DATA PRIVACY DAY OPEN TALK

La necessità di una governance complessiva dei dati per abilitare tutele e innovazione tecnologica

28 Gennaio 2022

ICT Open Talk

SCAI PARTNERS Management Consulting

GRUPPO SCAI

AIEA

Il dato come protagonista di dinamiche globali e riflessioni etiche. Privacy VS nuove tecnologie: l'importanza di un approccio risk-based in uno scenario in rapida evoluzione

Il rapporto tra privacy e tecnologie emergenti, le sfide e le aspettative per il futuro. I flussi di dati come protagonisti di dinamiche geopolitiche; i passi indispensabili per la protezione dei minori; etica e opportunità per le aziende rispetto all'uso dei dati biometrici; l'applicazione pratica dei principi di Privacy by Design e Privacy by Default; i concetti di "accountability" e "data trust" in un contesto globale; la figura del ***DPO*** *come avamposto autorevole e indipendente".*

Questi sono solo alcuni dei temi affrontati durante l'evento ***"Data Privacy Day | Open Talk 2022"****, organizzato da SCAI Partners, società del Gruppo SCAI, con il patrocinio dell'Associazione italiana degli IT Auditor (i.e., AIEA – ISACA Milan Chapter), che ha visto coinvolti una rappresentanza del Garante per la Protezione dei Dati Personali ed ospiti illustri del panorama italiano della privacy:*

- ***Filiberto E. Brozzetti****, Consigliere giuridico del Vicepresidente del Garante per la protezione dei dati personali e docente di Data Protection Law all'Università LUISS Guido Carli;*
- ***Nicola Aliperti****, Data Protection Officer - The Coca-Cola Company Europa;*
- ***Fabrizio Corona****, Partner di e-lawyers, docente di informatica giuridica - Università Telematica Giustino Fortunato;*
- ***Ettore Guarnaccia****, Cybersecurity Manager ed autore di testi sugli effetti di social e digitale sui più giovani;*
- ***Luca Lazzeri****, Data Protection Officer - Italgas;*
- ***Marco Martorana****, Professore a contratto in Diritto della Privacy - Universitas Mercatorum;*
- ***Flavia Messina,*** *Avvocato con esperienza nell'ambito del Diritto digitale e della Protezione dei dati personali, presso l'Ufficio Privacy BPER Banca;*
- ***Mario Mosca****, Data Protection Officer - Gruppo BNPP Italia.*

Un evento in cui si sono alternate voci, prospettive ed esperienze diverse, tutte con il fine unico di promuovere la sensibilizzazione sull'importanza dell'impegno collettivo nel rafforzamento delle tutele privacy.

Ad introdurre il dibattito - moderato da Simona di Felice, Head of Data Gravity & IT Integrated Governance di SCAI Partners – **Guido Scorza**, membro del Collegio del Garante per la Protezione dei Dati Personali, che ha voluto sottolineare nel suo messaggio due sfide principali. In prima battuta, la ricerca di opportune **garanzie per una riapertura delle frontiere nel transito dei dati da UE a Stati Uniti** (n.d.r., di fatto rallentata dalla Sentenza Schrems II del 2020). In seconda battuta, la definizione di **un compromesso tra la realtà economica dello scambio di dati e servizi e la tutela dei diritti fondamentali**, che, in una società democratica, dovrebbero rimanere prioritari rispetto a processi di mercificazione del dato che non sempre corrispondono al valore del dato, basti pensare all'utilizzo delle piattaforme di social network.

Privacy e tecnologie emergenti: le novità più attese nel quadro normativo

Lo spinoso rapporto tra tecnologie emergenti, misure di protezione e tutela dei dati personali è stato affrontato con **Flavia Messina**. Emerge un quadro dinamico e in costante evoluzione e una duplice difficoltà per il legislatore: da un lato, tenere conto dei processi democratici e transnazionali, dall'altro, operare all'interno di un quadro normativo complesso, che si trova quasi sempre a "rincorrere" la rapidissima evoluzione tecnologica.
Le novità più attese sul fronte regolamentare sono il **Regolamento E-Privacy** e le evoluzioni del **Digital Services Act (DSA)** della Commissione Europea. Tra le principali misure promosse da queste normative: la rimozione diretta dei contenuti illegali o nocivi, la responsabilità legale per le Big Tech nei confronti degli utenti, più opzioni per negare il consenso alla pubblicità mirata e una maggiore trasparenza sugli algoritmi. Concetto, questo, indissolubilmente connesso al principio dell'**accountability**.
Altri importanti interventi riguarderanno singoli ordinamenti nazionali, in materia di sicurezza informatica: la **Direttiva NIS per la Cyber Security e la proposta di Regolamento sull'Intelligenza Artificiale**.
Come già successo con il GDPR, ci si augura che anche in questi campi, l'Unione Europea possa assurgere a modello di riferimento normativo anche per gli altri Paesi.

Come cambia la tutela della privacy nel Metaverso: "mixed reality" e dati biometrici. Un'economia senza contatto

Al tema dell'AI si affianca il dibattito sulle conseguenze del consolidamento di una realtà virtuale parallela, il **Metaverso**, e sull'**uso dei dati biometrici**. Con **Ettore Guarnaccia**, sono stati citati alcuni dei riferimenti culturali che hanno creato le basi per l'adozione della tecnologia digitale in tutti gli aspetti della nostra vita, facendo cenno ad alcune tecnologie in via di sviluppo, che vanno di pari passo con una crescita costante della quantità e della qualità dei dati personali: **interfacce e strumenti che interagiscono con il corpo umano ai prototipi BCI (brain-computer interface)**, sui quali già si concentra l'interesse delle multinazionali guidate da Mark Zuckerberg e Elon Musk, algoritmi di **machine learning, AI e teorie di neuromarketing**

per predire e guidare bisogni, comportamenti e reazioni del consumatore, formule di **Mixed Reality** e **Extended Reality**, con l'obiettivo di creare quasi delle **"protesi" ai sensi dell'utente**.
Un'**economia senza contatto**: che si parli di ingegneria, telemedicina, addestramento tecnico o intrattenimento, etc., i rischi per la privacy degli utenti sono gli stessi.
Dal punto di vista aziendale, il social engineering potrebbe favorire lo spionaggio informatico mentre, dal punto di vista dell'utente/consumatore, ci si trova di fronte ad una profilazione sempre più mirata e accurata (eye tracking, finger tracking, real time tagging, ecc.), e per difendersi da fenomeni come **bullismo, shitstorm, molestie, revenge porn**, soprattutto quando l'utente non possiede la consapevolezza necessaria.

Una realtà immersiva, che richiama utenti da tutto il mondo, comporta anche il rischio psicologico di allontanarsi dalla realtà e di danneggiare la qualità delle proprie relazioni: ecco perché principi e regole andrebbero creati con il contributo di rappresentanti delle scienze umanistiche, della legge, della tecnologia, in uno sforzo condiviso.

Esistono già **proposte di regolamentazione del Metaverso**, così come regole per il mercato unico digitale. Ma si tratta, in ogni caso, di proposte.
Un aspetto fondamentale è rappresentato dai **meccanismi di acquisizione e gestione del consenso**, che dovrebbero diventare dinamici, proprio per rispondere alla rapidità dell'evoluzione tecnologica. Questo processo consentirebbe di tenere sotto controllo, almeno in parte, il comportamento delle aziende e il livello di competenza degli utenti sulla capacità di proteggere i propri dati.

Acquisizione dei dati e consenso: un problema etico

Al concetto di consenso, che deve necessariamente diventare più diversificato, si collega il tema delle **modalità di acquisizione dei dati**, su cui si è aperto un interessante dibattito con **Marco Martorana**.
Gli strumenti che interagiscono con il nostro corpo o con il tono della nostra voce - gli smart speaker, ad esempio - comportano osservazioni di tipo diverso rispetto al consenso prestato per l'utilizzo di una piattaforma social. In questi casi, infatti, il dato viene raccolto in modo **"indiretto"** e il livello di consapevolezza del singolo è ancora più basso: il rischio concreto è quindi di generare dei monopoli, dove i consensi vengono prestati quasi senza rendersene conto e chi possiede dati (e metadati) rischia di detenere un potere smisurato. **Il consenso a tali attività rappresenta un problema etico**, soprattutto per le aziende che lo acquisiscono.

Privacy by Design e Privacy by Default: tra obblighi e opportunità per le aziende

L'approccio Privacy by Design va applicato a flussi di informazione, processi e, persone e flussi di informazione, non soltanto al singolo prodotto. Con **Luca Lazzeri** e **Fabrizio Corona**, si è tornati sull'annosa questione di come applicare, concretamente, questo principio e di quali sono le principali sfide che le aziende si trovano a fronteggiare.

Infatti, pur essendo trascorsi ormai quasi 4 anni dall'effettiva entrata in vigore del GDPR, non vi è ancora consapevolezza di quanto sia profondo il processo di trasformazione digitale e di come questo debba coinvolgere le persone, oltre alle infrastrutture. Da un punto di vista organizzativo, per un'azienda, l'approccio prevede un modello generale per la designazione di un Responsabile per la protezione dei dati personali (il DPO), che dovrebbe essere integrato con la definizione di una **regolamentazione interna specifica** e da momenti dedicati alla **formazione delle persone**. Questo ad ulteriore dimostrazione del principio di "accountability" da parte del Titolare del trattamento.

L'approccio Privacy by Design dovrebbe essere inteso dalle aziende come **un'opportunità per migliorare i propri processi digitali**, sia a livello commerciale, ma soprattutto in aderenza ai valori che l'azienda rappresenta e persegue. Non devono essere, infatti, tanto le sanzioni a preoccupare le aziende, infatti, quanto **il danno di immagine e il suo corrispettivo positivo**: la creazione di un'**immagine solida** di azienda che non solo obbedisce ai principi di carattere generale ma, attraverso i suoi modelli interni, stabilisce **fiducia verso i titolari del trattamento**.

Accountability e Data Trust

Il tema della fiducia fa da "leit-motiv" all'intero dibattito, con un focus sul concetto di "accountability"e su quello più nuovo di "data trust".

Dal confronto con **Nicola Aliperti**, emerge che **modelli e tecnologie data-driven** sono ormai parte dei piani strategici di tutte le grandi organizzazioni. All'interno degli scenari che sono stati presentati - compresi i più avveniristici - la **relazione di fiducia** con tutti gli interessati (dipendenti, fornitori, colleghi, consumatori, clienti) e **il rispetto che le aziende trasmettono** assumeranno un valore sempre più significativo nel trattamento dei dati personali: diventeranno un **valore aggiunto**, che rende competitivi e distingue.

L’evoluzione della figura del DPO

Rispetto a come era stata ipotizzata nel 2018, sulla spinta delle trasformazioni tecnologiche, **la figura del DPO aziendale sta subendo una rapida evoluzione**, da entità atomica e a sé stante a struttura organizzativa.

Nella figura del DPO non possono risolversi tutte le competenze possibili, dal piano legale e giuridico a quello normativo, dalle tecnologie alla sicurezza fino ai processi di business. Il DPO deve operare in un **ecosistema** basato su efficaci meccanismi di collaborazione con altre strutture aziendali.

Durante l’intervento con Mario Mosca, il DPO è stato definito come una sorta di “grillo parlante”, con caratteristiche di **terzietà e di indipendenza**, indispensabili a definire con assertività la sua posizione rispetto a quella del titolare.

La **qualità dei dati** trattati in questo panorama complesso acquisisce particolare importanza: tornando a citare i dati biometrici, se una password o un identificativo aziendale possono essere facilmente sostituiti, un data breach che coinvolge dati biometrici va a mettere in pericolo l’identità stessa della persona. L’immagine evocata da Mosca rappresenta un **“Dorian Gray digitale”**, tanto affascinante, quanto inquietante.

Diritti e circolazione del dato: un equilibrio delicato da interpretare caso per caso

L’intervento di **Filiberto E. Brozzetti**, che ha chiuso magistralmente il dibattito, ripercorre tutti gli aspetti trattati dagli altri ospiti, dal punto di vista dello studioso e con l’approccio del Garante.

Si riparte dall’orizzonte internazionale e globale, come scenario nel quale opera il legislatore. Se già la Convenzione 108 del Consiglio d’Europa, risalente ormai a 41 anni fa, forniva una sorta di modello, uno standard che si è diffuso anche in altri Paesi, oggi, a maggior ragione, il Garante deve guardare ai movimenti di quella geopolitica dei flussi di dati che si osservano chiaramente nei tavoli internazionali.

Se non ha più molto senso parlare di frontiere nazionali in un mondo globalizzato dove il dato circola, permane comunque una certa di disparità tra la vecchia Europa e i colossi americani e asiatici in materia di digitale. Non è l’UE a dettare i tempi della tecnologia, e il modello dell’anglosfera, in modo più evidente negli Stati Uniti, sembra preferire una regolamentazione che non stabilisce neanche più una grande differenza tra dato personale e non. **Il digitale non è solo tema di prodotti immateriali:** la battaglia passa anche attraverso le infrastrutture destinate al passaggio dei flussi di dati.

Un sistema valoriale: la rivoluzione copernicana nell'approccio del legislatore

Durante la pandemia, il Garante è stato chiamato a vegliare su un diritto che va contemperato di volta in volta.

L'approccio risk-based consente di passare da una normazione formalista, prescrittiva, standardizzata, a principi più realisti attraverso i quali valutare concretamente i rischi caso per caso: Privacy by Design, Accountability da intendersi come Responsabilità o, meglio, Responsabilizzazione: **una vera e propria rivoluzione copernicana rispetto al precedente approccio del legislatore**.

L'obiettivo è **costruire una struttura programmatica declinata caso per caso da chi meglio di tutti conosce il singolo trattamento, ovvero il Titolare stesso**: perdiamo forse in termini di certezza, ma acquisiamo elasticità. La singola capillarità delle situazioni risponde alla realtà di un mondo complesso. **Un sistema valoriale, più che di meri adempimenti: guardare volta per volta al bene giuridico che andiamo a tutelare**.

Nel discorso sulla globalizzazione e sui flussi di dati si inserisce il tema del "data trust", centrale in molti tavoli aperti quest'anno (durante il G7, per la prima volta, è stata proposta una tavola dei Garanti degli stati appartenenti).

Si osserva inoltre una contiguità e una necessaria **complementarietà tra protezione dei dati e Cyber Security.** In Italia, è stato appena sottoscritto un accordo con l'Autorità Cybernazionale proprio per definire i reciproci spazi di competenza.

DPO: un avamposto del Garante

I DPO non è il Titolare. E neppure un consulente del Titolare.
Il DPO rappresenta la posizione degli interessati all'interno dell'azienda. Perciò, deve essere **indipendente rispetto al core business del titolare, quasi a rappresentare un avamposto, un "garante in miniatura"** all'interno della specifica realtà.

A chiudere l'evento, i messaggi di **Stefano Niccolini, Presidente uscente e membro del Consiglio direttivo di AIEA**, che ha sottolineato la rilevanza di questa materia e l'attenzione riservata dall'Associazione agli aspetti di divulgazione e formazione, non solo tra i soci, e di **Gian Piero Pepino, Corporate Managing Director di Gruppo SCAI**, che ha voluto rimarcare la sensibilità che il Gruppo ha verso i temi trattati e l'impegno di guardare al futuro con una nuova consapevolezza digitale, attenta ai rischi, alle opportunità e alle prospettive per le nuove generazioni.

Guarda gli highlight di Privacy Day Open Talk 2022

GRUPPO SCAI

TORINO
Corso E. Tazzoli 223
10137 Torino
T + 39 011 2273611

segreteria@grupposcai.it
comunicazione@grupposcai.it

P.IVA/CF/Reg Impr. Torino
02710060019

SCAI PARTNERS
Management Consulting

MILANO
Via Benigno Crespi 57
20159 Milano
T + 39 02 607 651

simona.difelice@scaipartners.it

GENOVA
Via Albareto 21
16153 Genova
T + 39 010 6519116

ROMA
Via F.Gentile 135
00173 Roma
T + 39 06 445 7180

SALERNO
Via S. Mobilio 82
84127 Salerno

PALERMO
Via Marchese Ugo 56/13
90141 Palermo

PESCARA
Via G. Mazzini 166
65122 Pescara

ANCONA
Via Isonzo 104/106
60124 Ancona

PADOVA
Via San Crispino 72
35129 Padova

TRENTO
Via dei Solteri 38
38121 Trento

BOLOGNA
Via Pastrengo 2
40123 Bologna
T + 39 051 644 0504

COSENZA
Via Venezia 24
87036 Rende (CS)
T + 39 0984 34 415

BARI
Via F.lli de Filippo
Cassano delle Murge 70020 Bari
T + 39 080 494 9138