La privacy oltreoceano

Il framework statunitense

L'Unione Europea è considerata il soggetto che, più di ogni altro a livello internazionale, si è interessato di protezione di dati personali e che, tradizionalmente, ha avviato un percorso di tutela normativa d'avanguardia. Ma siamo proprio sicuri che sia così? L'occasione per rispondere a questa domanda è data dall'avvio in consultazione pubblica, da parte del National Institute of Standards and Technology (NIST)[1], del *"NIST privacy framework: an enterprise risk management tool"*[2] (d'ora in poi, **Framework**).

Il NIST è un autorevole istituto federale statunitense, dipendente dal Dipartimento del Commercio, che ha la missione di promuovere la competitività, il miglioramento della qualità della vita e il potenziamento della sicurezza economica attraverso la definizione di standard scientifici e tecnologici.

Il Framework è un documento che ha l'obiettivo di fornire alle imprese un **riferimento metodologico** per assicurare che i dati personali siano adeguatamente protetti. Il documento è il frutto del consueto stile pragmatico di matrice anglosassone e, in particolare, statunitense; perché, se è vero che le norme americane non sono così giuridicamente *protettive* come le norme europee, l'approccio al risultato che contraddistingue gli yankee è molto più intenso rispetto a quello che caratterizza il Vecchio Continente.

Peraltro, il Framework è uno spin-off di un complesso percorso di studi che il NIST ha condotto, prevalentemente, per fornire indicazioni metodologiche agli Enti Federali americani (uno per tutti: *"An Introduction to Privacy Engineering and Risk Management in Federal Information Systems"*[3], d'ora in poi

PERM). D'altra parte, proprio il trattamento dei dati personali da parte di specifici enti governativi statunitensi (soprattutto a scopi di difesa e sicurezza nazionale) è stato oggetto di specifici approfondimenti nel rapporto dell'European Data Protection Board sul secondo incontro congiunto per la verifica dell'*U.S. Privacy Shield*, pubblicato lo scorso gennaio[4].

In ogni caso, le caratteristiche distintive del percorso tecnico scientifico del NIST sono due:

- viene introdotto il concetto di **privacy engineering**;
- è molto orientato ai sistemi informativi ancorché non vengano affatto trascurati gli aspetti organizzativi.

Privacy engineering vs privacy by design/privacy by default

Il PREM definisce l'ingegneria della privacy (la privacy engineering) come una:

"specialità della più generale ingegneria dei sistemi (la systems engineering) volta a ridurre le condizioni che possono creare problemi per gli individui con conseguenze inaccettabili che derivano da come il sistema tratta i dati personali".

Sembra una definizione che, nella sua vaghezza, la accomuna alle definizioni di privacy by design (privacy fin dalla progettazione):

"tenendo 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 il titolare del trattamento 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";

e privacy by default (privacy per impostazione definita):

"il titolare del trattamento mette 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. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica",

contenute nel nostro GDPR. Tuttavia, il PERM riconosce che i classici Fair Information Practice Principles (FIPPs, molto simili ai principi contenuti nell'art. 5 del GDPR) ovvero trasparenza, specificità della finalità, limitazione della conservazione, ecc., non sono misurabili. E, quindi, il NIST va alla ricerca di **obiettivi di privacy** che possano essere misurabili e che possano assicurare, fin dalla progettazione, un'efficace applicazione dei principi della privacy.

Gli obiettivi di privacy, definiti nel PERM e ripresi dal Framework, costituiscono gli elementi i cui indicatori quantitativi devono essere posti a base della progettazione dei processi di trattamento e dei sistemi di supporto. Per due motivi essenziali:

- per definire parametri che possano diventare pratiche comuni in contesti differenti;
- per garantire l'accountability misurando i progressi nel

tempo.

Per queste ragioni, il NIST stabilisce **tre obiettivi di privacy**:

- *prevedibilità* (*predictability*) ovvero l'obiettivo di misurare, sin dalla progettazione, l'uso che viene fatto del dato personale; è possibile misurare questo obiettivo in vari modi: numero di moduli software che richiamano il dato personale, numero di moduli software che (direttamente o indirettamente) espongono il dato personale a estrazioni massive, ecc.;
- *gestibilità* (*manageability*) ovvero l'obiettivo di calibrare la granularità di gestione del dato personale rispetto a tutte le fasi del trattamento anche per rendere effettiva la possibilità dell'interessato (cioè della persona alla quale i dati si riferiscono) di scegliere, nel tempo, i dati per i quali permettere il trattamento; questo obiettivo può essere misurato, per esempio, attraverso l'inverso del numero di data set in cui ogni attributo personale (nome, cognome, indirizzo email, post ricevuti, post inviati, ecc.) è contenuto. Più è basso questo rapporto meno gestibile sarà il singolo attributo;
- *disassociabilità* (*disassociability*) ovvero l'obiettivo di rendere difficile, se non impossibile, l'associazione dei dati al singolo soggetto; anche in questo caso, è possibile misurare l'obiettivo, per esempio, attraverso il rapporto tra numero di data set crittografati e numero totale di data set.

I dettagli del framework

Inoltre il pragmatismo statunitense completa il suo percorso, all'interno della proposta di Framework, nella definizione di una serie di funzioni che devono essere presidiate per garantire un approccio ingegneristico alla privacy. Ogni funzione, tra l'altro, è specificata in categorie di

interventi molto dettagliati che rispondono a specifiche azioni da condurre.

Le funzioni sono cinque, riepilogate attraverso verbi coniugati all'infinito: **identificare, proteggere, controllare, informare e rispondere**.

Prima di scendere nel dettaglio delle singole funzioni appare significativo che la funzione di informare sia preceduta, logicamente e forse anche cronologicamente, dalle funzioni identificare, proteggere, controllare. Significa che per poter informare correttamente l'interessato è opportuno aver svolto preventivamente le attività di analisi del processo di trattamento dei dati personali e di aver messo in campo i presidi del rischio scaturiti dall'analisi. Non possiamo nascondere che in Italia, nella maggior parte dei casi, i consulenti privacy partono, invece, dalla produzione delle informative per adempiere agli articoli 13 e 14 del GDPR.

La funzione di **identificazione** parte dall'inventariazione dei processi di trattamento, e dei rispettivi strumenti di supporto, per concludersi con la valutazione del rischio, comprendendo i rischi connessi alla catena del valore intesa come l'insieme dei legami che ogni organizzazione ha con il mondo esterno.

La funzione di **protezione** è quella nella quale vengono definite le misure di riduzione del rischio, in termini tecnici e organizzativi. È opportuno che quest'ultimo aspetto sia approfondito compiutamente: non si tratta solo di definire puntualmente i singoli processi di trattamento dei dati personali (p.e. il modo nel quale le analisi cliniche dei lavoratori debbano essere fatte pervenire dal laboratorio che le effettua al medico competente); si tratta di definire anche i processi che, apparentemente, possono non essere strettamente connessi ai dati personali (p.e. l'uso di appositi distruggi-documenti da installare presso le stampanti di rete multifunzione per evitare la dispersione di dati

contenuti nelle stampe malriuscite).

La funzione di **controllo** serve a definire le modalità con le quali si tengono costantemente aggiornate le misure di riduzione del rischio oltre che gli stessi dati personali. In questo ambito, per esempio, rientrano le attività di controllo di qualità dei dati personali che possono basarsi sulle diverse strategie disponibili: confronto con le controparti (ovvero con gli interessati), database bashing, ecc.

La funzione di **informazione** è la tipica funzione che assicura il principio di trasparenza e si basa sulla definizione, anche in co-ideazione e co-progettazione con gli interessati, degli elementi che consentono alla platea dei soggetti di cui si trattano dati personali di averne un controllo effettivo.

La funzione di **risposta** determina i processi di reazione a eventi sfavorevoli che possono, nel peggiore dei casi, culminare in un *data breach* ovvero in conseguenze che, per riprendere la definizione statunitense, "*creano problemi per gli individui con conseguenze inaccettabili*" (nel GDPR si parla di "*rischio elevato per i diritti e le libertà delle persone fisiche*").

Conclusioni

Siamo di fronte, quindi, a un'elaborazione di metodologie e strumenti che, seppur nati in un contesto molto diverso da quello europeo, possono offrire molti spunti di riflessione nei percorsi di *compliance* che le organizzazioni del Vecchio Continente stanno faticosamente articolando.

Note

[1] https://www.nist.gov/

[2] https://www.nist.gov/privacy-framework/working-drafts

[3]

https://www.nist.gov/publications/introduction-privacy-engineering-and-risk-management-federal-information-systems

[4] https://edpb.europa.eu/sites/edpb/files/files/file1/20190122edpb_2ndprivacyshieldreviewreport_final_en.pdf

Articolo a cura di **Francesco Maldera**



Francesco Maldera è Data Protection Officer e Data Scientist.

Il suo percorso professionale lo ha chiamato a responsabilità direzionali nell'ambito dei sistemi informativi, della safety&security, della privacy e dell'auditing svolgendo diversi incarichi dirigenziali nella Pubblica Amministrazione e in aziende private.

Attualmente, accompagna l'attività consulenziale a quella di sensibilizzazione delle persone tramite il sito www.prontoprivacy.it



https://www.ictsecuritymagazine.com/articoli/la-privacy-oltreoceano/