblicare un'informativa sul trattamento dei dati personali concisa, chiara e comprensibile, adottando un approccio di legal design per rendere i contenuti facilmente accessibili e consentendo così agli interessati di comprendere l'ambito di trattamento dei loro dati, i rischi a cui possono essere esposti, nonché le modalità di esercizio dei loro diritti.</p> |

| Principio | Esempio di applicazione |
|--|--|
| <p>7. Centralità dell'utente: secondo questa impostazione, l'utente è considerato il centro del sistema privacy (che, per definizione, è quindi "user centric"). Questo vuol dire che non è sufficiente una progettazione che sia conforme alle norme se poi l'utente non è adeguatamente protetto.</p> | <p>Attuare meccanismi efficienti che consentano agli interessati di esercitare i loro diritti in maniera efficace, ad esempio creando delle piattaforme per consentire agli interessati di avere direttamente accesso ai propri dati e di poterli modificare, esportare o cancellare, oppure di poter interagire con il titolare in tempo reale attraverso strumenti quali chatbot o assistenti virtuali, come PRISCA (il primo chatbot interamente sviluppato da avvocati e giuristi esperti di privacy che fornisce informazioni e indicazioni sulle principali questioni basilari relative alla privacy ed alla protezione dei dati personali, come quelle relative al GDPR ed al Regolamento e-Privacy).</p> |

Questo innovativo paradigma, che da molti viene considerato il futuro della privacy, può dunque permettere di **prevenire i rischi** ed **evitare i potenziali danni**, il tutto però, per poter funzionare presuppone che i principi fondazionali vengano implementati allo stadio di design dei trattamenti e siano rispettati lungo tutto il ciclo di vita delle informazioni.

Garantire la privacy nella selezione dei fornitori

10.3.2.

Per creare un modello virtuoso di compliance ai principi fondazionali della privacy by design, occorre garantire che tali principi siano adeguatamente implementati da tutti i soggetti lungo la filiera del trattamento. Occorre infatti **scegliere con attenzione i soggetti terzi cui affidare il trattamento**. La scelta del responsabile esterno del trattamento è un fattore fondamentale nell'ottica del principio dell'accountability e, qualora svolta in modo scorretto, potrebbe, in ipotesi di giudizio sulla responsabilità, determinare una eventuale c.d. *culpa in eligendo*, qualora si dovesse accertare ad opera del titolare la negligenza nella scelta dell'organizzazione a cui affidare le informazioni dei propri clienti o dipendenti.

È pertanto opportuno che la selezione dei fornitori avvenga **tra più offerenti**, tenendo in considerazione sia l'offerta economica, sia il servizio richiesto, sia gli indicatori di base relativi alle misure tecniche e organizzative in possesso del fornitore. Una scelta poco misurata ed una nomina frettolosa possono comportare un aggravio dei rischi in caso di contenzioso sia con il Garante che con il terzo.

Buone prassi nella selezione dei fornitori - Una buona prassi è quella di **effettuare dei controlli sul livello generale di compliance dell'offerente**, ad esempio attraverso l'utilizzo di checklist relative alle misure minime che devono essere garantite, e, una volta selezionato il miglior offerente, **fornire delle specifiche istruzioni sulla modalità di svolgimento dell'incarico**, anche effettuando degli audit a campione o delle simulazioni per verificarne il rispetto.

Esempio

Nell'ipotesi di *data breach* subito dal fornitore, è fondamentale includere nell'atto di nomina a responsabile esterno delle previsioni specifiche che obblighino il terzo a fornire al titolare - in maniera tempestiva - tutte le informazioni che occorrono per valutare, ed eventualmente effettuare, la notifica al Garante e la comunicazione agli interessati, secondo quanto previsto dal GDPR. Tale atto di nomi-

na, oltre ad includere una lista delle informazioni che devono essere raccolte e condivise, conformemente con il modello di notifica predisposto dal Garante, deve individuare un canale dedicato a cui inviarle (es. indirizzo email specifico costantemente monitorato) e deve prevedere un obbligo di riservatezza a carico del fornitore, impedendogli di divulgare ogni informazione in caso di incidenti, per evitare di ledere la reputazione aziendale.

La privacy nelle comunicazioni con i fornitori - Il ricorso a fornitori esterni può implicare la necessità di trasferire i dati fuori dal perimetro aziendale. Ciò implica che la protezione dei dati debba essere assicurata anche nelle comunicazioni adottando gli opportuni accorgimenti, ad esempio facendo in modo che:

- i dati trasmessi siano messi in sicurezza, attraverso l'utilizzo di misure idonee quali la crittografia o la pseudonimizzazione, di cui si dirà in seguito;
- i dati siano trasmessi attraverso canali cifrati e protetti in modo da oscurare la fonte e i tipi di dati;
- l'archiviazione delle informazioni raccolte dai dispositivi sui server, come i dati analitici o i metadati (es. in caso di Big Data o le altre tecnologie di derivazione di schemi caratteriali, sia limitata in modo da prevenire l'identificazione degli individui nei casi in cui non sia essenziale per la fruizione dei servizi.

Questi sono solo alcuni degli esempi concreti di misure da adottare per garantire il rispetto dei principi in analisi, per determinare quali siano tutti gli adempimenti specifici da porre in essere in relazione alle misure di sicurezza, è necessario procedere ad una valutazione caso per caso, sulla base della portata, dell'impatto e del livello di rischio del trattamento.

10.4. PRIVACY ENGINEERING: LE STRATEGIE PER INCORPORARE LA PRIVACY NEL *DESIGN* DEI TRATTAMENTI

Secondo il report "*Privacy by design in big data An overview of privacy enhancing technologies in the era of big data analytics*" dell'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA), la privacy by design è un concetto poliedrico: nei documenti giuridici è generalmente descritta in termini molto ampi come principio generale; dagli informatici e dagli ingegneri, è spesso equiparata all'uso di specifiche tecnologie di miglioramento della privacy (c.d. **privacy-enhancing technologies o PET**). Tuttavia, **la privacy by design non è un insieme di meri principi generali**, né può essere ridotta all'applicazione delle PET. Si tratta, infatti, di un processo che coinvolge varie componenti tecnologiche e organizzative, che attuano i principi della privacy e della protezione dei dati. L'attuazione concreta di tali principi richiede la collaborazione di tecnici e giuristi nel processo c.d. di privacy engineering.

10.4.1. Cos'è il *privacy engineering*?

Il privacy engineering è **un processo sistematico il cui obiettivo è quello di tradurre in termini pratici e operativi i principi della *privacy by design***, fornendo metodologie, strumenti e tecniche tali da incorporare i principi all'interno del ciclo di vita dei sistemi informatici dedicati al trattamento dei dati personali. Questo processo richiede un approccio sistematico e metodologico, per trasferire le proprietà e le funzionalità privacy individuate nelle fasi di analisi del concept (requisiti di privacy individuati) nella progettazione dell'architettura e realizzazione degli elementi del sistema (strategie e soluzioni concrete), lavorando così in modo sequenziale secondo diversi livelli di astrazione. Sul punto è interessante il documento recentemente pubblicato dell'Enisa volto proprio a supportare i professionisti e le società e

fornire chiarimenti e delucidazioni utili circa l'implementazione pratica degli aspetti tecnici della privacy by design e by default (*Data protection engineering, From Theory to Practice*, Gennaio 2022). Il documento infatti presenta le tecnologie e le tecniche di sicurezza esistenti e discute i possibili punti di forza e l'applicabilità in relazione al rispetto dei principi di protezione dei dati come stabilito nell'articolo 5 del GDPR.

Le strategie di privacy design

10.4.2.

Nelle fasi iniziali di sviluppo del concept e di analisi dei suoi requisiti, è necessario adottare approcci di alto livello volti a identificare le tattiche da seguire durante le diverse fasi del trattamento dei dati.

Queste strategie forniscono un modello accessibile agli ingegneri che progettano un oggetto per definire i requisiti di privacy identificati durante le fasi di analisi preliminare. Le strategie di progettazione della privacy fungono da ponte tra i principi di trattamento imposti dalla legge e l'implementazione della privacy in soluzioni concrete.

Sono state individuate in particolare **8 strategie** per aiutare a progettare sistemi, servizi e prodotti, nel rispetto del principio di privacy by design. Si tratta di strategie originariamente individuate da Jaap-Henk Hoepman, in "*Privacy Design Strategies*", nell'ottobre 2012 e successivamente riprese dall'ENISA nel report "*Privacy and Data Protection by Design - from policy to engineering*" del dicembre 2014, e dal Garante spagnolo (AEPD) nella "*Guía de Privacidad desde el Diseño*", di ottobre 2019.

| Strategie di privacy design | Esempio |
|---|---|
| <p>1. Minimizzare Limitare il più possibile il trattamento dei dati personali adottando le 4 tattiche di minimizzazione: (i) selezione dei dati rilevanti; (ii) esclusione delle informazioni in eccesso; (iii) rimozione dei dati a livello applicativo man mano che non sono più necessari; (iv) distruzione di tutti i dati a livello di storage una volta che non sono più rilevanti.</p> | <p>Ci sono metodi collaudati per cancellare e distruggere veramente i dati da dischi rigidi. Un metodo efficiente per distruggere i backup è criptando i dati prima di fare il backup. Associando alcune chiavi con particolari periodi di conservazione, tutti i dati di un determinato dato possono essere resi inutilizzabili semplicemente distruggendo la chiave di decriptazione associata.</p> |
| <p>2. Separare L'obiettivo di questa strategia è quello di evitare, o almeno di ridurre al minimo, il rischio che durante il trattamento, dati personali diversi di uno stesso individuo, che vengono utilizzati in processi indipendenti, possano essere combinati per creare un profilo completo dell'interessato. Questa strategia viene applicata attraverso le 2 tattiche di separazione: (i) isolamento dei dati in differenti database o applicazioni separate logicamente o a livello hardware; (ii) distribuzione delle attività di trattamento per evitare che tutti i dati siano in controllo di un unico soggetto.</p> | <p>In generale per migliorare la protezione della privacy si potrebbero utilizzare reti peer-to-peer o algoritmi distribuiti invece di approcci centralizzati. I moderni smartphone consentono agli utenti di autenticarsi utilizzando lo sblocco tramite dati biometrici, come l'impronta digitale o lo scan facciale. Questi software di autenticazione funzionano localmente nel telefono dell'utente, evitando così che i dati biometrici siano inviati a un server centrale per l'analisi.</p> |

| Strategie di privacy design | Esempio |
|--|---|
| <p>3. Nascondere Proteggere i dati personali rendendoli inaccessibili o non visualizzabili, per prevenire che diventino pubblici o conosciuti. Tale strategia si attua attraverso le seguenti tattiche: (i) restringere gli accessi nello spazio (solo i soggetti autorizzati) e nel tempo (solo per il tempo consentito); (ii) offuscare i dati rendendoli indecifrabili ai soggetti non autorizzati; (iii) dissociare i collegamenti fra i vari dataset, eliminando gli elementi che possono rendere indirettamente identificabili i dati, ad esempio i metadati; (iv) mixare le informazioni tra di loro per nascondere la fonte.</p> | <p>Alcuni servizi di comunicazione e di cloud storage utilizzano servizi crittografia end-to-end. In tal modo grazie all'utilizzo di un doppio paio di chiavi crittografiche necessarie per cifrare e decifrare i messaggi, solo il mittente ed il destinatario possono avere accesso al contenuto delle comunicazioni. Ciò garantisce che il fornitore di servizi non possa decifrare e leggere i dati che memorizza o inoltra. I dati sono disponibili solo negli "endpoint" (cioè lo smartphone o il laptop) degli utenti stessi.</p> |
| <p>4. Astrarre La strategia è quella di limitare il più possibile i dettagli dei dati personali trattati. Mentre la strategia del "minimizzare" effettua una precedente selezione dei dati da raccogliere, questa strategia si concentra sul grado di dettaglio dei dati trattati e sulla loro aggregazione utilizzando tre tattiche: (i) riassumere le informazioni dettagliate in categorie più ampie e meno invasive; (ii) raggruppare le informazioni in insieme aggregati evitando di trattare le informazioni sui singoli; (iii) perturbare, non riportare le informazioni con il massimo dettaglio specifico, ma aggiungere un disturbo casuale senza compromettere la qualità dell'informazione.</p> | <p>In molti casi, per effettuare delle segmentazioni efficaci, come nel caso di promozioni o prodotti destinati a soggetti determinati o nel caso di servizi riservati a soggetti adulti, non è necessario trattare la data di nascita specifica ma è possibile riassumere le informazioni nella sola età o addirittura raggrupparle definendo delle fasce di età (over 70/under 18). I servizi basati sul trattamento dei dati di localizzazione degli interessati alle volte non necessitano delle precise coordinate geografiche, ad esempio per mostrare il numero di farmacie nelle vicinanze, e possono funzionare ugualmente con una posizione approssimata con un raggio di chilometri e non necessariamente di metri.</p> |
| <p>5. Informare Questa strategia attua gli obiettivi e i principi di trasparenza stabiliti dal GDPR e cerca di rendere gli interessati pienamente consapevoli del trattamento dei loro dati in modo tempestivo, permettendogli così di prendere delle scelte consapevoli in relazione alla privacy.</p> | <p>Una strategia informativa efficace tiene conto delle esigenze di comunicazione specifiche dei soggetti cui ci si rivolge ed è parametrata sulle caratteristiche degli stessi: oltre l'utilizzo di icone, riquadri riassuntivi, caratteri ad elevato contrasto e periodi chiari, concisi e logici, è opportuno fare sì che le informazioni rese siano adeguatamente comprensibili all'utente medio cui ci si rivolge, ad esempio semplificando molto i concetti, anche tramite l'utilizzo di disegni e sezioni interattive, nel caso in cui ci si rivolga a bambini.</p> |

| Strategie di privacy design | Esempio |
|---|---|
| <p>La strategia si applica attraverso le seguenti 3 tattiche: (i) fornire tutte le informazioni utili, oltre a tutto ciò che è previsto dagli artt. 13 e 14 GDPR; (ii) spiegare con chiarezza quali dati si trattano e argomentare il perché è necessario il trattamento; (iii) notificare, fornire le informazioni agli interessati in tempo reale, non appena i dati sono raccolti, condivisi con i terzi, o sono oggetto di violazione, predisponendo delle adeguate procedure.</p> | <p>In questo senso può essere particolarmente utile coinvolgere un campione di soggetti destinatari nella fase di realizzazione delle informazioni per ricevere dei feedback durante il processo.</p> |
| <p>6. Controllare Fornire ai soggetti il controllo sulla raccolta, il trattamento, l'utilizzo e il trasferimento dei loro dati personali attraverso l'attuazione di meccanismi che consentono loro di esercitare in maniera diretta i diritti previsti dal GDPR o di modificare le opzioni di privacy nelle applicazioni e nei servizi. Le tattiche per fornire il controllo sono le seguenti: (i) chiedere agli utenti di manifestare la loro accettazione consapevole del trattamento dei dati, quando richiesto, attraverso una azione volitiva (come un consenso tramite la spunta di una casella o uno swipe); (ii) permettere agli interessati una alternativa in relazione al trattamento dei dati; (iii) aggiornare, permettere agli utenti di modificare le loro scelte in merito ai trattamenti autorizzati e (iv) ritrattare, consentire di ottenere la cancellazione dei dati personali.</p> | <p>Il consenso non è sempre una base legale valida per i trattamenti, ma quando può esserlo, è necessario che il soggetto sia stato reso effettivamente edotto degli effetti del suo consenso. Ad esempio le caselle di spunta possono essere rese accessibili solo dopo che il testo informativo è stato scrollato per intero.</p> <p>Per offrire una reale libertà di scelta agli utenti di un servizio o app, in alcuni casi oltre alla versione base con funzionalità limitate, accessibile anche a chi non fornisce il consenso, viene messa a disposizione una versione con funzionalità aggiuntive, offrendo poi una alternativa a pagamento o ad un prezzo maggiorato che preveda un trattamento dei dati meno invasivo.</p> <p>L'aggiornamento delle scelte in merito ai trattamenti può essere consentito in via diretta, predisponendo una dashboard con dei comandi (es. on/off) che tengano conto delle scelte effettuate, disponibili all'interno dell'area utente.</p> |
| <p>7. Applicare Affinché le strategie di privacy by design funzionino, è necessario che vengano adottate delle policy e procedure per farle applicare in concreto.</p> | <p>Per fare in modo che una politica sulla privacy sia efficace in concreto, occorre strutturarla in modo che sia allineata con gli obiettivi di business e con le altre policy e procedure interne. Anche in questo caso è fondamentale fare sì che siano molto chiari compiti e responsabilità di ogni risorsa.</p> |

| Strategie di privacy design | Esempio |
|---|--|
| Questa strategia è orientata all'interno per fare in modo che si garantisca ciò che si comunica all'esterno. La strategia prevede tre tattiche: (i) creare una politica sulla privacy, con ruoli specifici; (ii) fare in modo che sia conosciuta e rispettata innalzando il livello di consapevolezza in materia di privacy; e (iii) aggiornare le previsioni e le indicazioni tenendo conto dell'applicazione effettiva e dell'evoluzione delle esigenze di business e delle tecnologie di monitoraggio disponibili (es. audit e assessment da remoto, formazione a distanza periodica, ecc.). | Quanto all' applicazione effettiva, oltre alla attività di informazione e formazione iniziale, è opportuno prevedere l'allocatione di risorse per farla rispettare garantendo un monitoraggio capillare lungo la catena gerarchica, ma anche all'esterno, per le parti della policy che trovano applicazione in relazione ai terzi, ad esempio tramite checklist ed audit periodici. |
| <p>8. Dimostrare</p> <p>Questa strategia è orientata all'esterno ed è volta a dare prova della conformità dell'organizzazione. La dimostrazione si ottiene attraverso: (i) la raccolta della documentazione che comprovi i processi decisionali e le relative motivazioni; (ii) lo svolgimento di audit periodici relativi alle modalità di trattamento dei dati e dei processi privacy in generale; e (iii) la reportistica interna relativa agli esiti degli audit e delle altre attività privacy, es. DPIA.</p> | La dimostrazione del principio di privacy by design richiede di tenere traccia delle scelte prese durante la fase di sviluppo del progetto. È opportuno in tal senso che la raccolta delle informazioni sia completa, riportando eventuali tesi a favore o contrarie a determinate approcci, e spiegando le motivazioni che hanno portato alle decisioni finali, anche includendo le ragioni di business specifiche, come ad esempio l'impossibilità di procedere alla cancellazione di tutti i dati non più necessari immediatamente per mancanza di risorse, come nel caso della dispendiosa distruzione documentale, ma dimostrando di aver adottato un piano programmatico di cancellazione nel medio periodo. |

10.5. DATA MONETIZATION E PRIVACY: COME SBLOCCARE IL VALORE DEI DATI

10.5.1. Come superare i fattori bloccanti della *data monetization*

La ragione dell'enorme valore dei dati risiede nella loro natura non consumabile e nella capacità di acquistare valore ogni qual volta vengono riutilizzati per scopi differenti.

Ad oggi, la *data monetization* - la **capacità di trasformare i dati in informazione e l'informazione in valore in grado di generare benefici economici** misurabili - non ha ancora avuto l'impatto dirompente che ci si aspettava. Ciò deriva da una serie di fattori essenzialmente legati alla possibilità ed alla convenienza di diffondere e riutilizzare i dati. Grazie all'adozione concreta dei principi di privacy by design e default, è possibile sbloccare il potenziale della *data monetization*.

I rischi connessi alla perdita dei dati - Una delle maggiori preoccupazioni delle aziende è quella di perdere il controllo dei propri dati una volta diffusi o

addirittura di venire danneggiati dalla diffusione. Il disincentivo in questo caso deriva due ordini di fattori:

- *in primis* si teme di perdere i diritti di sfruttamento economico sui dati raccolti, a fronte di ingenti investimenti per predisporre la raccolta e l'immagazzinamento. I dati rappresentano un asset per le aziende il cui valore commerciale deriva dalla possibilità di trarne informazioni utili per orientare scelte strategiche (le preferenze dei consumatori, le criticità dei processi produttivi, l'orientamento di certi mercati, ecc.), per questo è di vitale importanza, per le imprese, proteggere i dati raccolti, per massimizzarne la produttività in termini economici;
- in secondo luogo, la *disclosure* potrebbe rivelare debolezze nei metodi di raccolta e quindi scarsa qualità dei dati, cagionando una diminuzione del loro valore commerciale.

Per sbloccare il potenziale dei dati è pertanto necessario comprendere quali siano gli strumenti giuridici attualmente disponibili in grado di favorire la circolazione delle idee e delle informazioni, e al contempo di incentivare la produzione e la diffusione di nuove creazioni intellettuali e raccolte di dati salvaguardando il vantaggio competitivo degli operatori.

I rischi nei trasferimenti di dati e gli strumenti giuridici di protezione disponibili 10.5.2.

L'indebita appropriazione dei dati da parte di soggetti non autorizzati, così come l'uso dei dati per finalità non consentite, nonché l'incauto inserimento di tali dati nel web, costituiscono tutti atti non solo in grado di eliminare il vantaggio competitivo che la banca dati rappresenta per l'impresa, ma anche di annichilire l'investimento operato per la sua realizzazione e per il suo mantenimento.

Oltretutto dal punto di vista della protezione dei dati personali, è essenziale valutare in che termini avvengono i trasferimenti onde evitare la propagazione di responsabilità ad ogni trasferimento.

Ad esempio, nell'ipotesi in cui un intero database sia reso disponibile in reti peer-to-peer (caso frequente quando ad appropriarsi dei dati sia un ex-dipendente in cerca di rivalsa) potrebbero insorgere responsabilità del titolare del trattamento qualora si dimostri che non sono state adottate le misure di sicurezza adeguate per evitare trattamenti illeciti dei dati.

CASO 1 - Indebita appropriazione dei dati

In relazione all'appropriazione indebita di dati si segnala la sentenza n. 11959/2020 Cass. pen., sez. II, che ha aperto alla possibilità di qualificare i dati informatici e i singoli file come "cose mobili", potendo pertanto costituire oggetto di condotte di appropriazione indebita ex art. 646 c.p. In particolare ad avviso della Suprema Corte, **i dati informatici, per struttura fisica, misurabilità delle dimensioni e trasferibilità, devono essere considerati come cose mobili ai sensi della legge penale** e la condotta volta "non solo all'interversione del possesso legittimamente acquisito" ma altresì a sottrarre definitivamente i dati informatici, "mediante la loro cancellazione, previamente duplicati e acquisiti autonomamente nella disponibilità del soggetto agente", è idonea ad integrare gli estremi del reato di appropriazione indebita ai sensi della normativa penale.

Prima di sviluppare strategie di *data monetization*, occorre pertanto **valutare come proteggere i database**.

Ad oggi la legge protegge le banche dati, il know-how ed il segreto industriale, mentre la meritevolezza di tutela dei dati puri (cioè considerati come singole unità informative), che gioca un ruolo fondamentale per lo sfruttamento del valore commerciale ed industriale, è tuttora incerta.

Ad esempio il c.d. **diritto sui generis** (una forma di tutela *ad hoc* per i costitutori delle banche di dati, introdotta dalla Dir. 96/9/CE e recepita negli artt. 102-*bis* e 102-*ter* della Legge sul diritto d'autore), attribuisce al «costitutore» di una banca di dati il diritto esclusivo di vietare le operazioni di estrazione o di reimpiego della totalità - o di una parte sostanziale - del proprio database nonché le forme di utilizzazione che costituiscono un illegittimo sfruttamento economico del relativo contenuto. Tuttavia, tale forma di protezione non protegge i dati singolarmente presi, ma solo quelli facenti parte di un database, il che esclude tutti quei dati misurati dai sensori o prodotti dalle macchine, perlomeno nella prima fase della loro esistenza, cioè prima di essere raccolti in un database. Ciò genera un vuoto di tutela nello spazio temporale che intercorre tra la produzione dei dati e la loro raccolta a danno del produttore.

La risposta dell'Unione europea - A questa esigenza, fortemente avvertita dagli *stakeholders*, l'UE sta cercando di dare una risposta soddisfacente e chiara come si evince dai recenti sviluppi legislativi, quali la Direttiva per il riuso dell'informazione nel settore pubblico (Dir. 2019/1024/UE) ed il Regolamento sulla circolazione dei dati non personali (Reg. 2018/1807/UE), ma soprattutto dalle varie consultazioni pubbliche lanciate durante gli ultimi anni, tra cui proprio quella dell'agosto 2017 sulla c.d. Direttiva Database (Dir. 96/9/CE), che ha introdotto la protezione sui generis delle banche dati, ma le cui disposizioni non sono - in parte - più adatte all'era di Internet, in particolare in un'epoca in cui i dati sono sempre più diffusi.

10.5.3. Strumenti contrattuali per la riutilizzazione sicura dei dati: la *privacy* come fattore abilitante

A completamento delle protezioni offerte dalla proprietà intellettuale discusse sin qui, è opportuno considerare le limitazioni contrattuali che andrebbero adottate al fine di ottenere una ulteriore protezione dei database da un uso non autorizzato e dalla *disclosure*, permettendo al contempo di condividere e far circolare i dati abilitandone il *safe reuse*, ovvero una riutilizzazione controllata e sicura tramite la predisposizione di una struttura contrattuale appropriata che preveda oltre alle clausole per l'attribuzione dei diritti sui database e sui derivative works, delle precise restrizioni in merito all'anonimizzazione e al trattamento dei dati condivisi, in aggiunta alle apposite garanzie e limitazioni di responsabilità del caso.

Il contratto di licenza - Il contratto tipo nelle transazioni aventi ad oggetto i *database* è il contratto di licenza, tramite il quale il concedente consente che l'altro contraente, il licenziatario, ponga in essere una attività che altrimenti in mancanza di licenza costituirebbe una violazione dei suoi diritti di esclusiva. All'interno dell'ordinamento giuridico italiano, questa tipologia di accordo viene fatta rientrare nella categoria dei **contratti atipici** ossia privi di regolamentazione legislativa *ad hoc*. Da ciò deriva l'assenza di una specifica disciplina suppletiva in grado di colmare eventuali lacune che le parti abbiano omesso di regolamentare in sede pattizia (fatte salve limitate eccezioni e il ricorso analogico al contratto di locazione).

Risulta quindi evidente come la redazione del contratto di licenza rivesta una importanza fondamentale al fine di evitare che eventuali situazioni si rivelino del tutto sprovviste di una disciplina specifica e, successivamente alla sottoscrizione dell'accordo, possano dare luogo a controversie tra le parti. Il contenuto del contratto può essere liberamente determinato dai contraenti, nei limiti imposti dalla legge, purché diretto a realizzare interessi meritevoli di tutela secondo l'ordinamento giuridico.

In ogni caso, se il contratto ha ad oggetto *database* contenenti informazioni che possono essere considerate dati personali ai sensi del GDPR, il trasferimento deve

avvenire mantenendo fermo il rispetto del diritto alla protezione dei dati personali dei singoli individui. Quanto più le informazioni personali sono infatti accessibili alle imprese, tanto più i dati medesimi possono essere messi in pericolo da strumenti e procedure aziendali non adatte o non idonee, le quali utilizzano in maniera non corretta i dati raccolti ed eventualmente organizzati in banche dati.

Nonostante l'adozione dei principi di privacy by design e by default, nonostante venga svolta una scrupolosa valutazione d'impatto (DPIA) e nonostante tutte le tecniche di de-identificazioni adottate, un soggetto con le adeguate risorse potrebbe potenzialmente riuscire a identificare i singoli individui a cui sono riferiti i dati. In tal senso il rispetto della privacy rappresenta il fattore abilitante del *safe reuse*.

Le clausole per limitare la re-identificazione - A seconda delle circostanze, il cedente potrebbe considerare di inserire all'interno del contratto di licenza una serie di previsioni volte a limitare la possibilità di re-identificazione degli individui:

- limitando l'uso del licenziatario ai soli datasets anonimizzati della banca dati;
- proibendo al licenziatario di identificare gli individui o di combinare i datasets con altri al fine di permettere la re-identificazione;
- proibendo l'uso dei dati per fini non autorizzati;
- richiedendo che il licenziatario notifichi prontamente in caso di avvenuta o probabile re-identificazione;
- prevedendo la possibilità di sospendere o interrompere l'accesso al database da parte del cessionario nell'ipotesi in cui si ravvisi il rischio di re-identificazione degli individui e conseguente compromissione del database.

Il licenziatario che non intenda identificare gli individui dal canto suo potrebbe considerare di inserire all'interno dell'accordo una serie di disposizioni volte a:

- assicurarsi che i dati forniti dal cedente siano adeguatamente anonimizzati e siano conformi al GDPR e alla normativa locale applicabile in materia di data protection;
- assicurarsi che il cedente abbia il diritto a trattare dati personali e a cederli a terzi, ed in tal caso verificare l'estensione del consenso acquisito dal cedente ai fini degli scopi di utilizzo previsti e prevedibili; e
- richiedere che il cedente notifichi prontamente in caso di avvenuta o probabile re-identificazione.

Il dilemma della re-identificazione

Le aziende traggono valore dalla possibilità di diffondere le informazioni raccolte. Al fine di permettere la libera trasferibilità (che rientra nelle operazioni di trattamento) dei dati, ma al contempo di bypassare il rischio di incorrere nelle pesanti sanzioni pecuniarie introdotte dal GDPR (fino a 20.000.000 di euro, o, per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore) per le violazioni della disciplina sulla protezione dei dati, le aziende adottano diversi stratagemmi tecnici per rendere non riferibili a persone fisiche particolari, e quindi liberamente trasferibili, i dati in loro possesso.

Il vero valore dei Big Data, soprattutto ai fini della profilazione, deriva però proprio dalla possibilità di poter ricondurre le informazioni raccolte ed aggregate a specifici individui. A questo fine le aziende che comprano dati anonimizzati si occupano di renderli nuovamente riferibili a specifiche persone fisiche tramite procedimenti di re-identificazione. In pratica incrociando i dati anonimi acquisiti da più fonti si riesce a de-anonimizzarli e ad attribuire con esattezza l'insieme delle informazioni estrapolate dai dati alla loro sorgente personale.

10.5.4.

CASO 2 - Possibilità di re-identificazione

Netflix, la società che fornisce video on demand in streaming, è riuscita grazie ai Big Data a rivoluzionare la struttura di una intera industria, semplicemente studiando le abitudini dei propri utenti e riuscendo così a produrre una serie, *House of Cards*, studiata su misura per loro, riscuotendo un enorme successo, che venne preannunciato ancor prima del lancio del primo episodio (S. Ramaswamy, "What the Companies Winning at Big Data Do Differently", in *Harvard Business Review*, giugno 2013).

Nel 2006 la compagnia lanciò il Netflix Prize, una competizione che premiava il team di ricercatori in grado di sviluppare il miglior algoritmo per raccomandare film da vedere agli utenti. Per permettere ai ricercatori di raggiungere il loro scopo, **Netflix rese pubblici i dati anonimizzati** relativi alle recensioni dei film di 500.000 utenti.

Poco dopo nel 2008, altri due ricercatori, durante il Simposio sulla sicurezza e sulla privacy di Washington, rivelarono come erano stati in grado, re-identificando i dati pubblicati da Netflix, di identificare i singoli utenti associandoli ai dati, dimostrando così che **la capacità di identificazione di un dato va valutata alla luce del livello di evoluzione delle tecniche di re-identificazione ragionevolmente disponibili nel mercato**, tenendo conto delle evoluzioni tecnologiche.

Tecniche per condurre l'anonimizzazione - La anonimizzazione dei dati può avvenire in modi diversi. K-anonimizzazione, L-diversità, randomizzazione, generalizzazione, sostituzione, privacy differenziale, sono solo alcuni esempi di tecniche, più o meno note, che sono state prese in considerazione dal Working Party art. 29 (ora European Data Protection Board - EDPB) nel Parere n. 05/2014 sulle tecniche di anonimizzazione.

Le varie tecniche sono state analizzate in base a tre criteri:

- possibilità di individuare l'interessato;
- possibilità di ricollegare i record relativi all'interessato;
- possibilità di dedurre informazioni riguardanti l'interessato, e quali.

Il Parere citato rileva come sia difficile - allo stato dell'attuale tecnologia - realizzare una raccolta dati che sia effettivamente anonima senza far degradare il valore informativo richiesto per lo svolgimento di determinate attività, e che anche se il dato anonimo non ricade nella protezione della legislazione in merito alla protezione della privacy, l'anonimizzazione rappresenta pur sempre un trattamento, come qualsiasi altra operazione compiuta intorno al dato personale. In ultima analisi il Working Party perviene alla conclusione che le tecniche di anonimizzazione in grado di fornire garanzie di riservatezza possono essere efficienti solo se la loro applicazione è progettata opportunamente e che la soluzione ottimale per un possibile scenario va valutata caso per caso, calibrando il grado di anonimizzazione necessario al contesto. Col parere si sottolinea dunque l'importanza (soprattutto per i produttori) di conoscere approfonditamente le varie tecniche di anonimizzazione in modo da poterne sfruttare le potenzialità limitando al massimo i pericoli a seconda dei tipi di dati trattati.

10.5.5. Anonimizzazione VS. Pseudonimizzazione

Come rilevato dall'ENISA nel report "*Recommendations on shaping technology according to GDPR provisions. An overview on data pseudonymization*" di novembre 2018, c'è spesso una certa **confusione tra la nozione di pseudonimizzazione (→12.1.1.) e quella di anonimizzazione** e la loro applicazione pratica. Tuttavia, **queste due nozioni sono chiaramente diverse**, come diverse sono le conseguenze di tali trattamenti sulle potenzialità di utilizzo dei dati personali.

Definizione - La norma ISO/TS 25237:2017 definisce l'anonimizzazione come un "processo mediante il quale i dati personali sono irreversibilmente modificati in modo tale che l'interessato non possa più essere identificato direttamente o indirettamente, né dal solo titolare del trattamento né in collaborazione con altre parti" [ISO, 2017].

Scopo pseudonimizzazione - La tutela introdotta con la pseudonimizzazione è volta a **garantire la confidenzialità del dato**, non più immediatamente intelligibile, ma anche, come avviene nel caso dell'applicazione di tecniche crittografiche, a garantirne l'integrità contro manipolazioni anche accidentali. La rimozione dell'identificativo di un utente è un prerequisito per l'anonimizzazione, ma in generale ciò non è sufficiente a garantire l'anonimato e occorre adottare approcci più sofisticati. In tale contesto infatti le tecniche di pseudonimizzazione sono le più svariate e la loro efficacia dipende anche dalla tipologia di dati oggetto di trattamento e dalla circostanza fattuali del caso concreto. Di aiuto sono certamente le posizioni dell'Enisa che ha in più riprese affrontato la tematica. A mero titolo esemplificativo si rileva come l'Enisa abbia recentemente pubblicato un documento volto a chiarire alcune tecniche di pseudonimizzazione nel settore *healthcare* ("*Deploying pseudonymisation techniques*", Marzo 2022) che, in considerazione delle tipologie di dati oggetto di analisi, è di interesse anche negli altri ambiti.

Scopo anonimizzazione - Nel caso dell'anonimizzazione, la tutela è invece volta a **impedire** - del tutto ed in maniera irreversibile - **la riferibilità del dato a una persona**, salvo il ricorso a mezzi non ragionevolmente utilizzabili. Per questo, si afferma che i dati anonimizzati sono una misura di tutela della privacy, mentre i dati pseudonimi sono una misura di sicurezza.

Pertanto, la re-identificazione è possibile in caso di pseudonimizzazione, mentre in caso di anonimizzazione ciò non è possibile, in linea di principio.

Come suggerito in base al Considerando 26 del GDPR, i dati pseudonimizzati sono comunque dati personali, mentre i dati resi anonimi non lo sono e pertanto mentre l'anonimizzazione consente di utilizzare i dati senza alcuna delle restrizioni previste dal GDPR, i dati pseudonimizzati rientrano comunque nel campo di applicazione della normativa in materia di protezione dei dati personali.

Tuttavia, occorre tenere presente che anche la distinzione fra dati pseudonimizzati e dati anonimi (e poi fra dati anonimi e dati personali) si rivela di carattere giuridico-stipulativo, o comunque una distinzione fondata su una valutazione del livello del rischio di re-identificazione di dati personali, in quanto astrattamente anche i dati anonimizzati possono permettere di risalire ai dati personali, e l'efficacia dell'anonimizzazione deve essere di volta in volta valutata in base all'evoluzione del contesto e dell'ambiente di trattamento dei dati stessi.

Indicazioni per anonimizzare i dati in sicurezza

10.5.6.

L'anonimizzazione si riferisce all'uso di un insieme di tecniche per eliminare la possibilità di collegare i dati ad una persona fisica identificata o identificabile nonostante qualsiasi sforzo "ragionevole". Questo "**test di ragionevolezza**" deve tener conto sia degli aspetti oggettivi (tempo e mezzi tecnici a disposizione) che degli elementi contestuali che possono variare caso per caso (rarietà di un fenomeno al netto della densità della popolazione, la natura e il volume dei dati). Se i dati non superano questo test, allora non sono stati resi anonimi e quindi rimangono nell'ambito di applicazione del GDPR.

La valutazione della solidità dell'anonimizzazione si basa su tre criteri:

- **individuazione** (isolando un individuo in un gruppo più ampio sulla base dei dati);
- **collegabilità** (collegando insieme due record riguardanti lo stesso individuo); e
- **inferenza** (deducendo, con una probabilità significativa, informazioni sconosciute su un individuo).

Esistono molte possibilità per ottenere un'effettiva anonimizzazione, ma con un avvertimento. I dati non possono essere resi anonimi in quanto tali, il che significa che solo le serie di dati nel loro insieme possono essere rese anonime o meno. In questo senso, qualsiasi intervento su un singolo modello di dati (tramite cifratura, o qualsiasi altro trasformazioni matematiche) può essere considerata, nella migliore delle ipotesi, una pseudonimizzazione.

I processi di anonimizzazione e gli attacchi di re-identificazione sono tuttora oggetto di studio. Per ogni titolare che implementa soluzioni di anonimizzazione è fondamentale monitorare i recenti sviluppi in questo campo, soprattutto per quanto riguarda i dati di localizzazione (provenienti da operatori di telecomunicazioni e/o servizi della società dell'informazione), notoriamente difficili da rendere anonimi.

CASO 3 - Dati di localizzazione

Diverse ricerche ha dimostrato che i dati di localizzazione che si pensa siano anonimi possono in realtà non esserlo. Le tracce di mobilità degli individui sono intrinsecamente correlate e uniche.

Pertanto, in determinate circostanze, possono essere vulnerabili a tentativi di re-identificazione.

Un unico modello di dati che traccia la posizione di un individuo per un periodo di tempo significativo non può essere completamente anonimizzato. Questa valutazione può essere ancora valida se la precisione della registrazione delle coordinate geografiche non viene sufficientemente abbassata, o se vengono rimossi i dettagli del percorso ma o l'ubicazione dei luoghi in cui l'interessato ha sostato per un periodo di tempo sostanziale vengono conservati. Ciò vale anche per i dati di localizzazione che sono scarsamente aggregati.

Per ottenere l'anonimizzazione completa, i dati di localizzazione devono essere adeguatamente trattati per soddisfare il test di ragionevolezza. In questo senso, un trattamento di tal genere non può prescindere dalla considerazione complessiva dei set di dati di localizzazione disponibili e dei dati di un insieme ragionevolmente ampio di individui utilizzando le tecniche di anonimizzazione disponibili, a condizione che siano attuate in modo adeguato ed efficace.

Data la complessità dei processi di anonimizzazione, la trasparenza della metodologia di anonimizzazione è fortemente incoraggiata.

10.5.7. Quale base legale per l'anonimizzazione

Il **processo di anonimizzazione dei dati** personali, che riveste una fondamentale importanza al fine di permettere la riutilizzo delle informazioni, è considerato dai Garanti Europei una attività di **trattamento** ulteriore a **tutti gli effetti**. Ciò emerge chiaramente dal Parere sull'Anonimizzazione dell'European Data Protection Board.

Tuttavia tale attività di trattamento potrebbe essere basata - oltre che su altre basi legali quali il **consenso dell'interessato** - sull'**interesse legittimo del titolare**, a condizione che:

- sia svolto il **test di compatibilità** del trattamento ai sensi delle linee guida sulla limitazione delle finalità del Working Party 29;

- sia svolto il **test di bilanciamento** per garantire che il legittimo interesse del titolare sia equamente bilanciato con i diritti e le libertà fondamentali degli interessati.

In tal senso, in base all'interpretazione delle norme, è possibile argomentare che il processo di anonimizzazione e il conseguente trattamento di dati e metadati trovi un fondamento di legittimazione ove, in aggiunta ai requisiti di cui sopra, esso:

- sia svolto **per finalità di analisi statistiche** a fini di miglioramento del servizio prestato all'utente finale;
- preveda una **anonimizzazione irreversibile** dei dati sin dal primo momento possibile;
- **non preveda la diffusione o comunicazione a terzi** dei dati personali eventualmente trattati salvo in caso di informazioni del tutto anonime; e
- preveda la **possibilità per i soggetti interessati di opporsi** a tale trattamento.

In particolare è significativo che i Garanti europei nel citato parere, con riguardo alla liceità del trattamento, prevedano un **parallelismo** ed un richiamo reciproco **tra le discipline in materia di protezione dei dati personali e quella in materia di comunicazioni elettroniche**: si prevede infatti che ove un trattamento di anonimizzazione trovi fondamento in base alla disciplina europea in materia di comunicazioni elettroniche, esso troverà un fondamento corrispondente anche ai sensi della disciplina in materia di protezione dei dati personali.

Questo parallelismo, seppur espresso in un momento storico differente rispetto a quello attuale, è particolarmente decisivo ai fini della corretta interpretazione dei requisiti di liceità del trattamento di anonimizzazione in quanto, relativamente alla sussistenza stessa della liceità, il titolare del trattamento viene accomunato al provider di servizi di comunicazione elettronica, in relazione al quale alcune delle bozze circolate del Regolamento e-Privacy pubblicate nell'arco del 2019 (➔23), prevedono espressamente una eccezione al divieto di trattamento ulteriore dei metadati, nel caso in cui tale trattamento sia effettuato per finalità statistiche o per finalità sostanzialmente allineate alla finalità principale e preveda l'anonimizzazione dei dati trattati.

Appare chiaro che, come affermato dal commissario UE Gunther Oettinger dal palco della fiera internazionale delle tecnologie industriali di Hannover: "abbiamo bisogno di una legge sulla proprietà virtuale e digitale, che includa i dati".

In attesa di auspicabili sviluppi legislativi, per il momento puntando sulla protezione dei dati personali è possibile realizzare strategie di *data monetization* in grado di garantire la raccolta e la circolazione sicura dei dati, favorendo il giusto equilibrio tra esclusione ed accesso.