Trade-off tra Privacy e Security

Prima di analizzare il rapporto vicendevolmente funzionale che lega privacy e security, occorre darne una definizione concettuale.

Il concetto di **privacy** è stato evocato, nel 1890, da Samuel Warren e Louis Brandeis i quali pubblicarono un articolo sulla rivista Harvard Law Review, [1] contenente la prima definizione del cosiddetto "diritto di essere lasciato da solo" (*right to be let alone*).

I due giuristi statunitensi rivendicavano l'esigenza che nei rapporti privati vi fosse un limite all'ingerenza nella vita altrui rappresentato dalla presenza di un interesse pubblico che legittimi la pubblicazione di una notizia. L'aspetto più problematico nell'esperienza americana è stato, quindi, sin da subito quello di trovare un equilibrio tra riservatezza e informazione, tema più che mai attuale dato l'elevato grado di commistione tra tecnologie e aspetti della vita privata. Ancora oggi, a distanza di più un secolo, l'obiettivo rimane quello di individuare dei criteri per stabilire quando, nel bilanciamento tra interesse del singolo e della collettività, quest'ultimo debba prevalere. Questo per dire che le preoccupazioni sorte più di 100 anni fa non hanno ancora ricevuto una chiara risposta.

Nell'esperienza europea, a seguito dell'avvento degli stati totalitari che utilizzavano le informazioni sui loro cittadini per eliminare ogni dissenso politico, il diritto alla riservatezza nasce, invece, come un diritto di personalità connaturato all'idea giuridica di persona fisica e, in quanto tale, trova il suo fondamento nel valore supremo della dignità umana.

Non a caso, infatti, i primi riconoscimenti internazionali del diritto alla Privacy si rinvengono proprio nella Dichiarazione Universale dei Diritti dell'Uomo del 1948 che all'art. 12 condanna le interferenze arbitrarie nella vita privata e nella Convenzione Europea dei Diritti dell'Uomo e del cittadino, che all'art. 8 impone il rispetto della vita privata e familiare.

Con il rapido sviluppo delle tecnologie e con la crescente esigenza di "iperconnettività" (accesso a informazioni fruibili in qualsiasi momento e da qualsiasi piattaforma), il rischio di ingerenza altrui nella propria sfera personale cresce in via esponenziale e si manifesta la necessità di porre dei limiti alla raccolta e all'uso delle informazioni personali. In tale contesto, quindi, il diritto alla riservatezza si arricchisce, cosicchè alla privacy di cui sin ora abbiamo parlato si affianca il diritto alla protezione dei dati personali. Esso è strettamente connesso alla tecnologia digitale, in quanto finalizzato a tutelare gli individui dai rischi derivanti da sistemi di diffusione dei dati personali sempre più veloci e dalle tecniche sempre più sofisticate di utilizzo degli stessi per le finalità più disparate (big data, data mining, marketing, profilazione, fidelizzazione, controllo sociale, influenza dell'opinione pubblica) [2].

Ed è qui che entra in gioco il concetto di **security**, definito come l'insieme di processi, risorse e tecnologie tesi alla protezione dei sistemi e degli asset informativi in termini di riservatezza, integrità e disponibilità.

A causa della crescente informatizzazione della società e dei servizi (pubblici e privati) in termini di asset e sistemi informatici e della parallela diffusione e specializzazione degli attaccanti, l'interesse per la sicurezza informatica è dunque cresciuto in maniera esponenziale negli ultimi anni.

Nella sicurezza informatica sono coinvolti elementi umani, tecnici, organizzativi e giuridici finalizzati ad individuare le minacce, le vulnerabilità e i rischi associati agli asset

informatici, per proteggerli da possibili attacchi sia interni che esterni, i quali potrebbero provocare danni diretti o indiretti di impatto superiore a una determinata soglia di tollerabilità (es. impatto economico, politico-sociale, di reputazione, ecc.).

L'elaborazione massiva e sistematica di dati personali, su cui si basa il trend dei nuovi servizi informatici presenti sul mercato (Internet of Things, Big Data, Machine learning), accresce il ruolo strategico ricoperto dalle tematiche di protezione e sicurezza di tali informazioni.

Uno dei più recenti fattori di crescita del settore dell'information security legato alla protezione dei dati, è considerato il nuovo General Data Protection Regulation (GDPR – Regolamento UE 2016/679) che, come noto, è entrato pienamente in applicazione lo scorso 25 maggio in tutti gli Stati dell'Unione Europea.

La centralità del principio di sicurezza del trattamento dei dati personali emerge, fra l'altro, anche dal considerando n. 83 dello stesso GDPR secondo cui:

"*Per mantenere la sicurezza e prevenire trattamenti in violazione al presente regolamento, il titolare del trattamento o il responsabile del trattamento dovrebbe valutare i rischi inerenti al trattamento e attuare misure per limitare tali rischi, quali la cifratura. Tali misure dovrebbero assicurare un* ***adeguato livello di sicurezza****, inclusa la riservatezza, tenuto conto dello stato dell'arte e dei costi di attuazione rispetto ai rischi che presentano i trattamenti e alla natura dei dati personali da proteggere. Nella valutazione del rischio per la sicurezza dei dati e` opportuno tenere in considerazione i rischi presentati dal trattamento dei dati personali, come la distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati a dati personali trasmessi, conservati o comunque elaborati, che potrebbero*

cagionare in particolare un danno fisico, materiale o immateriale" [3].

Occorre, dunque, porre l'attenzione sui seguenti concetti:

- **adeguato livello di sicurezza** che per essere determinato in maniera corretta richiede capacità analitiche approfondite e conoscenze dei processi di analisi dei rischi e delle tecnologie in uso;
- **migliore tecnologia disponibile** che richiede specifiche conoscenze del mercato e delle tecnologie, nonché budget (notoriamente limitato) da allocare sulle soluzioni ritenute più idonee.

Tali principi di sicurezza vengono inoltre cristallizzati nell'art. 32 del GDPR in base al quale il Titolare del trattamento e il Responsabile del trattamento – tenuto conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalita` del trattamento, come anche del rischio di varia probabilita` e gravita` per i diritti e le liberta` delle persone fisiche – mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre cose:

- la protezione del dato attraverso tecniche di cifratura e similari;
- una continua verifica dell'efficacia dei presidi di sicurezza atti a garantire riservatezza, integrità e disponibilità dei sistemi
- garantire la resilienza dei sistemi informativi per mezzo dell'implementazione dei principi di business continuity e disaster recovery
- un approccio fattuale legato all'esecuzione test di sicurezza (ad es. code review, penetration test e vulnerability assessment applicativi e sistemistici su base periodica) che forniscono dati oggettivi circa l'effettivo livello di sicurezza implementato e gli

eventuali piani di mitigazione da adottare.

Il vasto e complesso tema della tutela della protezione dei dati, nella sua accezione più estesa, non si esaurisce di certo con la sicurezza del dato.

Internet of Things, Intelligenza artificiale, Big Data e Social Network, costituiscono solo una parte delle nuove tecnologie che quotidianamente rischiano di "minare" la fiducia degli utenti, violandone la libertà.

Fra le tante novità del nuovo Regolamento – Data Protection Impact Assessment, Data Protection Officer, Diritto all'oblio, Diritto alla portabilità dei dati, Registro dei trattamenti e il robusto apparato sanzionatorio solo per citarne alcune – si segnala l'art. 25 relativo alla c.d. Privacy by Design e c.d. Privacy by Default.

In particolare, per **Privacy by Design** si intende la necessità di progettare i sistemi informativi in modo da garantire la tutela del dato durante tutto il suo ciclo di vita (data at rest, data in transit). Questo implica la messa in atto di determinati meccanismi in base ai processi, alle tecnologie disponibili e alle tipologie di flussi informatici che caratterizzano quel dato trattamento.

Il concetto di **Privacy by Default**, invece, prevede che il titolare del trattamento metta in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità.

Tali principi, previsti dall'art. 25 del GDPR, introducono concetti di processo ingegneristici atti a garantire la necessità di tutelare il dato sin dalla progettazione di sistemi informatici che ne prevedano l'utilizzo. Precisamente tale norma stabilisce che il Titolare del trattamento – tenuto

conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso – mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.

Già l'attuale Codice della Privacy fa espresso riferimento alla definizione delle PET – Privacy enabling technologies – che del concetto di "privacy by design" costituiscono il fondamento.

Secondo l'art. 3 del D.Lgs. 196/2003 infatti "*i sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità*".

Il tema della Privacy by Design rafforza questo approccio costituendone di fatto il futuro. Secondo il Regolamento europeo, infatti, qualsiasi progetto (sia esso strutturale o concettuale) è necessario che venga realizzato considerando sin dalle fasi di *project design*, ovvero dalla fase di progettazione, la riservatezza e la protezione dei dati personali coinvolti nello stesso.

È auspicabile, dunque, pensare ai concetti di *privacy* e *security* non come ambiti distinti e separati ma come due facce della stessa medaglia, concorrenti – ognuno per la propria

parte – al raggiungimento di un unico obiettivo.

BIBLIOGRAFIA

[1] Samuel D. Warren, Louis D. Brandeis, *The Right to Privacy*, Harvard Law Review, 15 dicembre 1890

[2] *Diritto alla protezione dei dati personali – Data Protection Law | Privacy e protezione dati personali*, in *Data Protection Law | Privacy e protezione dati personali*

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

A cura di: **Roberto De Sortis** e **Anastasia Ambesi**

L’articolo Trade-off tra Privacy e Security proviene da ICT Security Magazine.

https://www.ictsecuritymagazine.com/articoli/trade-off-tra-privacy-e-security/