Politecnico di Torino | Nexa Center for Internet & Society

Foresight e regolamentazioni sui dati: stato dell'arte e possibili intersezioni

Autori

Stefano Leucci - lavora nel campo della condivisione, governance e protezione dei dati. Ha arricchito la sua formazione giuridica con competenze informatiche, previsione strategica e studi di futuro. Stefano ha un'esperienza diversificata sia in organizzazioni private che pubbliche.

Giuseppe Vaciago - Avvocato Cassazionista esperto in diritto penale delle nuove tecnologie. Docente di Cybersecurity and Law e Computer Forensics and Cybercrime presso il Politecnico di Torino. Ha prestato la sua attività professionale per alcune importanti società nazionali e internazionali leader nel settore IT. È Lead Auditor ISO/IEC 27001:2013 e DPO certificato UNI 11697:2017.

Introduzione

Da qualche anno, una disciplina apparentemente nuova è emersa sui tavoli di chi si occupa di regolamentazione dei dati: il foresight, anche chiamato “studi di futuro”. Per foresight intendiamo un processo strutturato che mira a prevedere e gestire il cambiamento attraverso l'analisi sistematica di tendenze, sfide e opportunità future. Si fonda sulla raccolta e l’interpretazione di segnali deboli[1], la costruzione di scenari e la valutazione di possibili risposte, al fine di preparare decisioni strategiche resilienti e innovative. Come descritto da Michel Godet, "Il foresight non è tanto un modo di prevedere il futuro, quanto una preparazione a esso, affinché diventi una fonte di opportunità piuttosto che un luogo di incertezza"[2].

Varie organizzazioni pubbliche e private stanno utilizzando il foresight come una nuova cassetta degli attrezzi per gestire in maniera efficiente aspetti come la compliance e l’enforcement.

In particolare, nel campo della protezione dei dati, sono soprattutto le autorità di supervisione ad averne esplorato l’utilizzo: in particolare, EDPS, CNIL e ICO. Questo contributo vuole soffermarsi su queste iniziative per comprenderle meglio, per capire come il foresight stia venendo implementato nelle attività delle autorità di supervisione.

[1] I segnali deboli, noti in inglese come weak signals, sono indizi iniziali di cambiamento o innovazione che, sebbene poco definiti o rilevanti nel presente, possono anticipare sviluppi significativi nel futuro. Riconoscerli e interpretarli richiede attenzione a tendenze emergenti, comportamenti atipici o eventi isolati che potrebbero diventare rilevanti in uno scenario futuro. Per più informazioni si veda H. I. Ansoff, Strategic Management, Palgrave Macmillan, Londra, 2007.

[2] M. *Godet, La Prospective stratégique: Pour les entreprises et les territoires*, Dunod, Parigi, 2007, p. 89

LINC, il laboratorio d'innovazione della CNIL

La prima autorità a mostrare interesse per l'uso del foresight nel contesto della privacy e delle nuove tecnologie è stata la Commission Nationale de l'Informatique et des Libertés (CNIL), l'Autorità francese per la protezione dei dati personali. Fin dal 2011, la CNIL ha costituito un team interdisciplinare dedicato alla produzione di rapporti prospettici, articoli, pubblicazioni, blog e studi empirici, con l'obiettivo di gettare luce sulle tendenze emergenti del futuro.

Un primo esempio è dato da "La plateforme d'une ville"[3] un report incentrato su una analisi delle smart city anche in risposta al nuovo panorama dato dall'arrivo delle grandi aziende di dati, focalizzandosi sulla creazione di nuovi modelli di regolamentazione che rispettino gli individui e le loro libertà. Un'altra dimostrazione dell'interessante lavoro svolto dalla CNIL è data da un libro bianco dedicato ai mezzi di pagamento. Questo libro intitolato "Quand la confiance paie"[4] si concentra invece sulle sfide per la protezione dei dati nei pagamenti individuando ed analizzando le diverse modalità di pagamento attuali e quelle future.

Nell'analisi di questi report emerge un passo in avanti rispetto ai classici documenti di questo tipo che sono disponibili in grandi quantità sui siti delle autorità di regolamentazione. Infatti, gli esperti non solo analizzano con grande precisione le tecnologie, i processi e gli effetti del loro utilizzo, ma proiettano nel futuro quanto appreso per comprenderne meglio le possibili evoluzioni alternative e dunque i rischi connessi ad ognuna di queste. In questo modo, sarà possibile pianificare azioni nel presente che permetteranno di evitare il materializzarsi di alcuni di questi rischi.

In più, questo team vuole tentare di superare il confine dei semplici aspetti legali e tecnici, coinvolgendo dimensioni etiche, sociali, aziendali ed

[3] https://www.cnil.fr/sites/cnil/files/atoms/files/cnil_cahiers_ip5.pdf
[4] https://www.cnil.fr/sites/cnil/files/atoms/files/cnil_livre_blanc_2-paiement.pdf

economiche. Questi elementi multidisciplinari vengono successivamente integrati nelle decisioni e nelle comunicazioni ufficiali promosse dalla CNIL[5].

Uno degli strumenti più utilizzati per raggiungere questo risultato è rappresentato dalla matrice a quattro scenari, come rappresentato più volte dal team di lavoro[6].

Si tratta di uno strumento usato per analizzare e organizzare scenari futuri, prendendo in considerazione due variabili principali che influenzano il contesto in esame. In genere, gli assi della matrice rappresentano variabili incerte ma rilevanti, come tendenze sociali, economiche o tecnologiche. Ogni quadrante della matrice rappresenta un possibile scenario futuro, combinando i valori delle due variabili.

In questo modo, il CNIL riesce a visualizzare chiaramente le principali prospettive e dimensioni del fenomeno analizzato per garantire un quadro giuridico adeguato e una protezione dei dati equilibrata.

L'obiettivo della CNIL è quello di dotarsi di una visione proattiva e anticipante, non limitatamente a specifici settori – come quello tecnologico o di policy – ma in maniera più generale, con il fine di stimolare l'intera struttura da adottare un pensiero più olistico e innovativo. Questa trasformazione permette alla CNIL di espandere la gamma di soluzioni che può offrire, arricchendo così la sua capacità di risposta e la sua proposta di valore in un contesto in continua evoluzione.

[5] A. Rossi, R. Chatellier, S. Leucci, R. Ducato, and E. Hary, (2022) *What if data protection embraced foresight and speculative design?*, in Lockton, D., Lenzi, S., Hekkert, P., Oak, A., Sádaba, J., Lloyd, P. (eds.), DRS2022: Bilbao, 25 June - 3 July, Bilbao, Spain. <https://doi.org/10.21606/drs.2022.681 >

[6] Si veda il panel "Effective enforcement in the digital world" in seno alla conferenza dello European Data Protection Supervisor del 17 giugno 2'022, dove esperti di Foresight hanno discusso gli strumenti più utilizzati nell'ambito delle autorità. Registrazione disponibile al seguente link: https://www.youtube.com/watch?v=bsZNDQgEHTE&t=1450s

TechSonar, per le tecnologie emergenti in EDPS

Il progetto TechSonar dell'*European Data Protection Supervisor* (EDPS) ha lo scopo di identificare le tendenze emergenti nel campo delle nuove tecnologie e della tutela dei dati personali, consentendo di migliorare l'efficacia di politiche e strategie dell'autorità.

Nel tempo, il progetto si è evoluto seguendo l'evoluzione delle necessità di conoscenza tecnologica dell'Autorità. Infatti, l'EDPS è particolarmente esposto a esigenze di comprensione di tecnologie emergenti nel processo di policy making. Per questo, gli esperti hanno diviso il lavoro in due finestre temporali di analisi[7] . La prima, di più breve periodo (1-3 anni), cerca di individuare e approfondire le tecnologie che arriveranno sul tavolo dell'autorità a fronte di azioni già programmate dagli stakeholders istituzionali. La seconda, di più lungo periodo (3-5 anni), cerca di comprendere le prossime novità.

La caratteristica fondamentale di TechSonar è il rigore metodologico che garantisce accuratezza nei risultati. L'approccio si sviluppa attraverso diverse fasi. La prima fase è caratterizzata da uno scouting iniziale, affidato ad un coordinatore interno, il quale si dedica a un monitoraggio continuo di fonti rilevanti online e all'analisi dei dati forniti da piattaforme di settore e proprietarie.

Successivamente, si dà avvio ad una fase di brainstorming collettivo all'interno di una apposita "task force" costituita da esperti interni all'autorità, con l'obiettivo di comprendere le forze che guidano il cambiamento, identificare i segnali deboli e riconoscere le loro interazioni. I risultati di questa fase permettono di identificare quali saranno le tecnologie che, in una finestra temporale prestabilita (solitamente un anno), produrranno i maggiori effetti per quanto riguarda la protezione dei dati personali (es. nuove tecnologie particolarmente invasive e potenzialmente lesive dei diritti dei soggetti interessati). Ciascuna di queste tecnologie è quindi affidata a un "*Tech Champion*", un esperto interno designato che ne segue da vicino lo sviluppo e

[7] Si veda la sezione "Continuous improvement process" a pagina 5 del TechSonar Report 2023 – 2024: https://www.edps.europa.eu/system/files/2023-12/23-12-04_techsonar_23-24_en.pdf

che redige un rapporto dedicato che viene analizzato e discusso dall'intero team di Tech Sonar per migliorare e affinare i risultati.

Al termine, l'esito delle analisi viene pubblicato in un report e viene dato avvio a una serie di attività promozionali e di advocacy sia interne che esterne.

I report riflettono l'evoluzione e la complessità delle dinamiche relative alle tecnologie analizzate, esponendo sia i vantaggi che le sfide connesse a questa pratica emergente nel panorama delle nuove tecnologie e della privacy.

TechHorizon, gli scenari del futuro dell'ICO

Anche l'*Information Commissioner's Office* (ICO), autorità inglese di protezione dei dati, ha avviato una attività di foresight. Più specificamente, l'ICO analizza e valuta le tecnologie emergenti con il fine di agevolare le organizzazioni pubbliche e private nella comprensione di tali tecnologie e dei loro effetti. Il rapporto annuale "TechHorizons"[8] mette in luce le evoluzioni tecnologiche più rilevanti del momento, ma si proietta anche nel futuro, analizzando le potenziali ricadute sulla privacy in intervalli temporali che variano dai due ai cinque anni.

L'ICO utilizza un approccio predittivo per analizzare un elenco di 65 tecnologie emergenti, valutando ciascuna con una matrice di priorità che considera la probabilità e la portata della loro adozione, insieme ai possibili impatti positivi e negativi sui diritti e le libertà delle persone coinvolte. Per determinare i principali fattori e la rilevanza di queste tecnologie, l'ICO ha esaminato vari elementi, come la quantità di persone potenzialmente interessate, la sensibilità dei dati coinvolti, la gravità dei rischi e delle conseguenze per individui e società, i benefici potenziali, e altri aspetti normativi, commerciali e di investimento specifici del contesto britannico.

[8] https://ico.org.uk/about-the-ico/research-reports-impact-and-evaluation/research-and-reports/technology-and-innovation/tech-horizons-report/

Attraverso questo processo di valutazione, l'ICO ha identificato 11 tecnologie con maggiori probabilità di influenzare la privacy nei prossimi anni. Per la selezione e l'analisi delle quattro tecnologie approfondite nel primo rapporto Tech Horizon, sono state realizzate interviste dettagliate con esperti accademici e professionisti del settore, oltre a una serie di workshop per comprendere meglio il futuro sviluppo di queste tecnologie emergenti.

Per esplorare come potrebbe evolvere ciascun settore tecnologico, l'ICO ha collaborato con gruppi di stakeholders chiave per immaginare possibili scenari futuri di adozione e sviluppo tecnologico, e definire azioni suggerite a regolatori e organizzazioni al fine di prepararsi a questi possibili scenari.

Conclusioni

Un approccio proattivo punta a prevedere e a regolamentare l'evoluzione dei fenomeni prima che questi si manifestino pienamente, piuttosto che intervenire solo a posteriori. La meticolosa metodologia dell'EDPS, la visione olistica del CNIL nell'analisi dei fenomeni tecnologici e l'approccio dell'ICO, che si basa sulla previsione degli scenari per comprendere le possibili adozioni tecnologiche nel tempo, rappresentano tre elementi chiave in un progetto di previsione strategica.

Trasportare questo approccio nel contesto di un data protection officer (DPO) richiede di valutare come queste competenze possano essere integrate nelle attività quotidiane. Un DPO, infatti, potrebbe trarre grande beneficio da una formazione mirata nelle metodologie di foresight, che gli permetterebbe di anticipare le sfide emergenti e di adottare misure preventive, evitando così di agire solo di fronte a crisi. La chiave è sviluppare un atteggiamento proattivo nella protezione dei dati, esattamente come suggeriscono i progetti delle autorità analizzate.