Officine Dati

ISLC
Information Society Law Center

POSITION PAPER

GLOBAL DATA CONFERENCE 2023

Officine Dati

GLOBAL DATA CONFERENCE

Prima Edizione

INDICE

LA GLOBAL DATA CONFERENCE 2023 E LE FUTURE EDIZIONI

Il 9 febbraio 2023 si è svolta la prima edizione dell'evento "Global Data Conference", organizzato dall'Associazione Officine Dati e dall'Information Society Law Center dell'Università degli Studi di Milano.

L'iniziativa si è tenuta presso l'Università degli Studi di Milano, in via S. Antonio, n. 5 - Aula Pio XII, e ha ruotato attorno al lavoro di quattro tavoli tematici che hanno visto la partecipazione di oltre 80 esperti del mondo professionale legato alla privacy e di rappresentanti del mondo istituzionale, accademico e delle BigTech.

Figura 1 - La plenaria del mattino.

La GDC ha ricevuto il patrocinio dell'Autorità Garante per la Protezione dei Dati Personali, del Comune di Milano, dell'Ordine degli Avvocati di Milano e dell'Ordine dei Commercialisti e degli Esperti Contabili di Milano.

L'attività di ogni tavolo ha riguardato un argomento specifico.

- La discussione del Tavolo 1 ha ruotato attorno alla '**Strategia Digitale dell'UE**'.
- Il Tavolo 2 ha, invece, affrontato il tema del '**Ruolo e Poteri delle Autorità Indipendenti Nazionali**'.
- Il confronto del Tavolo 3 ha riguardato il tema dei '**Soggetti Vulnerabili ed Effettività delle Tutele**'.
- Infine, il Tavolo 4 ha avuto al centro della discussione il tema della '**Monetizzazione del Dato**'.

L'evento è stato poi integrato dagli interventi di keynote speakers internazionali che hanno affrontato, da aspetti e punti di vista continentali differenti, il tema del digitale, dei dati e delle connesse sfide in Cina, Stati Uniti d'America ed Europa.

Il lavoro dei tavoli si è sviluppato nell'arco della mattina.

Nel pomeriggio, nella sessione Plenaria collettiva, i risultati della giornata sono stati presentati al pubblico dai singoli co-conduttori.

A seguire, il Comitato Organizzatore della Global Data Conference ha elaborato i risultati della giornata per produrre questo Position Paper, successivamente pubblicato dagli organizzatori.

La Global Data Conference intende diventare un punto di riferimento nel panorama scientifico-divulgativo legato ai temi della trasformazione digitale, della protezione dei dati e dello sviluppo della sensibilità tecnologica in Italia. Auspicabilmente, le linee tracciate in questo documento potranno essere d'aiuto e d'indirizzo per l'avanzamento del programma di governo in questi temi.

Il Position Paper va inteso come esercizio collettivo di 'policy draft' uscito da un consesso divulgativo formato da rappresentanti delle istituzioni, ricercatori e professori universitari, e rappresentanti del mondo professionale e delle grandi società tecnologiche.

Il documento è strutturato nel modo seguente:

- La prima sezione indica le caratteristiche e le regole d'ingaggio della Global Data Conference 2023 e presenta i due enti organizzatori, l'Associazione Officine Dati e l'Information Society Law Center dell'Università degli Studi di Milano.
- A seguire, sono riportati i sunti degli elaborati dei singoli tavoli e le rispettive analisi.
- In allegato, sono esposti i risultati del sondaggio propedeutico ai lavori.

GDC 2023, OFFICINE DATI & INFORMATION SOCIETY LAW CENTER UNIMI

La Global Data Conference 2023 si è svolta per l'intera giornata del 9 febbraio 2023, coinvolgendo più di 80 tra i principali esperti italiani ed europei del digitale e della protezione dati, in rappresentanza di istituzioni, accademia e mondo professionale. Ogni tavolo discuteva un tema generale suddiviso in 3 o 4 temi più specifici.

Nella mattina, dopo una breve introduzione ai lavori in Sala Pio XII da parte del Comitato Organizzatore, 4 tavoli di lavoro si sono riuniti in due sessioni da 1 ora e mezza circa affrontando, in modalità collettiva o divisi in sotto-panel, la discussione di analisi rispetto ai temi oggetto dell'iniziativa. Nel pomeriggio, i tavoli si sono riuniti in Plenaria generale in Sala Pio XII e l'iniziativa è stata aperta al pubblico.

Figura 2 – Introduzione della GDC 2023 da parte del comitato organizzatore.

Il Comitato Organizzatore ha quindi proceduto a condurre la sessione collettiva. Per prima cosa, sono stati proiettati gli interventi registrati dei Keynote Speakers internazionali, che hanno portato la loro visione da diversi punti di vista continentali, con focus su Unione Europea e Nord America, letti in un contesto di trend globali.[1] Dopo l'intervento dei Keynote speakers, i coordinatori delle discussioni in ogni tavolo hanno presentato all'assemblea i risultati dei dibattiti della mattina, che sono poi stati analizzati, assemblati, processati e redatti per la stesura di questo Position Paper.

Figura 3 - L'intervento di Ann Cavoukian.

Officine Dati nasce come *think tank* volto a stimolare discussioni e approfondimenti e, più in generale, allargare gli orizzonti e la sensibilizzazione sul tema dei dati (personali e non) e della loro protezione e diffusione. Attraverso eventi, iniziative di confronto, momenti di

[1] **Ann Cavoukian** | Executive Director at Global Privacy & Security by Design Center
Gianclaudio Malgieri | Associate Professor of Law at Leiden University
Patrizia Toia | Member of the European Parliament
Lothar Determann | Partner Baker McKenzie Palo Alto – Professor Freie Universität Berlin Law School

divulgazione e ricerca, l'associazione vuole coinvolgere, nella maniera più completa possibile, quanti più soggetti privati, pubblici, istituzionali e del mondo accademico, con l'obiettivo di divulgare conoscenza nelle tematiche connesse alla protezione e alla valorizzazione dei dati, all'AI, alla cybersecurity, alla tutela delle comunicazioni elettroniche e all'armonizzazione e sviluppo dell'economia digitale. Officine Dati si propone come punto di riferimento in un contesto caotico, caratterizzato da un forte rumore di fondo fatto di sovrapproduzione normativa e di molte voci non sempre supportate da un retroterra conoscitivo adeguato. La missione dell'Associazione è quindi quella di accrescere la consapevolezza che la tutela dei dati è un diritto individuale fondamentale e un caposaldo del principio stesso di democrazia.

L'Information Society Law Center è un centro di ricerca multidisciplinare dell'Università degli Studi di Milano istituito presso il Dipartimento di Scienze Giuridiche "Cesare Beccaria". Nato nel 2017, è un centro dedicato allo studio degli aspetti giuridici, tecnologici, politici e sociali della Società dell'Informazione. L'obiettivo del Centro è quello di condurre ricerche sui temi legati al rapporto tra diritto e società digitale, con particolare attenzione a quei cambiamenti - presenti e futuri - che incideranno profondamente sulla nostra società. Il Dipartimento di Scienze Giuridiche "Cesare Beccaria" è strutturato intorno all'idea, di origine illuministica, che lo studio del diritto non possa prescindere dall'analisi delle istituzioni socio-economiche di base, che sono entrambe influenzate dal diritto stesso e lo plasmano. Il Dipartimento promuove progetti di ricerca interdisciplinari, volti a rafforzare la comprensione delle molteplici connessioni del diritto con le dinamiche socio-economiche sottostanti.

POSITION PAPER

1. STRATEGIA DIGITALE DELL'UNIONE EUROPEA

Il tema della strategia digitale dell'UE è stato affrontato in base ai seguenti profili:

1. Strategia digitale e governo dei dati
2. Sovranità digitale
3. Strategia europea e obiettivi sfidanti

A. Strategia digitale e governo dei dati

Executive summary

I tre pilastri fondamentali della strategia digitale europea

La strategia digitale europea, presentata dalla Commissione europea nel febbraio 2020, si basa su tre pilastri fondamentali:

1. Tecnologie che funzionano per le persone: questo pilastro pone l'accento sul miglioramento delle competenze digitali dei cittadini europei, al fine di garantire che siano in grado di utilizzare le tecnologie digitali in modo efficace e consapevole. Inoltre, s'impegna a fornire l'accesso ai servizi pubblici digitali di alta qualità in tutta l'UE, garantendo che siano inclusivi e accessibili a tutti. Questo pilastro sottolinea anche l'importanza della protezione dei diritti dei cittadini, compresa la privacy e la sicurezza dei dati personali.

2. Un'economia giusta e competitiva: questo pilastro si concentra sulla promozione di un ambiente favorevole all'innovazione digitale e all'adozione delle tecnologie digitali da parte delle imprese europee. Ciò include la promozione degli investimenti nelle tecnologie emergenti, come l'intelligenza artificiale, l'Internet delle Cose, la blockchain e altre. Inoltre, s'impegna a sviluppare infrastrutture digitali ad alta velocità in tutta l'UE, garantendo una connettività affidabile e veloce per tutti i cittadini e le imprese. Un altro obiettivo di questo pilastro è quello di creare un mercato digitale europeo unico, eliminando le barriere che impediscono il libero flusso di dati e servizi digitali tra gli Stati membri dell'UE.

3. Una società aperta, democratica e sostenibile: Questo pilastro si concentra sulla promozione dei valori europei nella sfera digitale. Ciò include la tutela dei diritti fondamentali dei cittadini nell'ambiente digitale, come la libertà d'espressione, la protezione dei dati personali e la lotta alla disinformazione online. Questo pilastro s'impegna anche a garantire la sicurezza cibernetica, proteggendo le infrastrutture digitali e contrastando le minacce informatiche. Inoltre, si propone di utilizzare la tecnologia digitale per affrontare le sfide ambientali, come la transizione verso un'economia a basse emissioni di carbonio.

Le azioni da un punto di vista regolamentare

L'implementazione della strategia digitale europea coinvolge una serie di azioni, tra cui l'elaborazione di nuove leggi e regolamenti, programmi di finanziamento per l'innovazione digitale, collaborazioni pubblico-private e partenariati internazionali. L'obiettivo è promuovere una visione comune di una società e un'economia digitali europee, garantendo allo stesso tempo l'inclusione, la tutela dei diritti e la sostenibilità.

La strategia digitale europea può essere intesa in due sensi distinti, che si completano reciprocamente.

In senso stretto, la strategia digitale si riferisce alle norme europee che disciplinano i dati, compresi i dati personali. Queste norme bilanciano la necessità di garantire la circolazione dei dati come presupposto essenziale per una società digitale avanzata, con la protezione dei dati personali come diritto fondamentale. Il Regolamento generale sulla protezione dei dati (GDPR) è un pilastro importante di questa disciplina. Il GDPR stabilisce regole chiare sulla raccolta, l'elaborazione e la conservazione dei dati personali, proteggendo così la privacy e i diritti dei cittadini europei. Questo quadro normativo fornisce una base coerente per la gestione dei dati all'interno dell'UE.

In senso ampio, la strategia digitale europea si estende oltre la disciplina dei dati personali e include il pacchetto digitale, un insieme di normative europee che mirano a regolare la società digitale nel suo complesso. Questo pacchetto normativo si propone di creare una regolazione comune a livello europeo per promuovere l'innovazione digitale, garantire l'accesso equo ai servizi digitali, promuovere un mercato digitale unico e garantire la sicurezza cibernetica. Inoltre, comprende iniziative per migliorare le infrastrutture digitali e la connettività in tutta l'UE.

Le due interpretazioni si integrano a vicenda: la disciplina dei dati personali, come previsto dal GDPR e altre norme connesse, rappresenta una componente fondamentale per garantire la protezione dei diritti individuali nell'ambiente digitale. Allo stesso tempo, il pacchetto digitale rappresenta una visione più ampia della regolamentazione della società digitale, che comprende la promozione dell'innovazione, la creazione di un mercato digitale europeo unico e la sicurezza cibernetica.

In sintesi, la strategia digitale europea si estende sia alla disciplina dei dati personali che al pacchetto digitale. La protezione dei dati personali e la promozione della società digitale avanzata sono obiettivi strettamente interconnessi all'interno di questa strategia.

Le azioni da un punto di vista tecnologico

Nel Discorso sullo Stato dell'Unione nel settembre 2020, la Presidente von der Leyen ha annunciato che l'Europa dovrebbe garantire la sovranità digitale con una visione comune dell'UE nel 2030, basata su obiettivi e principi chiari. La Presidente ha posto particolare enfasi su Europa Cloud, sulla leadership nell'intelligenza artificiale etica, sull'identità digitale sicura per tutti e sul miglioramento delle infrastrutture dati, supercomputer e di connettività. In risposta, il Consiglio europeo ha invitato la Commissione a presentare una completa Bussola Digitale entro marzo 2021, delineando le ambizioni digitali per il 2030, istituendo un sistema di monitoraggio e delineando gli obiettivi chiave e i mezzi per raggiungerli.

La strategia già delineata in un programma di riforme politiche, iniziate con il Data Governance Act, il Digital Services Act, il Digital Markets Act e la Strategia per la sicurezza informatica, prevede inoltre finanziamenti per costruire la Decade Digitale dell'Europa. Diversi strumenti di bilancio dell'Unione sosterranno gli investimenti necessari per accompagnare la transizione digitale.

Le ambizioni digitali dell'UE sono state concretamente tradotte in una Bussola Digitale in cui sono fissati obiettivi concreti che dovranno essere raggiunti entro il 2030. I principali tra questi obiettivi sono:

- Il Mercato unico digitale presuppone la libera circolazione dei dati tra gli Stati membri e comporta l'armonizzazione delle normative, la riduzione delle barriere e la promozione delle attività digitali transfrontaliere.
- Oltre all'obiettivo sulle competenze digitali di base definito nel Piano d'azione del Pilastro europeo dei diritti sociali che prevede che nel 2030 l'80% degli adulti abbia almeno competenze digitali di base, ci si prefigge di formare 20 milioni di specialisti ICT occupati nell'UE.

- Tutte le famiglie europee saranno coperte da una rete Gigabit, con tutte le aree abitate coperte dal 5G.
- La produzione di semiconduttori all'avanguardia e sostenibili in Europa, compresi i processori, rappresenti almeno il 20% della produzione mondiale in valore (cioè capacità di produzione inferiore a 5nm mirando a 2nm e con un'efficienza energetica 10 volte superiore rispetto ad oggi).
- Il nostro livello di ambizione proposto è che entro il 2025, l'Europa avrà il suo primo computer con accelerazione quantistica aprendo la strada per essere all'avanguardia delle capacità quantistiche entro il 2030.
- Il 75% delle imprese europee adotterà servizi di cloud computing, big data e intelligenza artificiale.
- Più del 90% delle piccole e medie imprese europee raggiungerà almeno un indice di intensità digitale di base[2].
- L'Europa aumenterà il numero delle sue scale-up innovative e migliorerà il loro accesso al finanziamento, portando al raddoppio del numero di unicorni in Europa.

Non manca ovviamente un impegno rispetto alla PA:

- Il 100% dei servizi pubblici chiave sarà disponibile online per cittadini e imprese europee.
- Il 100% dei cittadini europei avrà accesso alle cartelle cliniche elettroniche.
- L'80% dei cittadini utilizzerà una soluzione di identità digitale.

A nessuno può sfuggire il carattere fortemente sfidante di questi obiettivi, ed è convinzione diffusa che difficilmente potranno essere raggiunti. Il gap conoscitivo da recuperare rispetto a queste tematiche è enorme, l'Europa si è accorta nel 2020 che è in atto una rivoluzione digitale iniziata negli anni '80.

Una rivoluzione digitale il cui ingrediente principale è, purtroppo, il know-how.

[2] L'indice di intensità digitale (DII) è un indicatore composito, derivato dall'indagine sull'uso delle TIC e del commercio elettronico nelle imprese. Con ognuna delle 12 variabili incluse che hanno un punteggio di 1 punto, il DII distingue quattro livelli di intensità digitale per ogni impresa: il conteggio da 0 a 3 punti implica un livello base di intensità digitale, da 4 a 6 - basso, da 7 a 9 - alto e da 10 a 12 punti - DII molto alto.

Diciamo purtroppo, perché si tratta di un elemento che non si compra ma che si acquisisce sul lungo periodo, con molta fatica e investendo in formazione e ricerca.

Anche se le diverse tematiche relative alle tecnologie digitali sono sempre state oggetto dei diversi programmi di ricerca finanziati dalla UE, la prospettiva con cui questi programmi erano scritti era quello di facilitare l'adozione e l'uso di queste tecnologie, quindi una prospettiva di "fruitori" di servizi.

Con la strategia digitale europea l'accento viene invece posto sulla capacità di "sviluppare e fornire" servizi, un'inversione di paradigma che può sicuramente essere attuata se supportata dai giusti investimenti, ma sicuramente non nell'arco di un decennio e nemmeno di un ventennio.

Le criticità dell'approccio UE

Due sono le grandi categorie di tecnologie che contraddistinguono il mondo digitale: l'hardware e il software. Queste due anime, che caratterizzano il digitale sin dalle sue origini, si completano a vicenda, un hardware o un'infrastruttura efficiente perdono di ogni significato se gestite da un sistema operativo o da un software inefficienti e viceversa. Da una lettura della strategia europea emerge in modo molto evidente come la stessa sia concentrata nel far assumere un qualche ruolo al nostro Continente nel contesto delle piattaforme hardware e delle infrastrutture, trascurando la componente che queste infrastrutture dovrebbe gestirle: il software. Senza lo sviluppo di conoscenze specifiche in questo contesto e la predisposizione di piattaforme software made in UE difficilmente l'Europa potrà giocare un ruolo significativo nel contesto della trasformazione digitale.

Le norme emanate e in via di emanazione sul tema del digitale che stanno accompagnando la strategia digitale stanno assumendo una numerosità e voluminosità al limite della gestibilità. Questi alcuni commenti a riguardo emersi durante la discussione:

- La questione più evidente, ora, è capire come trasformare lo sforzo normativo in vera innovazione con la creazione di un mercato unico digitale tra gli Stati membri dell'Unione Europea. È evidente, tuttavia, come tutto quanto rappresentato possa comportare anche un rischio di ricaduta di natura contraria: un impianto normativo

troppo stringente blocca innovazione ed economia. È sì opportuna, quindi, una politica sovrana, ma non in valore assoluto: poche ma efficaci norme a fungere da "nodi" di regolamentazione nelle "relazioni" tra dati, tecnologie e scienza dei dati e mercato e servizi digitali, perché altrimenti si rischia di generare una strategia con limitati gradi di libertà/sviluppo. Il quadro del legislatore europeo risulta coerente nella misura in cui le varie regolamentazioni in corso di emanazione e introduzione:

- possano coesistere senza creare frammentarietà a livello dell'Unione;
- possano essere comprese ed effettivamente adottate dalle parti coinvolte, sia europee che di Paesi terzi;
- siano rapidamente e progressivamente modificabili, nel caso emergano incoerenze.
- L'eccessiva frammentazione della regolazione europea e un pacchetto di regole non troppo funzionali può comportare il rischio di incertezza dell'applicabilità delle norme sulla digital economy sia per gli operatori, sia per gli utenti. Questo aspetto dovrebbe essere chiarito nelle successive regolamentazioni oppure attraverso linee-guida emesse dalle autorità di controllo.
- Sicuramente mancano un approccio e una struttura normativa accettata anche internazionalmente con una governance sistemica e coerente con la finalità di utilizzo, in grado di favorire un'economia globale, ma anche la mancanza di un governo delle normative con animo Europeo in grado di determinare un ordine diverso di controllo per non mettere mai in discussione le libertà dell'individuo e i suoi diritti.
- Il legislatore europeo sta adottando regolamenti in diversi ambiti, secondo un modello basato sulla gestione del rischio (per es. regolamentazione dell'AI) e sulla piena responsabilizzazione degli operatori economici privati e pubblici (per es. accountability del GDPR) stabiliti sia in Europa che in Paesi terzi. Si tratta, come noto, di attività che comportano numerosi adempimenti in materia di compliance, dall'analisi dei rischi connessi a ciascuna realtà imprenditoriale, all'identificazione e all'implementazione di misure tecniche e

organizzative (by design e by default), all'ottenimento di certificazioni ecc., attività assai costose in termini di risorse umane ed economiche da impiegare.

B. Sovranità digitale

Executive summary

Il concetto di "sovranità digitale"

La sovranità digitale si riferisce alla capacità di un Paese, di un'organizzazione o di un'entità di esercitare un controllo autonomo e indipendente sui propri affari digitali, compresi i dati, le infrastrutture, le tecnologie e i servizi digitali. L'obiettivo della sovranità digitale è garantire che le entità abbiano la capacità di prendere decisioni autonome e proteggere i propri interessi nell'ambiente digitale, senza dipendere in modo eccessivo da attori esterni.

La sovranità digitale implica diversi aspetti:

- **Controllo dei dati**: La sovranità digitale richiede che un paese o un'organizzazione abbia il controllo dei propri dati, compresi i dati personali, aziendali e governativi. Ciò significa che i dati devono essere archiviati, elaborati e controllati all'interno dei confini nazionali o aziendali, garantendo la sicurezza e la protezione dei dati.
- **Infrastrutture digitali**: La sovranità digitale implica anche l'accesso e il controllo delle infrastrutture digitali, come le reti di comunicazione, i data center e le piattaforme tecnologiche. Un paese o un'organizzazione dovrebbero essere in grado di gestire e controllare le proprie infrastrutture digitali, riducendo la dipendenza da fornitori esterni.
- **Tecnologie e servizi digitali**: La sovranità digitale comporta anche la capacità di sviluppare e utilizzare tecnologie digitali e servizi digitali autonomamente, senza dipendere in modo eccessivo da fornitori stranieri. Ciò può includere lo sviluppo di competenze tecniche interne, la promozione dell'innovazione digitale nazionale e l'adozione di soluzioni digitali locali.

La sovranità digitale può essere considerata come una risposta alle preoccupazioni riguardanti la dipendenza da attori esterni, la sicurezza dei dati, la protezione della privacy e la concorrenza equa nel mercato digitale globale. Molti paesi e organizzazioni stanno cercando di promuovere la propria sovranità digitale attraverso politiche e strategie che favoriscono l'autonomia digitale e riducono la dipendenza da attori esterni.

La sovranità digitale in UE: spunti critici

L'espressione sovranità digitale, ancorché piuttosto di moda, appare se riferita alle politiche UE piuttosto fuorviante.

Le politiche UE mirano infatti a disegnare un modello europeo di società digitale che si possa confrontare con i modelli americano e cinese

Il modello europeo di società digitale si basa su un approccio che mira a garantire un equilibrio tra l'innovazione digitale, la protezione dei diritti dei cittadini e la promozione dell'interesse pubblico. Questo modello cerca di integrare l'aspetto economico e tecnologico della trasformazione digitale con valori sociali, inclusione, tutela dei diritti umani, protezione dei dati personali e sicurezza cibernetica.

Ci sono diversi principi chiave che caratterizzano il modello europeo di società digitale:

- **Protezione dei dati personali**: L'Unione Europea ha adottato il Regolamento generale sulla protezione dei dati (GDPR), che rappresenta uno dei pilastri del modello europeo di società digitale. Il GDPR garantisce ai cittadini europei un elevato livello di protezione dei dati personali e definisce regole chiare per la raccolta, l'elaborazione e la conservazione dei dati personali.
- **Rispetto dei diritti fondamentali**: Il modello europeo di società digitale si basa sul rispetto dei diritti fondamentali, come la privacy, la libertà di espressione, la non discriminazione e la protezione dei diritti di proprietà intellettuale. Si cerca di garantire che la trasformazione digitale non comprometta tali diritti, ma li promuova e li tuteli.
- **Inclusione e accessibilità**: Il modello europeo promuove l'inclusione digitale e cerca di ridurre il divario digitale tra diverse categorie di cittadini. S'impegna a garantire

l'accesso equo e universale alle tecnologie digitali, ai servizi e alle opportunità digitali per tutti i cittadini, indipendentemente dal loro background socio-economico.

- **Sicurezza cibernetica**: Il modello europeo di società digitale pone una forte enfasi sulla sicurezza cibernetica. Si promuovono politiche e norme volte a proteggere le infrastrutture digitali, prevenire le minacce informatiche e garantire la sicurezza dei dati. Ciò include l'adozione di misure di protezione, la cooperazione internazionale e lo sviluppo di competenze nel campo della sicurezza cibernetica.
- **Sostenibilità e responsabilità sociale**: Il modello europeo si impegna a promuovere un'innovazione digitale sostenibile, che tenga conto degli aspetti ambientali, sociali ed economici. Si cerca di garantire che la società digitale contribuisca al raggiungimento degli obiettivi di sostenibilità, promuova la responsabilità sociale delle imprese e affronti le sfide ambientali attraverso soluzioni digitali.

Questi principi guida del modello europeo di società digitale riflettono l'approccio europeo alla trasformazione digitale, che cerca di bilanciare gli aspetti economici e tecnologici con i valori sociali, la protezione dei diritti e la sostenibilità.

La sovranità digitale in altri Paesi

Il modello nordamericano di società digitale presenta alcune differenze rispetto al modello europeo. Mentre entrambi i modelli mirano a sfruttare le opportunità della trasformazione digitale, ci sono alcune caratteristiche distintive nel modello americano:

- **Approccio alla regolamentazione**: Nel modello americano, l'approccio alla regolamentazione è generalmente più leggero rispetto al modello europeo. Gli Stati Uniti tendono a adottare una prospettiva più basata sul libero mercato, favorendo la minima interferenza governativa nel settore digitale. Ciò ha favorito un clima di innovazione e rapido sviluppo di tecnologie digitali negli Stati Uniti.
- **Protezione dei dati personali**: Rispetto al modello europeo, gli Stati Uniti non hanno una normativa unificata e completa sulla protezione dei dati personale comparabile al GDPR. Negli Stati Uniti, la protezione dei dati personali è disciplinata da diverse leggi settoriali, come la legge sulla protezione della privacy dei consumatori della California (CCPA) o l'Health Insurance Portability and Accountability Act (HIPAA) per i dati

sanitari. Questo ha portato a una maggiore frammentazione normativa negli Stati Uniti rispetto all'approccio armonizzato dell'UE.

- **Iniziativa del settore privato**: Negli Stati Uniti, il settore privato, inclusa la Silicon Valley, ha avuto un ruolo di primo piano nello sviluppo della società digitale. Molte delle principali aziende tecnologiche e piattaforme digitali provengono dagli Stati Uniti, e il modello americano si basa fortemente sull'innovazione e l'imprenditorialità del settore privato.
- **Focus sull'economia digitale**: Il modello americano è spesso orientato verso l'economia digitale, enfatizzando l'importanza dell'innovazione, della competitività e della creazione di nuove opportunità economiche attraverso il settore digitale. Ciò ha portato a una rapida adozione di tecnologie digitali e all'espansione delle imprese tecnologiche.
- **Libertà di espressione**: Gli Stati Uniti attribuiscono un'importanza fondamentale alla libertà di espressione, anche nell'ambito digitale. La protezione del diritto alla libera espressione è vista come un principio centrale del modello americano di società digitale, spesso incoraggiando un approccio meno restrittivo rispetto ad alcune regolamentazioni europee sulla moderazione dei contenuti online.

Tuttavia, è importante notare che ci sono anche aree di sovrapposizione tra i due modelli, poiché entrambi cercano di promuovere l'innovazione digitale, l'accesso equo ai servizi digitali e affrontare le sfide della sicurezza cibernetica. Le differenze principali riguardano principalmente l'approccio normativo e le priorità politiche nell'ambito della trasformazione digitale.

Il modello cinese di società digitale presenta differenze significative rispetto tanto al modello europeo quanto a quello americano che riflettono anche le marcate antinomie politiche e culturali. Mentre il modello europeo enfatizza la protezione dei diritti individuali, la privacy e la tutela dei dati personali e quello americano il libero mercato, il modello cinese si basa su una combinazione di controllo statale, sviluppo tecnologico e sorveglianza di massa. Ecco alcune delle principali differenze:

- **Controllo statale e censura**: Il modello cinese è caratterizzato da un forte controllo e supervisione governativa sulle attività digitali. Ciò si riflette nella censura e nel filtraggio dei contenuti online, che limitano la libertà di espressione e l'accesso a informazioni considerate sensibili dal governo cinese.
- **Sorveglianza di massa**: La Cina ha implementato uno dei sistemi di sorveglianza di massa più avanzati al mondo, con tecnologie come il riconoscimento facciale e la raccolta massiccia di dati personali. Ciò ha sollevato preoccupazioni riguardo alla privacy e alla possibile violazione dei diritti umani.
- **Controllo delle piattaforme e delle imprese tecnologiche**: Il governo cinese ha un ruolo significativo nella regolamentazione e nel controllo delle principali imprese tecnologiche del paese, spesso richiedendo la condivisione di dati e l'adesione a direttive governative. Ciò può influenzare la concorrenza e la libertà d'impresa.
- **Protezione dei dati e privacy**: Mentre l'UE ha adottato il GDPR per proteggere i dati personali dei cittadini europei, la Cina ha regolamentazioni sulla protezione dei dati che sono più orientate alla sicurezza nazionale e al controllo governativo. La privacy individuale potrebbe essere sacrificata per favorire gli interessi del governo cinese.
- **Economia digitale e innovazione**: La Cina ha fatto importanti progressi nell'innovazione digitale, diventando un attore chiave nell'economia digitale globale. Ha promosso l'adozione di tecnologie emergenti come l'intelligenza artificiale e l'e-commerce su larga scala. Tuttavia, l'approccio alla concorrenza e alla proprietà intellettuale potrebbe essere diverso rispetto all'UE.

L'adozione di un quadro normativo europeo in materia di società digitale rappresenta una sfida esistenziale per l'Unione europea (UE). Senza un approccio unitario, la transizione digitale potrebbe minacciare il mercato unico europeo sia nei mercati tradizionali che vengono trasformati dall'innovazione digitale, sia nei nuovi mercati digitali.

Se l'UE non interviene tempestivamente, gli Stati membri potrebbero intervenire singolarmente, creando una frammentazione nel mercato unico e ripristinando barriere normative che si ritenevano superate. È quindi essenziale che l'UE assuma un ruolo di guida per garantire un approccio unitario e coerente alla regolamentazione della società digitale.

La sovranità digitale da un punto di vista tecnologico

Per affrontare questo tema anche da un punto di vista di sovranità tecnologica, non si può ignorare la mancanza all'interno della UE di un settore d'avanguardia. La dipendenza digitale dell'UE riguarda sia i prodotti hardware (microprocessori, apparati di rete, computer, ecc.) sia i prodotti software, come browser, motori di ricerca e sistemi operativi, la maggior parte, se non tutti, sviluppati al di fuori dell'UE.

Volendo essere più concreti, uno studio recente commissionato dalla Konrad Adenauer Stiftung (https://digitaldependence.eu/en/) ha mostrato fino a che punto i paesi europei dipendono dalle tecnologie digitali straniere attraverso il cosiddetto Indice di dipendenza digitale (DDI).

Il DDI misura sistematicamente il grado e le tendenze della dipendenza digitale nazionale che va al di là di particolari settori o di determinate tecnologie come i semiconduttori. Questo indice ha valori che vanno da 0 (assoluta indipendenza) a 1 (massima dipendenza), e i cui valori intermedi riportiamo nella sottostante tabella. Dallo studio in oggetto emerge che il grado di dipendenza digitale della maggior parte dei paesi rientra nella categoria di "alta vulnerabilità".

Paesi europei come Italia (0,86), Germania (0,82), Francia (0,84), Estonia (0,8) e Regno Unito (0,82) sono rimasti molto vulnerabili negli ultimi dieci anni. La Cina e gli Stati Uniti, nel frattempo, sono molto meno dipendenti dal digitale rispetto ad altri paesi.

Per raggiungere l'ideale di "autonomia" digitale che attualmente anima i dibattiti politici, i paesi della UE dovrebbero guadagnare nei prossimi anni 10 punti percentuali sul loro indice DDI, impresa riuscita, negli ultimi 10 anni, solo alla Cina.

Detto in altri termini se l'Europa volesse quantomeno sfiorare un ideale di sovranità digitale dovrebbe crescere nei prossimi 10 anni come la Cina. Visti i trend economico/finanziari dei due soggetti degli ultimi dieci, si ritiene che al di là delle buone intenzioni e di tutti gli sforzi, la sovranità digitale potrebbe non essere la corretta strategia da perseguire per la UE.

Degrees of dependence	DDI value	The relation between domestic and foreign supply
Absolute independence	DDI = 0	Autarky.
Low sensitivity	0 < DDI ≤ 0,25	Autonomy very high. Domestic digital technology is in a dominant position.
High sensitivity	0.25 < DDI < 0.5	Domestic supply delivers majority of digital tech. Considerable level of resilience.
Low vulnerability	0,5 < DDI ≤ 0,75	Global markets supply majority of digital tech.
High vulnerability	0,75 <DDI < 1	Autonomy very low. Foreign digital technology is in a dominant position.
Absolute dependence	DDI = 1	Foreign digital technologies fully cover domestic demand.

La rete Internet e le tecnologie dell'informazione e della comunicazione hanno le potenzialità per poter dar vita ad uno spazio cibernetico libero, aperto, sicuro e protetto che può produrre il massimo rendimento in termini di ricadute positive sull'intero pianeta se usato per stimolare la collaborazione e la cooperazione tra tutte le entità che popolano la rete.

Lavorare in un'ottica di sovranità digitale significa rinunciare a queste potenzialità e trasformare la rete globale in una rete di reti chiuse che comunicheranno tra loro solo in base a predefiniti accordi e protocolli. Esistono sfide che la rete ci pone come, ad esempio, la cybersecurity, che possono essere risolte solo attraverso uno sforzo comune e per le quali il discorso di sovranità digitale è solo deleterio. L'auspicio, quindi, è che la UE abbandoni questo approccio e si faccia promotore verso le altre Nazioni di promuovere la condivisione di conoscenze, valori e strumenti. Un'attitudine che è risultata vincente nel superamento della recente pandemia. Questo non significa rinunciare ai propri sogni di indipendenza, ma sostenerli promuovendo lo sviluppo e l'adozione di prodotti e soluzioni che possano contribuire a migliorare lo stato della rete globale, immettendo sul mercato prodotti e soluzioni che contribuiscano a diffondere nella rete i principi di libertà, eguaglianza, dignità e diversità delle persone e che possano contrastare l'affermarsi di una società della sorveglianza, del controllo e della selezione sociale.

C. Strategia Europea e obiettivi sfidanti

Executive summary

Le sfide poste dalla strategia digitale europea

L'adozione di un quadro normativo europeo in materia di società digitale rappresenta una sfida importante per l'Unione europea (UE), anche per contrastare alcune criticità emerse durante la transizione

Per affrontare questa sfida, l'UE deve considerare diversi aspetti chiave:

- Prima di tutto, sono necessarie **competenze adeguate** per gestire la trasformazione digitale in modo efficace. Ciò richiede un investimento significativo nella formazione e nello sviluppo delle competenze digitali, sia per i cittadini che per le imprese. In particolare, è importante diffondere una cultura digitale di base per garantire una partecipazione piena e consapevole alla società digitale.
- Inoltre, è fondamentale garantire una **copertura di rete adeguata** in tutte le zone, comprese quelle rurali, al fine di evitare una "frattura digitale" e garantire che tutti i cittadini abbiano accesso equo ai servizi digitali e alle opportunità offerte dalla società digitale. Questo richiede investimenti significativi nelle infrastrutture digitali, come la connettività a banda larga e l'implementazione di tecnologie come il 5G.
- Un altro elemento critico è una **normativa coerente ed equilibrata** per la società digitale. L'UE deve sviluppare un quadro normativo chiaro che promuova l'innovazione, protegga i diritti dei cittadini e crei un ambiente di fiducia per le imprese. Questo include la protezione dei dati personali, la sicurezza cibernetica, la moderazione dei contenuti online e la promozione della concorrenza leale nel mercato digitale.
- È inoltre essenziale rispettare le **tempistiche dei Piani Nazionali di Ripresa e Resilienza** (PNRR), che sono strumenti chiave per guidare gli investimenti nella trasformazione digitale. L'UE deve garantire che i fondi previsti dai PNRR vengano utilizzati in modo efficace per sostenere la digitalizzazione e affrontare le sfide identificate.

- Per quanto riguarda la **pubblica amministrazione** (PA), sono necessari sforzi significativi per garantire un'interpretazione coerente delle norme digitali e per promuovere una formazione adeguata per i funzionari pubblici. Inoltre, è importante sviluppare competenze digitali specifiche all'interno della PA, al fine di facilitare la trasformazione digitale dei servizi pubblici e migliorare l'efficienza e l'accessibilità.
- Tuttavia, ci sono anche **sfide di governance** da affrontare. È necessario garantire un'adeguata coordinazione tra gli attori chiave, sia a livello nazionale che europeo, per evitare frammentazione e duplicazione degli sforzi. Inoltre, è importante promuovere l'interoperabilità tra i sistemi digitali, sia a livello nazionale che transfrontaliero, al fine di garantire una comunicazione e uno scambio di dati efficienti tra le diverse entità.
- Infine, la questione del **cloud frammentato** rappresenta una sfida significativa. È necessario promuovere l'adozione di standard comuni e garantire l'interoperabilità tra i servizi cloud, al fine di favorire la portabilità dei dati e la scelta degli utenti. Ciò contribuirà a evitare la dipendenza eccessiva da un numero limitato di fornitori e garantire una maggiore sicurezza e autonomia nella gestione dei dati.

Conclusioni

Quando diventerà definitivamente applicabile la "Digital Strategy" europea, sarà da comprendere se (e come) il nuovo quadro normativo in materia di protezione dei dati "resisterà" alle nuove spinte volte alla condivisione dei dati (tra cui anche quelli non personali).

Fermo restando che il nuovo pacchetto di regole europee dovrà essere applicato parallelamente al Regolamento UE 2016/679 e che il GDPR (una delle cui peculiarità è quella di essere "neutrale" dal punto di vista tecnologico) può ancora costituire il testo di riferimento per la protezione dei dati, deve tenersi conto anche della circostanza che l'art. 97 attribuisce alla Commissione il potere di presentare opportune proposte di modifica del GDPR tenuto conto, in particolare, degli sviluppi delle tecnologie dell'informazione e dei progressi della società dell'informazione.

Ulteriore tematica concerne l'architettura della governance delle Autorità di controllo esistenti al fine di evitare un'eccessiva frammentazione e le sovrapposizioni con i nuovi organi introdotti dalla strategia digitale UE: si pensi, per esempio, al "coordinatore dei servizi digitali"

chiamato a vigilare sul rispetto del “Digital Service Act” o al Comitato Europeo per i servizi digitali atteso che, per esempio, con riferimento alla materia della protezione dei dati, le singole Autorità si riuniscono già in seno al Comitato Europeo per la protezione dei dati.

Per quanto riguarda l’Autorità di controllo prevista nelle prime bozze rese pubbliche dello AI Act, lo European Data Protection Board e lo European Data Protection Supervisor, nel parere congiunto 5/2021, hanno chiesto più chiarimenti sul punto della governance. Inoltre, hanno ricordato che le autorità di protezione dei dati stanno già applicando il GDPR, l'EUDPR e il LED ai sistemi di intelligenza artificiale che coinvolgono dati personali, e quindi loro dovrebbero essere segnalate come Autorità nazionali di sorveglianza.

Non da ultimo, ulteriore elemento da cui non si può prescindere è costituito dalla necessità di investire sull’innalzamento delle conoscenze digitali dei cittadini attraverso un’adeguata attività formativa sul corretto utilizzo delle piattaforme digitali allo scopo di rendere sempre più consapevoli gli utenti sulle proprie scelte in materia di protezione dei dati e condizioni contrattuali delle piattaforme digitali in un’ottica di privacy by design e by default.

Nelle modifiche introdotte dal Parlamento EU alla prima proposta di AI Act, e stato introdotto il concetto di AI literacy, cioè, l’obbligo per gli Stati membri di promuovere l’alfabetizzazione, l’educazione, e l’insegnamento di nozioni e abilità di base sui sistemi di IA e sul loro funzionamento.

In sintesi, l’UE si confronta con diverse sfide nella creazione di un proprio quadro normativo per la società digitale. È necessario affrontare questioni relative alle competenze, alla tecnologia, alla normativa, alla pubblica amministrazione e alla governance, al fine di garantire una transizione digitale efficace, inclusiva e sostenibile nel mercato unico europeo.

2. RUOLI E POTERI DELL'AUTORITÀ DI CONTROLLO

Il tema dei ruoli e poteri dell'Autorità è stato affrontato in base ai seguenti profili:

1. Indipendenza delle Autorità
2. Pluralità di Autorità di controllo
3. Cooperazione tra Autorità
4. Poteri sanzionatori

A. Indipendenza delle Autorità

Executive summary

Il concetto di "indipendenza" delle Autorità amministrative va visto alla luce di un'esperienza applicativa che – in tutta l'Unione Europea e quindi anche in Italia – è di più di 30 anni per le Autorità in generale e di 25 anni per il Garante per la protezione dei dati personali.

Pur ritenendo ormai necessaria una riflessione sul tema per l'intero ecosistema delle Autorità amministrative indipendenti, ci si è soffermati sul significato del concetto con riferimento all'Autorità di controllo in materia di protezione dei dati personali (in Italia, il Garante), nella sua attualità e nelle sue possibili evoluzioni.

Il dibattito si concentra su quattro chiavi di lettura dell'indipendenza, considerandola come:

1. esito dei criteri di selezione dei membri del Collegio e dell'Ufficio
2. libertà da condizionamenti dalle altre funzioni dello Stato e dal potere politico
3. autonomia organizzativa e finanziaria
4. competenza settoriale e potere nomofilattico.

Criteri di selezione

1) Indipendenza come esito dei criteri di selezione dei membri del Collegio e dell'Ufficio

Questa chiave di lettura del concetto di indipendenza si rivela significativa adottando la visuale nazionale. Infatti, l'art. 54 del GDPR rimette alle leggi dei singoli Stati la definizione delle qualifiche e delle condizioni di idoneità richieste per essere nominato componente dell'autorità di controllo nonché il varo delle pertinenti norme e procedure.

In Italia, i quattro membri del Collegio sono eletti per legge dai due rami del Parlamento, seguendo una prassi consolidata che ne assegna due alla maggioranza e due all'opposizione. Invece, l'organico (Ufficio) è composto da personale vincitore di concorso, direttamente presso l'Autorità o presso altre amministrazioni.

L'art. 153 del Codice in materia di protezione dei dati personali prevede che i membri del Collegio siano eletti tra coloro che presentano la propria candidatura nell'ambito di una procedura di selezione, che le candidature possano essere avanzate da persone che assicurino

indipendenza e che risultino di comprovata esperienza nel settore della protezione dei dati personali, con particolare riferimento alle discipline giuridiche e dell'informatica.

Proprio come per le altre Autorità indipendenti, anche per il Garante nulla è previsto circa il percorso da seguire per arrivare all'elezione. Nella prassi, i componenti vengono scelti dopo un accordo a porte chiuse fra le segreterie dei partiti e sono votati senza dibattito sui loro profili. Dopo 25 anni di vita dell'istituzione, riconsiderare il concetto di indipendenza significa chiedersi se sia venuto il momento di rendere più trasparente, più aperta al contraddittorio e meglio definita nella sua parte istruttoria la selezione dei componenti delle Autorità indipendenti e quindi anche del Collegio del Garante.

Gli esperti della materia dovrebbero farsi promotori attraverso tutti i corpi intermedi cui afferiscono (partiti, associazioni, comitati, ecc.) di un'integrazione dell'art. 153 del Codice in materia di protezione dei dati personali che imponga una scelta parlamentare più consapevole e più libera.

Per quanto attiene all'Ufficio, le modalità di selezione appaiono idonee a garantire indipendenza.

Libertà da condizionamenti

2) Libertà da condizionamenti dalle altre funzioni dello Stato e dal potere politico

Quando sono nate le prime Autorità indipendenti, appariva implicita la soggezione al Legislativo (nella misura in cui questo rispettava i vincoli europei, ove applicabili), mentre l'indipendenza dall'Esecutivo poteva essere garantita svincolando le sorti dell'Autorità da quelle dell'Esecutivo e della maggioranza parlamentare che lo sostiene e, più in generale, conferendo ad esso una durata predeterminata e un'adeguata copertura finanziaria. Ciò appare tuttora importante, anche se la notevole durata del Collegio del Garante (7 anni) potrebbe essere oggetto di una riconsiderazione.

Tuttavia, se guardiamo all'Italia, negli ultimi 25 anni la divisione di poteri fra Esecutivo e Legislativo è sempre meno chiara. Viviamo un'ipertrofia dell'Esecutivo: la decretazione d'urgenza si è estesa a dismisura, l'iniziativa parlamentare si è ridotta a ben poco. Indipendenza dal Potere Esecutivo, oggi, può significare anche necessità di una dialettica

inedita su scelte legislative fatte sostanzialmente dal Governo. Si è discusso del tema del sindacato del Garante su scelte di merito effettuate dal Legislativo (sempre più spesso, derivante da iniziativa dell'Esecutivo).

L'urgenza di legiferare può rappresentare una situazione in cui i diritti, le libertà e la protezione dei dati personali sono oggettivamente a rischio. Lo si è visto con la pandemia, con una sequenza di atti normativi che hanno toccato in modo evidente aspetti di protezione dei dati personali. Lo si potrebbe vedere con l'acuirsi e l'estendersi del conflitto in Ucraina e di altri conflitti che vedono maggiormente coinvolto il nostro Paese, anche se indirettamente.

L'Autorità di controllo non può né deve sindacare scelte politiche; tuttavia, di fronte a scelte che toccano l'essenza del rapporto fra cittadino e Stato, l'Autorità deve svolgere non solo il compito di consulenza a Parlamento e Governo (lettera c) dell'art. 57 del GDPR), ma anche il **compito di verifica dell'applicazione del GDPR** (lettera a) dell'art. 57 del GDPR).

Ci si interroga anche sul permanere di una doppia velocità nell'attuazione della normativa a protezione dei dati personali fra settore pubblico e settore privato. È unanime l'apprezzamento per la profondità con cui il Garante ha svolto accertamenti e procedimenti nel settore pubblico in ambiti specifici di notevole rilievo. Tuttavia, per il settore pubblico (a partire dai comparti dell'amministrazione statale) vengono auspicate **ricognizioni approfondite sui modelli organizzativi e sulle scelte complessive di conformità**, e un **impulso ad attività di analisi e progettazione** (come la Valutazione di impatto) figlie dell'approccio basato sui rischi.

Autonomia organizzativa e finanziaria

3) Autonomia organizzativa e finanziaria

L'esperienza italiana sul fronte dell'autonomia organizzativa e finanziaria dell'Autorità di controllo in materia di protezione dei dati personali è un caso di successo. Tuttavia, c'è un **margine di miglioramento su due fronti:**

a) **allocazione delle risorse interne e rispetto dei tempi procedimentali;**
b) **orientamento al servizio**.

Sul fronte a), l'Autorità ha regolato il suo funzionamento nei Regolamenti del Garante, ma non è in grado di rispettare i tempi procedimentali che ha definito. È probabile che questo dipenda da insufficienza delle risorse umane. Sono auspicabili trasparenza sul fabbisogno di risorse umane dell'Autorità, rendicontazione sui criteri di allocazione interna delle risorse umane e sul grado di rispetto dei tempi procedimentali (che è elemento qualificante dei livelli di servizio del Garante).

Sul fronte b), si ritiene che l'Ufficio Relazioni con il Pubblico, soprattutto per come attualmente dimensionato e funzionante (perfino negli orari di apertura) non sia sufficiente ad avvicinare l'Autorità ai cittadini. Bisognerebbe considerare il primo supporto a cittadini e imprese come un servizio pubblico essenziale. L'autonomia del Garante verrebbe rafforzata se l'URP diventasse uno sportello operante, anche attraverso i canali digitali, in fasce orarie più estese, eventualmente introducendo un sistema di ticketing. Andrebbe anche fatta una riflessione in merito all'avvicinamento alle comunità di interesse a livello territoriale (ad esempio, regionale).

Competenza settoriale e potere nomofilattico

4) Competenza settoriale e potere nomofilattico

I risultati del questionario del Comitato organizzatore sono un utile punto di riferimento. Alla domanda se si ritiene che sussista il rischio di autoreferenzialità delle Autorità sotto questo aspetto, la maggioranza dei rispondenti (55%) sostiene che "*Sì, spesso le autorità a fondamento delle proprie decisioni fanno riferimento a precedenti loro provvedimenti o linee guida prive di efficacia vincolante verso tutti*".

Non si può imputare all'Autorità un certo timore reverenziale della giurisprudenza nei suoi confronti. E non si può trascurare che il collasso e i costi della giustizia civile scoraggiano ulteriormente l'impugnazione di provvedimenti del Garante e la nascita di correnti interpretative. Tuttavia, **occorre un rafforzamento della cultura della difesa, sia dei Titolari e dei Responsabili che degli interessati**.

Un atteggiamento chiesastico rispetto alla normativa a protezione dei dati personali nuoce alla vita del diritto, creando una sorta di perenne alternativa fra l'applicare gli indirizzi del Garante o il rinunciare a conformarsi. La comunità dei professionisti del settore e degli

studiosi deve **osare la sfida interpretativa**. E occorre lavorare sulla mentalità di Titolari e Responsabili e della magistratura, per evitare l'appiattimento interpretativo.

Anticipatory compliance

Se nel GDPR possono intravedersi tracce – come nella regolamentazione del principio di protezione dei dati sin dalla progettazione – della cosiddetta "anticipatory compliance", qualcosa di simile si potrebbe ipotizzare riguardo alla competenza dell'Autorità. Mediante un'adeguata copertura normativa, i metodi procedurali delle autorità di controllo indipendenti dovrebbero essere impostati tenendo conto dei possibili scenari futuri, con maggiore ricorso a considerazioni di tipo etico e con maggiore attenzione alla sostenibilità.

B. Pluralità di Autorità di controllo

Executive summary

Nel corso dell'ultimo decennio abbiamo assistito a una proliferazione di Autorità indipendenti provviste anche di poteri nomofilattici ed esecutivi. Un nuovo potere che si aggiunge ai tradizionali tre di fonte Montesquieuiana.

Questo processo di proliferazione provoca una molteplicità di competenze e la scelta della loro ripartizione, spesso causando sovrapposizioni e rischio di conflitti. Ne emerge la necessità di un accelerato e adeguato processo di integrazione delle attività di queste Autorità, in grado di non penalizzare l'unitarietà dei processi decisionali complessivi in relazione a obiettivi e progetti evoluti.

Proliferazione di Autorità

Con l'enunciazione della strategia digitale dell'Unione e la sua prima fase applicativa si assiste ad un processo di proliferazione di Autorità amministrative indipendenti cui è affidato il compito di supervisione dei singoli temi oggetto della specifica normazione unionale.

L'oggetto di riferimento di questa normazione è variabile; esso può consistere in

- **un bene**, come nel caso del Regolamento generale sulla protezione dei dati personali (GDPR)

- **uno strumento**, come per la proposta di Regolamento sull'intelligenza artificiale (AI Act)
- **un processo**, come per il Regolamento sul governo dei dati (DGA)
- **un impatto**, come per il Regolamento sui mercati digitali (DMA).

In generale, la previsione – quindi, l'istituzione – di una specifica Autorità di supervisione "segue" la norma e il perimetro del suo ambito applicativo, con la conseguenza che a ogni fenomeno regolato nell'ambiente digitale, corrisponde un'Autorità indipendente. Questo modello, inevitabilmente, innesca un processo di **proliferazione di Autorità** e di potenziale **sovrapposizione di competenze**.

In aggiunta, la norma unionale riconosce il potere discrezionale degli Stati membri di decidere, per ciascuno degli ambiti applicativi di riferimento, se istituire un'Autorità *ad hoc* o, in alternativa, accorpare le competenze previste dalla norma a quelle di un'Autorità già esistente. Ne consegue che, a livello europeo, si può registrare un'accentuata **diversificazione di approccio** in questo contesto, con gravi ripercussioni riguardo ad un'auspicata attività di cooperazione e sinergia.

Questa tendenza – apparentemente più dovuta a un effetto collaterale piuttosto che essere derivata da una scelta strategica – rischia di vanificare il tradizionale sforzo delle istituzioni dell'Unione europea verso una maggiore armonizzazione unionale a tutti i livelli.

La constatazione della pluralità di Autorità di controllo indipendenti nazionali solleva l'interrogativo dell'adeguatezza di questo tipo di framework di controllo rispetto alla governance dei fenomeni che queste stesse Autorità sono chiamate a supervisionare.

Pluralità di competenze

La tendenza verso la proliferazione delle Autorità si accompagna al processo di moltiplicazione delle competenze assegnate, sempre più **numerose ed estese, che spesso si intersecano e si sovrappongono**. Anche su questo versante si intravede l'insorgere di **rischi di segmentazione e conflitti di competenza** a danno dell'esigenza del governo unitario dei processi: come quelli caratterizzati dallo sviluppo tecnologico e dalla trasformazione digitale.

Ripartizione di competenze

La moltiplicazione delle competenze assegnate a una pluralità di Autorità pone il problema della loro ripartizione. L'assegnazione delle competenze deve essere chiara – cioè, agevolmente riconoscibile – e specifica, cioè, individuata in modo preciso e corrispondente alle finalità perseguite dalla norma istitutiva dell'Autorità.

In ogni caso, il **binomio competenza/Autorità**, se replicato numerose volte, porta a una compartimentazione delle *expertise* e a una **frammentazione del processo decisionale** complessivo. Queste condizioni, se consolidate, possono rallentare o addirittura ostacolare **l'approccio per obiettivi** che, invece, è connaturato all'ambito imprenditoriale e al più generale sviluppo economico.

Integrazione fra Autorità

Il richiamato binomio competenza/Autorità innesca anche un processo di **verticalizzazione degli ambiti di intervento** delle singole Autorità, col rischio di segregazione delle attività, se non persino di conflitti tra le stesse. Questo induce a un ripensamento dell'attuale modello di articolazione delle attività e dei compiti delle Autorità, promovendo **nuovi modelli di convergenza** finalizzati alla **cooperazione** e all'**efficientamento**.

Sebbene il tema della cooperazione fra Autorità sia indirizzato in modo specifico in seguito, sembra opportuno farne cenno anche in ambito di discussione in merito alla pluralità di Autorità.

In aggiunta agli attuali **protocolli di intesa**, che non sembrano aver sortito risultati significativi, è ipotizzabile una **Conferenza dei servizi digitali** con un organo di raccordo che preveda la costituzione di un **forum** volto al confronto costante tra le diverse Autorità chiamate al controllo indipendente di tematiche connesse/relative al digitale in senso lato. Una sorta di "**corpo integrato**" – avente caratteristiche di composizione fissa, unificata e ricorrente – che svolga una funzione olistica, coordinata e sinergica, finalizzata a evitare i sovra citati rischi di duplicazioni e/o frammentazioni di funzioni attribuite alle differenti Autorità di controllo indipendenti.

Un esempio pratico in questa direzione riguarda la costruzione di **città cognitive** in grado di utilizzare i dati per mettere al primo posto le esigenze dei cittadini e dell'ambiente circostante, come il caso del **progetto NEOM**. Ad oggi, le città intelligenti utilizzano solo l'1% dei dati generati dai residenti. Una città cognitiva potrebbe sfruttare fino al 90% dei dati ottenibili dalla popolazione. Questo consentirebbe di potenziare i servizi al cittadino, dall'accesso all'istruzione, al miglioramento delle prestazioni sanitarie digitali. La connessione digitale agli oggetti fisici che compongono le nostre città, in modo che il calcolo e l'analisi dei dati permetta di contestualizzare le necessità in modo più efficiente e facilitare le decisioni, non può prescindere da un **modello di cooperazione integrata fra Autorità indipendenti**. Alla base, la *ratio* di questo tipo di intervento sarebbe quella di intervenire per la risoluzione di problematiche come la dispersione di risorse, la disconnessione sociale, l'inquinamento, il traffico e l'esaurimento delle risorse del territorio e del pianeta.

Asimmetrie strutturali delle Autorità

Indubbiamente, le citate proposte devono tener conto delle asimmetrie strutturali tra le diverse Autorità, determinate da differenze nelle risorse disponibili, nei poteri attribuiti e nello stesso percorso effettuato da queste istituzioni nel corso degli anni.

C. Cooperazione tra Autorità

Executive summary

La cooperazione tra Autorità presenta margini di miglioramento strettamente connessi agli scenari di seguito indicati:

- **a livello europeo**, risulta necessario ridurre gli ostacoli procedurali, determinati dalle diverse tradizioni giuridiche degli Stati Membri, mediante specifici progetti legislativi;
- analogamente, **a livello nazionale**, emerge la necessità che vengano predisposti strumenti normativi per rendere strutturale la cooperazione tra Autorità, definendo per esempio strutture congiunte di cooperazione (es. task force);
- infine, è fondamentale che gli Stati Membri colgano le opportunità che vengono offerte dalle **nuove normative** predisposte (es. Digital Services Act, Digital Markets

Act) o in corso di predisposizione (es. Artificial Intelligence Act), individuando la corretta collocazione delle nuove competenze legate a tali atti normativi.

Introduzione

Dall'analisi delle risposte al questionario somministrato ai partecipanti alla Global Data Conference, la **collaborazione tra Autorità risulta insufficiente**, ma **il numero delle Autorità attualmente esistenti è ritenuto adeguato**.

Pur nell'apprezzamento per gli sforzi registrati in relazione alla cooperazione tra Autorità, vengono rilevati **diversi aspetti migliorabili**. In generale, i tre scenari di cooperazione possibili possono essere qualificati come segue:

1. cooperazione tra autorità di controllo indipendenti nazionali di **diversi paesi UE** preposte alla supervisione della **medesima materia** (ad esempio, con riferimento alla data protection, una collaborazione tra il Garante privacy francese e il Garante privacy italiano);
2. cooperazione tra autorità di controllo indipendenti nazionali preposte alla supervisione di **materie differenti**, relative al digitale, **all'interno dello stesso paese UE** (ad esempio, una collaborazione tra Garante privacy e AGCM);
3. cooperazione tra autorità di controllo indipendenti nazionali di **diversi paesi UE** preposte alla supervisione di **materie differenti**, relative al digitale (ad esempio, una collaborazione tra autorità per la protezione dei dati e autorità di regolamentazione e controllo delle telecomunicazioni, come potrebbe essere ipoteticamente una collaborazione tra il Garante privacy francese e l'AGCOM).

Cooperazione tra Autorità UE preposte alla stessa materia

Cooperazione tra autorità di controllo indipendenti nazionali di diversi paesi UE preposte alla supervisione della medesima materia

Un esempio riferibile a questa tipologia di cooperazione potrebbe riguardare, nell'ambito della data protection, una collaborazione tra CNIL (autorità francese) e il Garante privacy italiano.

In linea generale, la cooperazione tra autorità indipendenti nazionali preposte alla supervisione della medesima materia **risulta strutturata, per quanto sia migliorabile**.

Dal punto di vista dell'*European Data Protection Board* (EDPB), a titolo esemplificativo, sono state individuate 639 decisioni finali (dal 2018 al 31/12/2022) pervenute a consenso, di cui solo 7 sono state oggetto di una decisione vincolante dell'EDPB, ai sensi dell'art. 65 del GDPR. Le tipologie di cooperazione rilevabili possono essere riassunte come segue:

a) **cooperazione proattiva**, finalizzata alla predisposizione di un'interpretazione congiunta e preventiva in merito ad uno specifico tema concordato; in tal senso, le linee guida sono il risultato di tale cooperazione;
b) **cooperazione reattiva**, finalizzata a dirimere una questione emersa con riferimento ad un caso concreto. Per esempio, si pensi alle attività svolte in relazione alla task force dell'EDPB dedicata ai reclami proposti da None Of Your Business (NOYB) in merito alla gestione dei cookie[3].

Emerge tuttavia che vi siano rallentamenti in relazione a specifiche tematiche particolarmente complesse, le quali non vedono il raggiungimento di un compromesso in tempi brevi (es. monetizzazione del dato). In tal senso, la cooperazione potrebbe **focalizzare le priorità** in modo da sostenere le imprese del mercato che risentono di tali rallentamenti.

Inoltre, esistono alcuni **ostacoli alla cooperazione**, tra cui emergono in particolare le differenze procedurali che caratterizzano ogni Stato membro. Queste differenze derivano primariamente dalle diverse tradizioni giuridiche proprie di ogni Stato membro. Tali differenze procedurali sono state riconosciute come un effettivo ostacolo al meccanismo del *One Stop Shop* promosso dal GDPR. Pertanto, nel momento in cui viene gestito un caso transfrontaliero, vi sono delle barriere legali e operative che generano ostacoli importanti alla cooperazione. Una possibile soluzione a tale inefficienza è la definizione di **progetti legislativi di miglioramento della cooperazione**. In tal senso, la Commissione europea ha inserito nel

[3] Cfr. edpb.europa.eu, Report of the work undertaken by the Cookie Banner Taskforce, https://edpb.europa.eu/our-work-tools/our-documents/other/report-work-undertaken-cookie-banner-taskforce_en.

programma di lavoro un progetto per eliminare (o quantomeno ridurre) gli ostacoli giuridici e amministrativi in ambito transfrontaliero[4].

Cooperazione tra Autorità nazionali preposte a differenti materie ma nell'ambito del digitale

Cooperazione tra autorità di controllo indipendenti nazionali preposte alla supervisione di materie differenti relative al digitale, all'interno dello stesso paese europeo

Un esempio riferibile a questa tipologia di cooperazione potrebbe essere una collaborazione strutturata tra Garante Privacy e AGCM.

Attualmente può già registrarsi una cooperazione tra autorità di controllo nazionali preposte alla supervisione di materie differenti, ma tale cooperazione **non risulta strutturata**.

In questo contesto, si può accennare alla sentenza del **Consiglio di Stato relativa a Facebook e AGCM**[5] oppure a livello europeo alle conclusioni dell'Avvocato Generale riferibili ad un **provvedimento dell'autorità tedesca per la concorrenza contro Meta**[6]. In questi casi, vi è stata una sovrapposizione tra le competenze data protection e antitrust, ma senza che vi sia stata una comunicazione tra le relative autorità. In tal senso, anche l'Avvocato Generale nelle citate conclusioni ha affermato che sarebbe necessario che le autorità mantenessero i contatti per tenere traccia e considerazione dei rispettivi punti di vista. Esaminando il caso italiano, non vi è una normativa che impone alle autorità di cooperare; pertanto, le collaborazioni in larga parte sono un atto volontario delle Autorità stesse, le quali definiscono protocolli di intesa per la condivisione di informazioni. In assenza di una norma regolatrice, vi è quindi il rischio che vengano realizzate istruttorie "fotocopia", le quali determinano, quindi, sovrapposizioni di contenuto.

[4] Cfr. europarl.europa.eu, Legislative Train Schedule, Proposal for a Regulation on a Mechanism to resolve legal and administrative obstacles in a cross-border context, https://www.europarl.europa.eu/legislative-train/theme-an-economy-that-works-for-people/file-mff-mechanism-to-resolve-cross-border-obstacles.
[5] Cfr. Cons. Stato, Sezione VI, 29 marzo 2021 n. 2631, https://www.giustizia-amministrativa.it/portale/pages/istituzionale/visualizza/?nodeRef=&schema=cds&nrg=202001825&nomeFile=202102631_11.html&subDir=Provvedimenti.
[6] Cfr. Conclusioni dell'Avvocato Generale Athanasios Rantos, Causa C-252/21, https://curia.europa.eu/juris/document/document.jsf;jsessionid=64A1E9F024B440B7EC7642BF7697B046?text=&docid=265901&pageIndex=0&doclang=IT&mode=req&dir=&occ=first&part=1&cid=209721.

È d'auspicio che a livello normativo vengano predisposte **strutture congiunte di cooperazione**, da avviare nel momento in cui è necessario deliberare in relazione ad un caso specifico oppure da avviare in modo sistematico e periodico.

Cooperazione tra Autorità UE, preposte a differenti materie ma nell'ambito del digitale

Cooperazione tra autorità di controllo indipendenti nazionali di diversi paesi UE preposte alla supervisione di materie differenti relative al digitale

Un esempio riferibile a questa tipologia di cooperazione potrebbe essere un'ipotetica collaborazione tra il CNIL francese (autorità privacy) e l'Autorità italiana per le garanzie nelle comunicazioni (AGCOM).

In questo contesto, **non esiste ancora un livello di cooperazione definito**. Infatti, il diritto dell'Unione europea non prevede norme specifiche per la cooperazione tra Autorità di diversi settori.

Analogamente a quanto indicato per la cooperazione tra Autorità nazionali preposte a materie differenti, l'eventuale cooperazione, in modo da tenere conto dei rispettivi punti di vista, è su base discrezionale. Sebbene potrebbe sin d'ora farsi ricorso al principio della leale cooperazione, è necessario un enforcement maggiore per sistematizzare tali collaborazioni.

Si auspica, pertanto, **l'adozione di norme che determinino strutture funzionali di cooperazione**, che operino in via preventiva. Queste nuove norme renderebbero la cooperazione un obbligo di legge. In tal senso, alcune anticipazioni possono cogliersi nei livelli di cooperazione definiti nel Digital Services Act[7], nel Digital Markets Act[8], nonché nelle

[7] Cfr. Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali), Capo IV "Attuazione, cooperazione, sanzioni ed esecuzione", https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32022R2065&from=EN#d1e4753 -1-1.

[8] Cfr. Regolamento (UE) 2022/1925 del Parlamento europeo e del Consiglio del 14 settembre 2022 relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive (UE) 2019/1937 e (UE) 2020/1828 (regolamento sui mercati digitali), artt. 37-39, https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32022R1925&from=EN#d1e3503-1-1.

proposte di Regolamento sull'Intelligenza Artificiale[9] e di Data Act[10]. In questo modo sarà possibile **strutturare forme di collaborazione funzionali**.

D. Poteri sanzionatori

Executive Summary

Un sistema sanzionatorio basato unicamente sulla sanzione pecuniaria, come quello previsto dal GDPR, rischia di portare le imprese e gli enti a considerare la **sanzione come un costo da computare nell'attività di impresa** e potrebbe rappresentare per le PMI un costo sproporzionato con **effetti distorsivi sul mercato**, senza assicurare un'efficace tutela dei diritti e libertà degli interessati.

La sanzione non dovrebbe avere una funzione meramente punitiva ma dovrebbe puntare ad **aumentare il livello di *accountability* e incentivare la conformità** alla norma.

Di conseguenza, gli strumenti individuati per perseguire questo fine potrebbero essere

- regolamentazione interna delle autorità di supervisione,
- modulazione delle sanzioni,
- trasparenza e destinazione degli introiti.

Regolamentazione interna delle Autorità di Supervisione

- **Migliore definizione e trasparenza dei processi interni sanzionatori.** È d'auspicio l'adozione di nuovi strumenti di regolamentazione interna, per una maggiore definizione delle attività di accertamento, verifica e contestazione, in modo da garantire:

[9] Cfr. Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione, Titolo VI "Governance", Capo 1 e 2, https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52021PC0206&from=EN. All'atto della pubblicazione di questo Position paper, la proposta di regolamento risulta aver completato il suo iter approvativo ma si è ancora in attesa della sua pubblicazione in GUCE.

[10] Cfr. Proposta di regolamento del Parlamento europeo e del Consiglio riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo (normativa sui dati), Capo IX "Attuazione ed esecuzione", https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52022PC0068&from=EN. All'atto della pubblicazione di questo Position paper, la proposta di regolamento risulta aver completato il suo iter approvativo ma si è ancora in attesa della sua pubblicazione in GUCE.

  - il rispetto del diritto alla difesa (gli *Engel criteria,* rif. Corte Europea dei Diritti Umani, sent. Grande Stevens),
  - un'efficace tutela degli interessati e
  - l'applicazione della norma.
- **Certezza dei tempi.** È d'auspicio l'adozione di misure volte a favorire una maggiore **trasparenza dei criteri seguiti** dalle autorità nazionali nella gestione dei procedimenti amministrativi e una maggiore **certezza dei tempi di definizione** dei procedimenti sanzionatori.
- **Armonizzazione unionale dei principi.** Le norme di regolamentazione (criteri di determinazione delle sanzioni, struttura dell'attività ispettiva, individuazione delle categorie di soggetti da sottoporre ad accertamento, alle modalità di avvio delle ispezioni, esercizio del potere sanzionatorio in genere) dovrebbero essere inserite in un contesto di armonizzazione a livello unionale tramite verifica dell'European Data Protection Board.

Modulazione delle sanzioni

- **Utilizzo di strumenti alternativi.** Viene auspicata una differente modulazione delle sanzioni. Uno strumento di azione potrebbe essere la creazione di griglie che distinguano le categorie di violazioni, il range delle sanzioni e le categorie di soggetti destinatari delle stesse. In particolare, la posizione delle PMI dovrebbe essere oggetto di specifica valutazione, al fine di fornire criteri sanzionatori proporzionati alla dimensione dell'azienda. Le linee guida EDPB 04/2022 nella versione finale sembrerebbero andare in questa direzione. Si potrebbe valutare l'introduzione di nuovi strumenti quali, sul modello già adottato dalle autorità *antitrust* (provv. Antitrust 25/09/2018, res. SIAE), l'irrogazione di sanzioni simboliche in modo da consentire la prevalenza degli strumenti di compliance rispetto a quelli sanzionatori, sia nei confronti dei soggetti privati che pubblici.
- **Maggiore utilizzo di ammonimenti e richieste di assunzione impegni.** Si auspica un approccio sanzionatorio "per fasi", all'interno del quale la sanzione pecuniaria rappresenta l'*extrema ratio.* Si incoraggia, al contrario, un approccio basato su ammonimenti che, a seguito dell'accertamento della violazione, impongano assunzioni

di impegni e piani di adeguamento alla norma, con rigorosi riscontri e valorizzando maggiormente il ruolo del DPO in queste fasi.

- **Promozione degli strumenti di responsabilizzazione (Certificazioni e codici di condotta).** Sotto questo profilo potrebbe essere valorizzata la promozione di strumenti di responsabilizzazione come codici di condotta e certificazioni e la valorizzazione dei relativi organismi di monitoraggio e certificazione al fine di favorire maggiormente l'*accountability* e prevenire la necessità di un sistema prevalentemente sanzionatorio.

Orientamento nella destinazione degli introiti da sanzione

- **Formazione ad imprese.** Infine, si sottolinea l'importanza di orientare la destinazione degli introiti derivanti dalle sanzioni a una promozione di piattaforme formative e di interventi per aiutare gli operatori ad aumentare il livello di sensibilizzazione e conformità alla norma.
- **Sensibilizzazione degli interessati.** I fondi derivanti dall'attività sanzionatoria troverebbero la loro naturale destinazione nell'adozione di iniziative di sensibilizzazione degli interessati, con lo scopo di favorire l'educazione digitale e consegnare a questi ultimi migliori strumenti per la gestione dei propri dati personali.

3. SOGGETTI VULNERABILI ED EFFETTIVITÀ DELLE TUTELE

Il tavolo ha discusso, prima in sottogruppi "verticali" specifici e, poi, in sessione plenaria, del rapporto critico tra alcune categorie di interessati considerati particolarmente "delicati" e le comuni attività di trattamento dei dati che avvengono nella società digitale attuale e, soprattutto, sulle piattaforme.

Dopo un'analisi dello stato dell'arte e una preliminare ricognizione normativa, nonché un'obbligata attenzione alle pronunce (e sanzioni) delle autorità Garanti in tutta Europa, i componenti dei sottogruppi hanno iniziato a elencare, e formalizzare, i principali punti di discussione, affiancando al "problema" alcune possibili "soluzioni".

A. Alcuni aspetti critici nel rapporto tra protezione dei dati e tutela dell'utente/consumatore (e alcuni suggerimenti regolatori)

Executive summary

Il primo momento di discussione ha riguardato la tutela **dell'interessato/utente/consumatore** nella società elettronica, nel commercio elettronico, sulle piattaforme e nell'utilizzo delle app.

Sono numerosi i **punti critici** individuati in questo delicato settore, attingendo anche all'esperienza di consulenti e DPO di grandi aziende, piattaforme e servizi.

Un primo punto: la mancanza di incentivi "alla compliance"

In primis, è stata segnalata, nel quadro attuale, la mancanza di **incentivi** (oltre all'art. 166 comma 7 codice privacy) che possano spingere un titolare ad avviare campagne di **responsabilizzazione** e di **sensibilizzazione** nei confronti dei consumatori sul punto della data protection.

Sarebbe, questo, un passaggio importante: consentirebbe di interpretare l'applicazione e il rispetto della normativa non come un **onere fastidioso** ma come un "**valore**" aziendale, una nuova e moderna **opportunità** di business, e un valore **reputazionale** da "giocarsi" sul mercato.

Il gruppo di lavoro ha trovato critica proprio questa mancanza diffusa di idea di **qualità** nel creare e gestire una relazione con il **soggetto interessato** fatta non solo di risposte ma, anche, di attività collaterali per mantenere sempre un rapporto **corretto** e, in alcuni casi, anche **proattivo**.

Ultimo, ma non ultimo, in questo primo punto si è riflettuto sull'opzione di rafforzare alcuni **parametri di sostenibilità** integrandoli con i principi essenziali per la protezione dei dati personali.

La proposta, in particolare, è quella di inserire tali principi nei **parametri di valutazione** di cui gli investitori devono tenere conto.

Un secondo punto: anticipare la tutela (e la compliance…)

La discussione si è poi spostata sul punto più specifico della tutela dei soggetti vulnerabili, prospettando due necessità ben distinte tra loro.

La prima è quella di **aumentare la tutela in forma anticipata**, operando sulla creazione e applicazione di **best practices**, di **codici di condotta** (un esempio che è stato fatto ha riguardato, ad esempio, i ben noti settori del telemarketing e del teleselling) e la previsione di **incentivi** sia per aziende sia per istituzioni.

La seconda è quella di garantire in ogni momento una **migliore gestione** delle modalità di **esercizio automatizzato dei diritti** e maggior chiarezza anche da parte delle autorità sugli elementi essenziali da implementare e garantire.

Un terzo punto: la definizione di standard comunicativi *ad hoc*

Ultimo suggerimento uscito dalla discussione su questo punto è legato alla possibilità di **definire degli standard comunicativi** *ad hoc* che siano pensati, ovviamente, a favore degli interessati.

In particolare, i partecipanti al gruppo hanno ravvisato esigenze manifeste di elaborazione di standard comunicativi più **trasparenti** e di facile **accessibilità**, parametrati alla piattaforma e alla sua importanza, per le informazioni rivolte ai consumatori.

Al contempo, è apparso necessario un maggiore focus su **obblighi di lealtà** e **trasparenza** nella **spiegazione** dei criteri di funzionamento di meccanismi decisionali automatizzati e analisi predittive e nelle modalità di **risposta** agli esercizi dei diritti, sulla falsariga di ciò che hanno previsto altre autorità di controllo.

L'ambiente delle **piattaforme**, chiaramente, è stato visto da tutti i partecipanti e le partecipanti al tavolo come il **più adatto** per rendere evidente una esigenza ormai improcrastinabile di rafforzare gli obblighi di **sensibilizzazione** nei confronti dei milioni di utenti.

B. Il mondo della sanità: punti critici sulla tutela dei pazienti (e alcune proposte)

Executive summary

Terminata la discussione assai costruttiva sul ruolo dell'utente delle piattaforme, è parso naturale ragionare **sull'interessato/paziente**, ossia un tipo di soggetto che si trova in un contesto di grandissima **vulnerabilità**: spesso malato o preoccupato e in un ambiente che lo suggestiona e dove si sente debole.

L'analisi preliminare ha preso le mosse da una riflessione sul **quadro legislativo**, e ha contributo a evidenziare immediatamente un problema di fondo: il quadro legislativo, nell'interpretazione degli studiosi e delle studiose di questo gruppo, si presenta ancora molto **consenso-centrico** (ossia con il consenso che è visto come una sorta di **panacea**) e un simile approccio è ancora più evidente, ed "esaltato", nell'ambito della ricerca in ambito medico.

Un primo punto di discussione: siamo sicuri che il consenso sia (ancora) la base giuridica più corretta?

Il dibattito si è acceso durante una riflessione comune sul fatto che il consenso (come base giuridica), in realtà e in molti contesti medici, non si presenti come una base giuridica così corretta e "ideale", proprio in ragione del fatto che il paziente si trova in una posizione di **debolezza psicologica** e di **vulnerabilità**.

Come si può, ad esempio, individuare la presenza di un **consenso pienamente libero** in simili situazioni traumatiche?

Un secondo punto di discussione: adottiamo una visione più moderna?

Evidenziate le criticità del consenso, il gruppo di lavoro ha riflettuto, in maniera costruttiva, su tre possibili rimedi che garantirebbero una visione più moderna di questo ambito.

Il primo è l'abbandono di questa eredità culturale consenso-centrica che impedisce di valorizzare le altre basi giuridiche o, addirittura, di disegnarne di nuove e che, comunque, dovrebbe sempre essere affiancata da un sistema di informazione (trasparenza e fruibilità)

che consenta veramente una comprensione reale in capo al paziente del suo futuro trattamento dei dati (anche utilizzando infografiche e principi del legal design).

Tale apertura ad altre basi giuridiche non deve essere in alcun modo vissuta come una diminuzione di tutela nei confronti del paziente: la tutela del paziente infatti non passa attraverso un *favor* di una base giuridica rispetto ad altre ma si concretizza tramite una maggior consapevolezza e comprensione del paziente su come vengono trattati i suoi dati, permettendogli quindi anche in corretto esercizio dei diritti. Sotto questo profilo andrebbe promosso in ambito sanitario un potenziamento delle informative, utilizzando anche strumenti innovativi e maggiormente incisivi quali (ad esempio) l'utilizzo del *legal design.*

Il secondo porta con sé una migliore elaborazione teorica dell'idea di "**consumatore-paziente**" o "**paziente-consumatore**" che dir si voglia. Non si è mai sviluppata compiutamente una logica di tutela e protezione del "consumatore paziente" nonché la predisposizione di strumenti di **tutela associativa** e consumeristica che oggi non vengono applicati al mondo della sanità ma che sarebbero perfetti per tutelare il paziente anche come un consumatore e un fruitore di servizi.

Il terzo rimedio richiede un aumento di **consapevolezza** e di **sensibilità** per i temi della protezione dei dati sia dal lato del mondo professionale, sia dal lato dei pazienti. Si pensi alla ricorrente **confusione** tra il "consenso informato" e "il consenso privacy", o alla mancanza cronica di **piani formativi** efficaci e ben strutturati per tutte le categorie coinvolte nel trattamento dei dati.

Un terzo punto di discussione: possiamo davvero parlare di privacy by design in sanità?

Tornando al tema delle competenze e della formazione, è apparso evidente al gruppo di studio e di ricerca come essenziale fosse riflettere sull'aspetto delle competenze (skills) e della reale consapevolezza del tema della data protection nell'ambito sanitario, richiamandosi anche ai principi della privacy by design e all'idea che tali concetti siano per così dire "incorporati" nel sistema stesso.

Sono stati condivisi, tra i partecipanti, due elementi critici.

Il primo evidenzia una scarsissima conoscenza/sensibilità da parte della classe medica, della dirigenza sanitaria e dei decisori sui temi della protezione dei dati.

Occorre quindi aumentare immediatamente il livello di sensibilità e di competenza manageriale sui temi della protezione dei dati anche, ad esempio, del singolo medico, che deve essere più proiettato al futuro, soprattutto con riferimento al digitale e al suo utilizzo.

Parallelamente è stata evidenziata, durante la discussione, una scarsa sensibilità/conoscenza in chi produce tecnologie nel settore sanitario.

Vi è una crescita diffusa di attenzione per il digitale ma non, purtroppo, dal punto di vista della protezione dei dati, cui si affiancano molte tecnologie native in Cina e Stati Uniti con esempi di privacy by design e by default non rispettata o, comunque, che abbracciano canoni sulla protezione dei dati concettualmente diversi (si pensi a una visione "proprietaria" del dato ancora diffusa in molti Paesi).

C. La centralità del minore nella società dell'informazione (e la sua tutela)

Executive summary

Il minore e i suoi dati sono, per molti interpreti, il futuro del commercio elettronico, dell'attività sui social e sulle piattaforme e, quindi, del trattamento dei dati.

L'età di primo accesso ai servizi online si è abbassata sensibilmente, sino a sfiorare, oggi, i 5/6 anni.

Al contempo, i dati di minori online aumentano sensibilmente sia per quantità sia per qualità, con una possibilità di profilazione che non è mai stata così precisa.

La tutela dei minori in rete rappresenta una delle sfide più attuali e delle esigenze più sentite in relazione a numerosi aspetti.

Nel presente assetto tecnologico, infatti, insieme agli innegabili benefici, hanno trovato terreno fertile anche nuove modalità di comportamenti illeciti, da cui i minori necessitano di essere salvaguardati.

Spesso, tuttavia, gli sforzi in tal senso tendono a concentrarsi esclusivamente sulle risorse tecnologiche, per la previsione di controlli più stringenti, e sugli interventi legislativi, per la repressione e la sanzione di determinate condotte.

In realtà, l'aspetto su cui si dovrebbe puntare maggiormente è quello educativo e culturale: si dovrebbero, cioè, fornire ai minori le conoscenze e gli strumenti necessari per proteggersi nel mondo virtuale tanto quanto in quello reale.

Tale educazione digitale dovrebbe riguardare non solo la persona del minore, al fine di renderlo più consapevole in merito ai rischi e ai vantaggi della rete, nonché ai diritti esercitabili in materia di trattamento dati; al contrario, dovrebbe interessare tutto quel sistema educativo integrato di stakeholder che contribuiscono alla crescita e allo sviluppo del minore stesso e nei confronti dei quali i più giovani assumono comportamenti di tipo imitativo (genitori, insegnanti, etc.).

Spesso, infatti, sono proprio gli adulti a non tenere condotte virtuose nel campo digitale, con la conseguenza di trasmettere *pattern* sbagliati a chi, da tali condotte, apprende e impara.

Dunque, l'approccio da adottare sul punto è di tipo extra-normativo: la legislazione in materia, infatti, è ampia e ben strutturata; quello che occorre è portarla a conoscenza dei soggetti a cui è rivolta ed educare questi ultimi ai propri diritti e al loro esercizio.

A tal fine, potrebbe risultare particolarmente efficace utilizzare i metodi educativi basati sulla strategia del "nudging", ossia della spinta gentile: in tal modo, i minori non percepirebbero l'adozione di determinate condotte (o cautele) come una costrizione proveniente dall'esterno, bensì come una scelta consapevole, frutto di una presa di coscienza e di un'adesione volontaria a specifici schemi di comportamento.

Norme, ambiente extra-normativo, informazioni, visione politica, incentivi e un "lifting" all'articolo 9 del GDPR sono i sei elementi critici che sono stati sollevati durante l'incontro nella discussione tra i partecipanti.

Primo punto: siamo certi dell'efficacia della normativa attuale?

La normativa a tutela dei minori, sia con riferimento alla protezione dei dati sia con riferimento, ad esempio, al cyberbullismo, si sta dimostrando efficace, oppure no? Cosa fare, in concreto, per cercare di migliorare la situazione e il quadro "digitale"? Aumentare le sanzioni? Descrivere meglio le fattispecie da vietare o punire?

Secondo punto: e se i problemi fossero meta-giuridici?

Forse il problema non è la normativa: e se la normativa fosse sufficiente o, addirittura, troppo dettagliata, ma ciò che manca è extra-normativo?

Lacune negli approcci psicologici e pedagogici possono portare a conseguenze dannose nei confronti dei minori, oltre a possibili comportamenti imitativi (il minore "imita" l'utilizzo dei dati e dei dispositivi del genitore) sino a una completa mancanza di indirizzo nei confronti dei più giovani su un uso responsabile delle tecnologie e sulla protezione dei loro dati.

Terzo punto: ma i minori sanno? Sono correttamente informati?

Nel caso ritenessimo il quadro normativo sufficiente, e ben strutturato, quanti di questi contenuti arrivano realmente ai minori e sono da loro compresi? Ad avviso del gruppo, in tantissimi casi manca una vera e propria informazione ai minori, anche su come educarli ai propri diritti e al loro esercizio. Di qui una imprescindibile esigenza di "fare cultura".

Quarto punto: e la politica? Siamo in presenza di una "vision" politica adeguata e completa?

Secondo il gruppo di lavoro, si possono evidenziare delle lacune importanti legate alla mancanza di visione politica di sistema su tutto ciò che riguardi la presenza del minore online e il trattamento dei suoi dati.

Si pensi, per fare un esempio, ai dibattiti sull'età di accesso alle piattaforme e ai vari servizi e, soprattutto, sulla sua verifica reale.

Quinto punto: la necessità, anche in questo ambito, di incentivi alla comprensione del quadro giuridico e delle norme a protezione dei dati.

Il gruppo ha valutato la necessità di "spinte gentili" che avvicinino i minori sia alla comprensione dell'architettura alla base del trattamento dei loro dati, sia alla protezione degli stessi. Incentivi premiali, positivi e non di proibizione.

Sesto punto: e se ritoccassimo l'articolo 9 del GDPR?

Durante la discussione è stata discussa anche la possibilità di un *lifting* all'articolo 9 del GDPR per renderlo più attuale ma, soprattutto, che renda evidente la vulnerabilità del minore e, quindi, la necessità di una protezione maggiore. Ciò aiuterebbe anche il soggetto stesso a percepire, nel quadro normativo, strumenti maggiori, e immediati, di protezione.

D. Tutela del lavoratore in rapporto alla data protection

Executive summary

I lavori del gruppo si sono conclusi con l'analisi del delicato rapporto tra datore di lavoro, **lavoratore** e disciplina sulla protezione dei dati personali.

Il metodo utilizzato è stato quello dell'analisi per punti di singoli aspetti per, poi, trarre delle conclusioni anche alla luce del quadro normativo e regolamentare attuale.

La discussione ha riguardato, in particolare, **otto punti**.

Primo punto: una caratteristica peculiare di questo ambito, ossia la tutela combinata

La tutela per il soggetto più debole esiste e deve esistere, in questo caso, nella combinazione tra normativa sulla protezione dei dati, disciplina dello Statuto dei Lavoratori, norme del Codice Civile, normativa sulla ergonomia del software e decreti antidiscriminazione.

Secondo punto: la traduzione del lavoro in dati

Il lavoro e l'attività lavorativa sono sempre più tradotti in dati, e ciò comporta la necessità di proteggere tutto ciò che è contenuto dentro il più complesso mondo del lavoro in sé.

Terzo punto: le nuove dimensioni di spazio e tempo

Il chi, il cosa, il dove, il quando, lo spazio e il tempo diventano i parametri più importanti per l'analisi giuridica. Si pensi alla centralità del problema della durata della prestazione nella società digitale.

Quarto punto: il (nuovo) valore dell'informazione

Il gruppo ha evidenziato un fondamentale, e centrale, **problema valoriale**. Ci si riferisce, come è chiaro, al valore dell'informazione prodotta dal lavoro che in tantissimi casi comporta ormai il valore stesso del lavoro e presenta all'interprete nuove prospettive di non facile soluzione (si pensi ai concetti di domanda e offerta nella società digitale).

Quinto punto: il delicato rapporto tra lavoratore e strumento che utilizza

Si è notato, durante i lavori, un progressivo impoverimento della professionalità del lavoratore, oltre ad aspetti molto delicati nella relazione tra lavoratore e strumento che utilizza sino a prospettare il rischio che questo valore si perda senza, al contempo, alcuna protezione per il lavoratore stesso.

Sesto punto: una nuova idea di "dignità"

Nella società digitale il concetto di dignità dovrebbe essere rivisto o ne andrebbe allargato il contenuto.

Settimo punto: porre dei limiti alla automazione?

Durante la discussione si è evidenziata una mancanza di limiti nello stabilire che cosa possa essere automatizzato e, soprattutto, che cosa introdurre per evitare il depauperamento della professionalità.

Ottavo punto: una fragilità fluida?

Si è discusso, in seno al gruppo, del concetto di una fragilità del lavoratore "fluida", simile ai fenomeni che si notano nella società digitale.

Come può aiutare il quadro attuale?

Al termine del dibattito, sempre sul tema del lavoratore nella società digitale, sono state portate alcune **ulteriori osservazioni** ed **esempi** che hanno contribuito a rendere ancora più chiaro il quadro di emergenza.

Si pensi, *inter alia*, alla necessità di adeguare l'intero quadro normativo al nuovo lavoro (ormai) basato sui **dati**, alla necessità di ripensare **all'originaria funzione** del diritto del lavoro e alla **nozione giuridica** di lavoro come strumento di mobilità sociale su cui si fonda il nostro ordinamento.

La "**datizzazione**", più volte citata nella discussione, ha infatti un'incidenza sul piano del mercato perché la produttività (nella relazione con la tecnica digitale) cambia (problema valoriale), sul piano di domanda e offerta e anche nel rapporto tra lavoratore/utilizzatore e tra lavoratore e collettività.

Il timore, come è chiaro, è che la trasformazione digitale possa comportare il **progressivo impoverimento** della professionalità del lavoratore, tanto più che, da un punto di vista normativo, manca un profilo fondamentale: stabilire che cosa possa essere **automatizzato** ("automation") e cosa introdurre per evitare il paradosso del **depauperamento** della professionalità attraverso l'esecuzione della prestazione (scelte di tecnica "augmented").

In questo quadro, sia il regolamento **sull'intelligenza artificiale** (visto come un "tetto" e non un "pavimento") sia la normativa precedente non sono visti come provvedimenti in grado di valorizzare **l'inclusione** (mentre potrebbe fare molto, ad esempio, un piano di formazione interdisciplinare come misura abilitante per garantire l'inclusività dei lavoratori e anche delle PMI).

4. MONETIZZAZIONE DEL DATO

Il tavolo si è confrontato sulle prospettive di sviluppo europee per la creazione del mercato digitale unico e sulla posizione dell'Europa nel contesto globale rispetto alla valorizzazione dei dati personali.

A. Valorizzazione dei dati e istituzioni

Executive summary

Il panel ha cercato di condividere scenari e valutazioni su di un tema che sta tentando di trovare ogni giorno un continuo equilibrio fra interessi sottesi, sia a livello europeo che nazionale.

Il primo tema riguarda la necessità di aumentare la consapevolezza sul valore del dato tra gli interessati e tra le organizzazioni, le quali spesso non sono consapevoli del valore dei dati e di come questi possano costituire un vero e proprio asset. Tale assunto va al di là della dicotomia dato personale/non personale, in quanto la mancanza di consapevolezza è trasversale a tutti gli ambiti.

Un secondo aspetto riguarda, quindi, il concetto di valorizzazione del dato che assume un significato molto più ampio e che va al di là della vera e propria monetizzazione dello stesso. La valorizzazione tende a rendere l'interessato partecipe dei processi elaborativi dei dati che gli appartengono e, nel caso dei dati personali, non lo priva della propria capacità di autodeterminazione e di controllo sul proprio patrimonio informativo.

Rendere l'interessato partecipe significa anche fargli percepire gli effetti ed i benefici, ad esempio, della condivisione del dato sulla collettività e sull'economia.

A tale proposito, si è portato, ad esempio, il processo di digitalizzazione delle reti elettriche che ha consentito l'ammodernamento della rete da parte degli operatori e al tempo stesso ha permesso agli utenti di poter immettere energia in rete, incentivando il risparmio energetico e la produzione di energia sostenibile. Gli effetti benefici sulla collettività sono stati oggetto di specifiche campagne informative da parte dei gestori dell'energia che hanno portato molti utenti ad accettare la condivisione dei propri dati producendo effetti positivi sul sistema energetico.

Un ultimo aspetto su cui il panel si è soffermato riguarda l'interrogativo e forse la necessità di ricorrere ad altre basi giuridiche, diverse dal consenso dell'interessato, al fine di adeguare al contesto specifico del trattamento (ad esempio, al contesto on line) le esigenze degli utenti e, quindi, consentire lo sviluppo del mercato digitale nell'Unione Europea, agevolando le imprese europee e consentendo loro di scalare il mercato e raggiungere le dimensioni dei player extra UE e, in particolare, di quelli statunitensi.

L'alternativa, nel caso si volesse perseguire una politica rigorista, anche alla luce delle turbolenze geopolitiche, resterebbe quella di rivendicare una sovranità digitale, come avviene in altri contesti. Si pensi alle normative in materia di cybersicurezza per le infrastrutture critiche. L'equilibrio tra le spinte del mercato e la tutela intransigente del diritto alla protezione dei dati personali, come peraltro evidenziato nella giurisprudenza della Corte di Giustizia e delle Autorità di controllo, infatti, appare precario e l'Unione sarà costretta a formalizzare una posizione valutandone gli effetti nei vari settori.

Introduzione

Il panel coordinato dall'Onorevole Giulia Pastorella ha evidenziato le contraddizioni che vive l'Europa sul tema della valorizzazione dei dati personali. Nel corso della discussione, i relatori si sono soffermati nell'esaminare le sollecitazioni che riceve il mercato europeo, tra la spinta verso una valorizzazione del dato e i timori connessi alle derive a cui il mercato può condurre, se non regolamentato in modo efficiente e corretto. I relatori hanno evidenziato i rischi di una iper-regolamentazione che, nel tentativo di proteggere la libertà di impresa e la concorrenza tra gli operatori, finisce invece per inibire i propositi di crescita e scalabilità del mercato da parte dei player europei, rischiando di condannare l'Europa a giocare una posizione marginale nel mercato digitale. Il confronto tra i relatori si è soffermato, altresì, sugli aspetti concorrenziali e di costruzione del mercato che hanno portato l'Europa alla situazione attuale, sulle possibili criticità e sui timori di evoluzioni contrarie allo spirito europeo e sollecitate dal mercato, per poi infine approdare a diverse ipotesi di equilibrio tra tutela del mercato e tutela dell'individuo, consapevoli che non vi sia una soluzione unitaria e un equilibrio definitivamente stabile, in un contesto che appare frammentato e in rapida trasformazione dal punto di vista tecnologico, di mercato, sociale e geopolitico.

La costruzione del mercato europeo

Fin dalle prime battute, è emerso come la posizione dell'Europa in materia di protezione dei dati personali e la struttura attuale del mercato digitale interno siano una conseguenza dell'evoluzione dell'Unione Europea come organismo di diritto internazionale e risentano delle varie tappe che hanno portato alla costruzione del mercato unico. Le norme europee, infatti, sono state elaborate con l'obiettivo di tutelare il mercato dell'Unione, cercando di

bilanciare, da un lato, il diritto di fare impresa delle piccole e medie imprese e, dall'altro, i poteri delle grandi società contro possibili abusi di mercato, attraverso l'imposizione di una serie di obblighi normativi in vari settori (il diritto del consumo, la sicurezza dei prodotti, la data protection, l'ambiente). Inoltre, le big tech si sono trovate a dover giustificare in sede Antitrust comportamenti sanzionati in altri settori normativi (quello attinente ai rapporti con i consumatori, ad esempio sul tema delle pratiche commerciali scorrette o della pubblicità ingannevole o quello in materia di protezione dei dati personali), in quanto in grado di produrre impatti sul mercato come conseguenza della forza dominante esercitata.[11] È stato, inoltre, più volte evidenziato come sia una particolarità tutta europea quella di avere come obiettivo la costruzione di un mercato unico e di considerare il diritto di fare impresa in posizione tuttavia secondaria rispetto ad altri diritti, e ciò sebbene nella normativa venga ribadito che i diritti devono esser bilanciati tra loro.

Il diritto alla protezione dei dati personali, per il suo aspetto trasversale, si è caratterizzato fin da subito come un elemento attraverso il quale l'Unione Europea è in grado di raggiungere e mantenere gli equilibri di mercato, e ciò ha finito per rendere la normativa sul digitale *data protection-centrica*.

Le ricadute sul mercato digitale sono state, da un lato, la protezione dell'Europa da possibili (o tentati) abusi di mercato e da distorsioni concorrenziali ma, d'altro canto, ha reso difficile alle aziende europee scalare il mercato e raggiungere le dimensioni di altri competitor. Infatti, i requisiti di compliance richiesti dalla normativa europea, per come sono stati interpretati e implementati, sono sostenibili da una grande impresa che decida di investire in Europa, mentre per le piccole e medie imprese europee costituirebbero un limite in grado di assorbire quote di capitale da destinare alla crescita del business.

Gli anni trascorsi sotto la vigenza delle vecchie direttive in materia di protezione dei dati personali sono stati caratterizzati dalla presenza di una normativa frammentata che, unitamente alle stringenti interpretazioni da parte della Corte di Giustizia, focalizzate sul rispetto dei diritti dell'individuo, e delle Autorità di controllo, focalizzate sugli interessati,

[11] Si veda la causa pendente avanti la Corte di Giustizia dell'Unione Europea Causa C-252/21 -Meta Platforms Inc., già Facebook Inc., Meta Platforms Ireland Limited, già Facebook Ireland Ltd., Facebook Deutschland GmbH contro Bundeskartellamt con l'intervento di: Verbraucherzentrale Bundesverband e.V. https://curia.europa.eu/juris/documents.jsf?num=C-252/21

hanno finito per creare una serie di costi di adeguamento che ha impedito alle aziende europee di crescere e ha lasciato il mercato del digitale a disposizione degli investimenti delle grandi aziende statunitensi proprio negli anni in cui il mercato digitale si sviluppava. L'entrata in vigore del Regolamento Europeo 2016/679 (GDPR) è stata in grado di uniformare molti ambiti della normativa e prevedere meccanismi di cooperazione nell'enforcement. Tuttavia, tale uniformità è giunta quando il mercato digitale era ben presidiato da altri player, lasciando la sensazione che il tema della valorizzazione dei dati personali e dello sviluppo del mercato europeo fosse un'occasione mancata e difficilmente recuperabile.

La riflessione si è quindi orientata verso la valorizzazione dei dati non personali, domandandosi se l'Europa riuscirà a garantire uno spazio per la loro valorizzazione e libera circolazione, in modo da sviluppare un mercato di operatori interni in grado di scalare a livello europeo ed extra-europeo o se l'orientamento sarà quello di regolamentare ciò che altri ordinamenti sono impegnati a realizzare secondo altri parametri. Il Data Governance Act (Reg. UE 2022/868) sembra voler muovere i passi in questa direzione prevedendo divieti di accordi in esclusiva sull'utilizzo dei dati pubblici e incentivare il riutilizzo, la condivisione e l'interconnessione, nonché di prevedere norme a sostegno di start-up e piccole e medie imprese.

Non solo, il Data Governance Act prevede come strada privilegiata per la condivisione e lo sfruttamento dei dati in possesso delle Pubbliche Amministrazioni, alcune soluzioni come l'anonimizzazione, la pseudonimizzazione o il trattamento in ambienti sicuri, controllati dagli stessi organismi pubblici. Se l'anonimizzazione è per definizione un procedimento sottoposto a continui controlli, in considerazione dell'evoluzione delle tecniche di riuso e che, in alcuni casi, può rendere l'informazione incorporata nel dato inutile in relazione alla finalità perseguita da chi chiede l'accesso (si pensi al settore della ricerca scientifica), altre soluzioni potrebbero consentire lo sviluppo di un mercato digitale in relazione al perimetro di applicazione della normativa.

Tuttavia, non si è mancato di evidenziare che nelle nuove proposte regolamentari europee vi siano spinte contrarie alla libera circolazione dei dati. Ne sono un esempio le proposte di modifica al Data Act che, laddove recepite in sede di pubblicazione del regolamento, consentirebbero al produttore del dispositivo *smart* di rifiutare all'utilizzatore l'accesso ai dati

e la loro condivisione con altri provider di servizi, laddove il produttore dimostri che tale divulgazione potrebbe determinare un danno economico a suo carico. Tale limitazione al diritto di accesso e di condivisione dei dati è stata inserita a seguito dei timori manifestati dagli stakeholder nell'ambito delle consultazioni con il mercato svolte dalla Commissione nell'ambito del processo legislativo ordinario, in relazione al tema della possibile circolazione di segreti industriali.

Un altro elemento che potrebbe rallentare lo sviluppo del mercato digitale all'interno dell'Unione Europea è stato ravvisato nella continua espansione delle categorie di sistemi di IA ad alto rischio all'interno dell'allegato alla proposta di regolamento sull'Intelligenza Artificiale.[12] Lo sviluppo di player europei nell'ambito di settori di avanguardia come l'Intelligenza Artificiale richiederà una serie di sforzi da parte della Commissione nel prevedere delle soluzioni percorribili per le piccole e medie imprese europee che stanno investendo nello sviluppo di questi sistemi. La combinazione degli oneri di conformità alle varie normative che, da diverse prospettive, producono effetti sul mercato dei dati, inteso in senso lato, potrebbe determinare delle ricadute sulle imprese europee in termini di sviluppo e scalabilità del mercato interno.

I timori

Il panel è consapevole che l'entusiasmo che circonda le previsioni sui possibili sviluppi del mercato unico digitale europeo, tuttavia, si accompagna ai timori su quello che Shoshana Zuboff ha definito *il capitalismo della sorveglianza*[13]. Il tema della sorveglianza di massa, infatti, richiama alla mente i drammatici eventi storici che hanno portato alla fondazione dell'Unione Europea, nata dalle ceneri della Seconda Guerra Mondiale e da quella che era una vera e propria profilazione di massa basata sull'appartenenza a una determinata confessione religiosa, a un orientamento sessuale giudicato non conforme o in conseguenza delle condizioni di salute e che ha determinato la discriminazione e la persecuzione di milioni di individui europei.

[12] Proposta di regolamento del parlamento europeo e del consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'unione - COM/2021/206 final: https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A52021PC0206

[13] Shoshana Zuboff, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'epoca dei nuovi poteri*, Luiss University press, 2019

Le conseguenze dell'Olocausto sono state disastrose su tutti i fronti, quello umanitario, in primo luogo. Di conseguenza, il timore che le nuove tecnologie siano portatrici del rischio di derive distopiche e discriminanti è ben presente nell'animo del legislatore europeo e dei giuristi del Continente, allo stesso modo in cui il passato dell'Europa ha inciso sull'anima dei trattati e delle carte costituzionali degli Stati membri, diventando di ispirazione per le costituzioni adottate successivamente anche in altre parti del mondo. L'effetto-scuola delle carte costituzionali nate dopo la Seconda Guerra Mondiale ha portato l'Unione Europea, nell'ambito della propria attività normativa, a valutare i possibili impatti che si possono produrre sui diritti e le libertà degli individui.

Il contesto geopolitico ha più volte sollecitato il Vecchio Continente a interrogarsi sui propri principi fondanti e sui pilastri su cui ha costruito la propria identità. Il terrorismo, in tutte le sue forme e matrici, ha portato spesso gli europei a interrogarsi sulla legittimità della legislazione emergenziale e fino a che punto l'emergenza sia in grado di derogare alle libertà democratiche.[14] Si sono richiamati gli esempi in cui (invocando finalità dichiaratamente emergenziali, quali il terrorismo o la tutela dell'ordine pubblico) diversi Comuni hanno valutato e adottato soluzioni di videosorveglianza dotate di sistemi di riconoscimento facciale, concretizzando così i rischi di sorveglianza di massa.[15] In tal senso, è intervenuto il Garante per la protezione dei dati personali, il quale ha ricordato alle amministrazioni coinvolte il pericolo di una schedatura di massa. Inoltre, il Parlamento europeo ha adottato una moratoria sui sistemi di videosorveglianza con riconoscimento biometrico che ha consentito di fermare alcune istanze per l'adozione di tali sistemi nelle città europee e persino a determinare l'uscita dal mercato europeo di alcuni player del settore del riconoscimento facciale, ciò a tutela di quella garanzia per i diritti fondamentali dell'essere umano che è nelle ragioni fondative dell'Unione Europea.

Allo stesso modo, un'altra emergenza, quella pandemica, ha richiesto agli attivisti dei diritti e alle istituzioni per la protezione dei dati personali di attivarsi per esigere che venissero previste delle garanzie per i diritti e le libertà degli individui nell'implementazione delle soluzioni di

[14] Si pensi agli interventi di Rodotà proprio sul tema del terrorismo e della legislazione emergenziale: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/6937167

[15] Sanzione del Garante ClearviewAI: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9751323

contact-tracing, al fine di evitare un monitoraggio dei movimenti, dei contatti e una profilazione indiscriminata di dati sanitari dei cittadini italiani ed europei.[16]

La consapevolezza della complessità del fenomeno ha richiamato esempi di *discriminazione positiva* i quali, tuttavia, non mancano di suscitare preoccupazioni per le possibili derive. Il riferimento è ai sistemi di *social credit score* annunciati dalla Fondazione per lo sviluppo sostenibile, dai Ministeri della Transizione ecologica e delle Infrastrutture, dal Comune di Bologna e da quello di Fidenza, progetti fermati dall'annuncio dell'apertura dell'istruttoria da parte dell'Autorità Garante per la protezione dei dati personali. Tali sistemi prevedevano l'assegnazione di punteggi e premi ai cittadini virtuosi con un meccanismo di credito sociale.[17] Sebbene la finalità fosse positiva, ossia legata ad incentivare il compimento di comportamenti socialmente positivi quali l'uso del trasporto pubblico o la corretta gestione della raccolta differenziata, vi erano dei potenziali risvolti discriminatori negativi, ad esempio per i cittadini che non potevano beneficiare dei vantaggi dati dallo scoring in quanto costretti a utilizzare l'automobile. Allo stesso modo, in Francia vi sono attualmente spinte verso la richiesta di pubblicazione da parte delle aziende del proprio *carbon footprint*, al fine di incentivare la diffusione di politiche di sostenibilità ambientale e raggiungere gli obiettivi di diminuzione delle emissioni fissati per il 2040[18]. Tuttavia, permane il timore che il perseguimento di tali obiettivi di sostenibilità possa poi essere esteso ai comportamenti individuali, sebbene ad oggi tale preoccupazione sembri essere esclusa.

I riferimenti alle situazioni emergenziali sono contenuti anche nei nuovi pacchetti regolamentari. Ad esempio, il Data Act prevede strumenti che consentono alle pubbliche autorità di accedere ai dati detenuti dai privati in caso di circostanze eccezionali come terremoti e inondazioni.[19] All'interno del campo di applicazione della previsione rientrano anche gli eventuali dati personali generati dai dispositivi oggetto di regolamentazione nel Data

[16] Si veda l'intervento dell'Autorità sulla proliferazione di App di contact tracing https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9447462

[17] https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9778361

[18] France clamps down on 'zero carbon' advertising to avoid greenwashing: https://www.rfi.fr/en/france/20220416-france-clamps-down-on-zero-carbon-advertising-to-avoid-greenwashing

[19] Proposta di REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo (normativa sui dati) - COM(2022) 68 final https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52022PC0068&from=EN

Act che saranno accessibili dalle pubbliche autorità in circostanze eccezionali, previa adozione di garanzie per gli interessati.

Ciò che ha colpito alcuni interpreti nelle letture della proposta del regolamento è che la definizione delle circostanze eccezionali è stata rimessa agli stati membri. Orbene, l'esperienza pandemica appena trascorsa e le tensioni geopolitiche causate dai conflitti in atto, anche alle porte dell'Unione Europea, sollevano il timore che le definizioni che verranno elaborate dagli stati membri possano fuoriuscire dagli stretti ambiti delle calamità naturali. Si pensi alle preoccupazioni sollevate da alcune politiche adottate in Polonia e Ungheria che hanno allarmato le istituzioni dell'Unione e di come esse potrebbero declinare le circostanze eccezionali legittimanti il potere di accesso delle pubbliche autorità ai dati disciplinati dal Data Act e detenuti dai privati.

B. Valorizzazione dei dati nella prospettiva del mercato

Executive summary

Tra le soluzioni individuate dai professionisti del panel è emersa una forte esigenza di cooperazione non solo tra le autorità, ma anche con le imprese e gli *over the top* per trovare un punto di incontro che tuteli gli interessati senza dimenticare le disposizioni normative e tutele anche civilistiche e consumeristiche.

Promuovere un dialogo tra le autorità italiane (Antistrust/ Garante Privacy/ AGCOM) e le Industries attraverso sand-box regolamentari o tavoli settoriali potrebbe rappresentare la chiave di svolta. La cooperazione dovrebbe avere come obiettivo finale quello di coadiuvare le aziende nell'approcciarsi in modo adeguato al tema della valorizzazione perché la semplice esistenza di "un principio di valorizzazione" non più ritenersi sufficiente. Tali riflessioni dovrebbero tener conto del contesto in cui la valorizzazione verrebbe applicata e ammettere che la base giuridica del consenso non consente di risolvere il problema. Il consenso dovrebbe essere affiancato da un'alternativa valida per essere pienamente conforme ai requisiti richiesti dagli artt. 6 e 7 del GDPR. Per alcuni professionisti, l'acquisizione di un consenso da parte di un titolare del trattamento rischia di essere interpretato, spesso, come "un via libera" per mettere in atto un'attività più invasiva. Per altri il consenso costituisce l'unica base giuridica

utilizzabile, ma deve essere strettamente connesso alla trasparenza in modo che possa rendersi chiaro ed intuitivo.

Introduzione

Il panel coordinato dalla Dott.ssa Layla Pavone ha visto la partecipazione di professionisti che da anni si occupano di temi data protection, i quali hanno analizzato il tema della valorizzazione partendo dalla propria esperienza professionale. I professionisti hanno introdotto il tema partendo dal concetto di civiltà digitale: si pensi all'uso della tecnologia per costruire un vero e proprio Digital twin (o gemello digitale), come ad esempio il progetto avviato dal Comune di Milano. Lo scopo di questo progetto di rilevazione ed elaborazione dei dati (non personali) è dotare l'Amministrazione comunale di informazioni dettagliate sul tessuto del territorio cittadino per affrontare le "moderne" sfide di gestione dello spazio pubblico. Il Gemello digitale costituisce il primo passo per far diventare Milano a tutti gli effetti una smart city grazie ad una corretta panoramica dell'esistente arricchita da dati e approfondimenti che possono essere utilizzati per migliorare la gestione della municipalità a beneficio di tutti i cittadini in ottica di sostenibilità economica e sociale. La coordinatrice del Board per l'Innovazione tecnologica e Trasformazione digitale del Comune di Milano, Layla Pavone, afferma infatti che l'innovazione digitale e la tecnologia avanzata possano migliore la governance delle città.

Si tratta di un progresso tecnologico con enormi potenzialità sui servizi offerti alle cittadine e ai cittadini, in termini di sostenibilità, efficientamento e sicurezza. La discussione ha tenuto conto dell'importanza degli *open data* e del ruolo che potrebbero assumere a livello istituzionale, oltre che ai progressi che si potrebbero raggiungere in ambito urbanistico, ambientale e di mobilità, attraverso un utilizzo efficiente e sicuro di questi dati. La valorizzazione rappresenta una sfida che non riguarda però solamente le istituzioni ma necessita della collaborazione di tutti players, ivi inclusi i cittadini. La valorizzazione dei dati assume un ruolo cardine anche per promuovere nuove occasioni di business in ambito aziendale senza trascurare l'importanza dell'etica, necessaria per porre dei limiti ed evitare disparità di trattamento sociale, nonché ottimizzare i benefici della tecnologia per la società e l'economia, in modalità tali da rafforzare i diritti e le libertà dei singoli.

La valorizzazione e le opportunità di business

La valorizzazione dei dati è, da tempo, un tema annoso per le imprese: da un lato consentirebbe agli utenti di usufruire di servizi a cui da soli non sarebbero in grado di accedere, dall'altro scoraggia le piccole-medie imprese che non possiedono sufficienti risorse per investire nel digitale e, in assenza di tali dati, sono incapaci di espandere il proprio business. Le PMI non riescono spesso in questo intento in quanto vi è una carenza di formazione anche nell'utilizzo dei software e degli strumenti a disposizione. In questo scenario la cultura, l'approccio strategico e le competenze digitali giocano un ruolo centrale nell'efficacia di tale trasformazione digitale. Molte aziende hanno come obiettivo quello di promuovere soluzioni digitali che consentano ai clienti B2B di trattare i dati personali in modo digitale puntando sulla trasparenza per non perdere competitività nel mercato e consentendo all'utente di fare scelte consapevoli. In questi ultimi anni, molte aziende hanno investito molto sul principio di trasparenza anche mediante la creazione di informative maggiormente comprensibili per l'utente, anche in un'ottica di *legal design*.

Un aspetto su cui i professionisti hanno voluto soffermarsi è la condizione di liceità per la valorizzazione dei dati personali, aspetto su cui non esiste, ad oggi, una visione univoca. La possibilità di avvalersi di altre basi giuridiche oltre al consenso come, ad esempio, il contratto o il legittimo interesse non sono nella maggior parte dei casi soluzioni percorribili. Tuttavia, secondo l'analisi dei professionisti al tavolo, si potrebbe pensare all'ideazione di strategie che consentano all'utente di effettuare delle scelte consapevoli, ad esempio valutare se usufruire di un abbonamento che abbia un costo inferiore rispetto all'abbonamento premium privo di pubblicità profilata (compenso che tenga conto della perdita economica).

Quando si parla di bilanciamento tra data protection e libertà economiche, la partita diventa molto più ampia se si tiene conto dell'Industry. Esiste, altresì, un tema di pluralismo dell'informazione: una testata che non riesce a "monetizzare" il dato non sopravvive ed è maggiormente influenzabile.[20]

Secondo i professionisti, la *over protection* limita, da un lato, le aziende in quanto annienta il business e, dall'altro, la libertà dell'utente. Sarebbe necessario, secondo i partecipanti al

[20] *Cookie wall: all'esame del Garante privacy le iniziative degli editori [doc. web. 815415].*

tavolo di lavoro, promuovere, dal punto di vista scientifico, modelli di business basati sulla valorizzazione dei dati che consentano di verificare, in concreto, i rischi per l'interessato al fine di adottare adeguate misure di sicurezza tecniche ed organizzative che garantiscano un livello di sicurezza adeguato al rischio. Con riferimento alle misure di sicurezza si è parlato anche di tecniche di anonimizzazione. Tuttavia, è ben noto che l'anonimizzazione costituisce un trattamento successivo dei dati personali e, pertanto, come ogni trattamento necessita di essere regolamentato, oltre che dal punto di vista tecnico in conformità con i requisiti richiesti[21], nel rispetto delle disposizioni per la data protection (ad esempio, il titolare del trattamento dovrà individuare una corretta base giuridica nonché darne evidenza agli interessati in linea con il principio di trasparenza).

Sarebbe necessaria, ad avviso dei professionisti, una maggiore consapevolezza da parte delle istituzioni e di tutti gli stakeholder sulla responsabilità storica circa la creazione di un modello di sviluppo digitale da proporre consentendo la sopravvivenza strategica di settori che costituiscono anche presidi di libertà costituzionali (es. testate giornalistiche). Infatti, come anticipato, nel caso delle testate, oltre al bilanciamento tra i diritti data protection e le libertà economiche vi è anche un tema più ampio legato all'Industry.

La valorizzazione e il GDPR

Le riflessioni connesse alla possibilità effettiva di valorizzare i dati hanno condotto i professionisti ad una breve discussione in merito all'esaustività e alla complessità del GDPR. Secondo alcuni professionisti, il GDPR non è del tutto sufficiente, ma fornisce delle basi solide per trovare delle soluzioni nel rispetto dei principi fondamentali anche in termini di sicurezza. Secondo altri, sarebbe necessario un momento evolutivo dal punto di vista intellettuale che consenta di trovare soluzioni utili per rispondere alle esigenze del mercato. La strategia dell'innovazione della trasparenza è sicuramente un *pillar* che deve accompagnare verso la digitalizzazione, rendendo gli utenti consapevoli sull'uso dei loro dati e scongiurando così il timore di un utilizzo non *compliant* dei loro dati personali. In questo scenario si deve tenere conto, altresì, del fatto che il quadro normativo necessiti di essere esteso, anche grazie al Regolamento e-privacy che disciplinerà tali aspetti.

[21] Working Party articles 29 "Parere 05/2014 sulle tecniche di anonimizzazione".

Secondo i professionisti, la valorizzazione dei dati personali è un concetto vissuto in modo differente da alcuni Stati europei rispetto al nostro ordinamento nazionale. Infatti, molti players europei effettuano da sempre la valorizzazione dei dati personali, considerando l'utente consapevole delle scelte prese. Secondo i professionisti, l'errore potrebbe essere quello di considerare, in Italia, l'utente incapace di comprendere e quindi suscettibile di tutela a priori.

In Italia, le prime linee guida sui cookie del 2014 hanno creato un livello di tutela elevato[22], mentre l'Europa ne ha creati diversi.

Inoltre, il GDPR non è interpretato in modo univoco da tutte le Data Protection Authorities: alcune autorità adottano un orientamento più restrittivo; pertanto, la visione della valorizzazione/monetizzazione è differente già all'interno dell'Europa stessa. L'esigenza rappresentata dai professionisti al tavolo è quella di giungere, quindi, ad un approccio univoco a livello europeo sulla valorizzazione del dato per evitare il c.d. *forum shopping* e svantaggi competitivi. La disomogeneità interpretativa è visibile già con il caso Meta. Il Garante irlandese ha dovuto adeguarsi alle conclusioni del Comitato dei Garanti europei (EDPB) che pure non condivideva, ingiungendo a Meta a pagare 390 milioni di euro per aver violato le regole europee sulla privacy.

In relazione a tale provvedimento, l'European Data Protection Board non ha ritenuto applicabile la base giuridica contrattuale. Infatti "*secondo il Comitato dei Garanti, non sarebbe idonea allo scopo per ragioni diverse che vanno dalla scarsa trasparenza con la quale Meta ha rappresentato detta circostanza agli interessati, alla dubbia validità di un contratto perfezionato almeno in presenza di una significativa asimmetria informativa tra le parti, al fatto che la più parte degli utenti di Facebook e Instagram non si sono mai neppure resi conto di aver concluso un contratto con Meta ma, soprattutto, al fatto che il trattamento in questione non appare effettivamente necessario a dare esecuzione al contratto che lega Meta ai suoi utenti, potendo detto contratto trovare esecuzione a prescindere dalla profilazione*

[22] *Individuazione delle modalità semplificate per l´informativa e l´acquisizione del consenso per l´uso dei cookie - 8 maggio 2014*

destinata alla trasmissione di pubblicità targettizzata e non avendo mai, in effetti, Meta assunto alcun obbligo specifico di fornire agli utenti tale pubblicità"[23].

C. Valorizzazione dei dati nella prospettiva dei giuristi

Executive summary

Il panel ha concluso il confronto con la condivisione di alcuni punti e proposte operative, partendo dal presupposto di mantenere una distinzione tra valorizzazione e monetizzazione e considerando come punto fermo l'esclusione della monetizzazione del diritto. Più nello specifico, sono state avanzate delle proposte per risolvere, o almeno attenuare, il problema dell'asimmetria informativa tra i soggetti coinvolti. In tal senso, è stato suggerito di assorbire l'informativa sul trattamento dei dati personali all'interno del contratto, mettendo in risalto le informazioni, al fine di far soffermare l'interessato/consumatore/utente sugli aspetti relativi al trattamento dei propri dati personali. Un'altra soluzione prospettata è stata quella di favorire l'utilizzo di informative iper-semplificate. Rispetto al secondo argomento affrontato, ossia l'individuazione delle norme su cui fondare la circolazione dei dati in ottica di valorizzazione, si è convenuto che il GDPR metta già a disposizioni delle basi giuridiche che possano essere considerate anche in ottica di valorizzazione del dato. È stato proposto, dunque, un modello che prenda come punto di partenza le basi giuridiche del GDPR in relazione ad una serie di modelli di business verticali. Infine, la riflessione è tornata sulla necessità di un bilanciamento tra diritto alla protezione dei dati personali e gli altri diritti.

Introduzione

Il Panel coordinato dall'Avvocato Panetta ha visto la partecipazione di importanti professionisti che si sono confrontati sulle questioni della valorizzazione e monetizzazione del dato al fine di individuare delle possibili soluzioni e fornire delle risposte giuridiche a quella che sembra già essere diventata una prassi. Più nello specifico, la discussione del panel ha riguardato tre aree principali: a) l'asimmetria informativa tra le parti nella costruzione del

[23] Pubblicità online, Scorza: "Ecco i tre scenari dopo la maxi multa a Meta" - Intervento di Guido Scorza https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9844860

rapporto contrattuale sotteso alla fornitura di servizi digitali e i possibili strumenti per ridurre tale asimmetria; b) la valorizzazione economica del dato personale e le basi giuridiche su cui può reggersi; c) il limite dell'autonomia negoziale delle parti nella costruzione di un rapporto fondato sulla fornitura di servizi in cambio di dati personali.

Il confronto ha preso il via dalla considerazione del ruolo del giurista, il quale deve tenere in considerazione anche l'evoluzione della società. È emersa sin da subito la necessità di creare consapevolezza nell'interessato/utente/consumatore ed è stata messa in luce la coesione ed esistenza di tre valori: economico, sociale e personalistico, i quali dovrebbero essere considerati per indirizzare il quadro normativo.

Trasparenza e asimmetria informativa

La prima importante questione discussa è stata quella relativa all'asimmetria informativa tra le parti nella costruzione del rapporto contrattuale sotteso alla fornitura di servizi digitali. Infatti, se da un lato ci sono i fornitori dei servizi digitali che dispongono di una visione complessiva del trattamento che viene effettuato sui dati personali, dall'altro ci sono gli interessati, utenti o consumatori che, spesso, non sono posti nella condizione di poter comprendere appieno che impiego verrà fatto dei propri dati personali. Il tema della trasparenza deve essere correttamente inquadrato e devono essere svolte delle valutazioni sulle modalità per veicolare le informazioni. Ci si è interrogati sul ruolo svolto dalle informative sul trattamento dei dati personali ed è stata evidenziata dai più l'inadeguatezza delle stesse a ridurre in modo efficace l'asimmetria informativa. Infatti, già in alcune sentenze è stata messa in luce la necessità di fornire ulteriori informazioni, oltre a quelle contenute nell'informativa sul trattamento dei dati personali, anche se non è stato specificato quali informazioni.[24] In

[24] Cfr. anche sentenza "Telepass" (Tar Lazio, sentenza n. 603/2023). In quest'ultima il TAR Lazio ha evidenziato che «*E' stato invero contestato che, nell'ambito dell'attività di collocamento di servizi assicurativi per conto delle compagnie partner, gli stessi ricevevano, senza che i consumatori ne fossero adeguatamente informati, flussi di informazioni riguardanti i dati dell'utente che richiedeva il preventivo. A tale condotta seguiva un processo di condivisione di tali informazioni fra le società del gruppo Telepass e le compagnie ovvero gli intermediari di assicurazione, senza che i potenziali aderenti ai preventivi delle polizze potessero essere adeguatamente informati sulla raccolta e sul modo con cui i loro dati venivano utilizzati a fini commerciali dalle società interessate. Inoltre è stato accertato che Telepass, Telepass Broker e le compagnie di assicurazioni partner condividevano un data base dedicato per la gestione e per l'acquisizione dei dati assicurativi, diverso rispetto alla piattaforma attraverso la quale parte ricorrente gestisce i dati degli utenti e titolari degli appositi dispositivi per i servizi di*

alcuni settori, ad esempio quello bancario, la problematica è stata affrontata e sono state inserite normative sull'informazione volte a riequilibrare la posizione di svantaggio. Per raggiungere l'obiettivo di un riequilibrio, la trasparenza nelle informazioni ha un ruolo fondamentale.[25]

È altresì importante il ruolo svolto dalle diverse Autorità (Garante per la protezione dei dati personali e AGCM), poiché i temi attinenti alla trasparenza sono trasversali e possono coinvolgere la protezione dati, la tutela del consumatore e l'antitrust e possono ricadere nell'ambito di intersezione di più autorità (ad esempio, l'uso abusivo di grandi banche dati rischia di generare un abuso di posizione dominante).[26] Un altro aspetto emerso nella discussione è che l'asimmetria informativa si riscontra anche nella collocazione delle informazioni. Dal confronto è sorta l'idea che una possibile soluzione sia quella di inserire l'informativa già nel contratto, avvertendo sui possibili rischi (ad esempio, per la profilazione) ed evidenziando in grassetto determinate informazioni per affievolire l'asimmetria. Si precisa che non si tratta di porre dei divieti, ma di sottoporre alcuni elementi ad una maggiore attenzione, come avviene già per le clausole vessatorie. Un'altra possibile soluzione per facilitare l'interessato/utente/consumatore nella comprensione delle informazioni ricevute potrebbe essere quella di fornire delle informative iper-semplificate.

---

pagamento autostradale. Data base del tutto separato e autonomo, in cui venivano condivise e conservate tutte le informazioni dei clienti che avevano stipulato una polizza assicurativa o avevano salvato un preventivo, ancora una volta senza che vi fosse stata alcuna informativa al consumatore dell'utilizzo dei propri dati a fini commerciali.» «*Il consumatore, se era rassicurato dalle informazioni attinenti allo specifico ambito inerente alla riservatezza dei dati personali, era, dall'altra parte e per converso, del tutto all'oscuro delle modalità di gestione e di conservazione, nonché di utilizzo, dei suoi dati, ai predetti fini commerciali. Dai claim sul sito ovvero nella procedura attivata con la APP non emergeva in alcun modo l'ulteriore uso dei dati, che sarebbero confluiti in banche dati condivise con i partner, per il perseguimento delle finalità commerciali attinenti ai servizi assicurativi*»

[25] Sul punto si noti anche l'attenzione posta dal legislatore europeo al tema della trasparenza intesa in senso ampio, ad esempio nell'art. 24 del Digital Services Act "Trasparenza della pubblicità online", il quale dispone che «*Le piattaforme online che visualizzano pubblicità sulle loro interfacce online provvedono affinché i destinatari del servizio siano in grado di identificare in modo chiaro e non ambiguo e in tempo reale, per ogni singolo messaggio pubblicitario mostrato a ogni singolo destinatario: a) la natura pubblicitaria delle informazioni visualizzate; b) la persona fisica o giuridica per conto della quale viene visualizzata la pubblicità; c)* ***informazioni rilevanti sui principali parametri utilizzati per determinare il destinatario al quale viene mostrata la pubblicità***»

[26] Negli USA, ad esempio, è la Federal Trade Commission (FTC) ad occuparsi anche della protezione dei dati.

Valorizzazione economica del dato personale e le basi giuridiche

Il secondo tema oggetto del confronto del panel è stato quello relativo alla presenza o meno, nel diritto positivo, di infrastrutture idonee a guidare il cambiamento. È emerso che il GDPR offra già delle basi giuridiche che possono essere prese come punto di riferimento ed in passato ci sono già stati dei provvedimenti del Garante con degli aspetti riconducibili alla valorizzazione del dato. In particolare, nel provvedimento sulle carte fedeltà, il Garante ha stabilito che i dati personali dell'interessato possono essere utilizzati per tre finalità: 1) raccolta punti per poi avere dei premi, ossia "fidelizzazione" in senso stretto (quest'aspetto potrebbe rientrare nel concetto di valorizzazione) utilizzando quale base giuridica il contratto; 2) marketing diretto e 3) profilazione.[27] Rispetto a queste ultime due finalità, la base giuridica è stata individuata nel consenso. Da qui è scaturita un'altra riflessione sui limiti dell'utilizzo delle rispettive basi giuridiche. È stato messo in evidenza, pertanto, che la valorizzazione del dato è il frutto anche di scelte del titolare del trattamento e che resta (e deve restare) un nocciolo duro nella protezione del dato personale che deve fare riferimento alla base giuridica del consenso (sullo schema, ad esempio, del provvedimento sulle carte fedeltà che individua l'utilizzo delle diverse basi giuridiche del contratto e del consenso in relazione alle finalità di trattamento). In ogni caso, è stato considerato inammissibile il ricorso a pratiche aggressive o a pratiche scorrette.

Riportato dunque il tema nella fisiologia, considerato anche che è un problema in evoluzione, è stato messo in evidenza che la valorizzazione economica del dato personale dal punto di vista delle basi giuridiche può seguire più strade: 1) il consenso; 2) il consenso un po' "incoraggiato", al fine di consentire l'utilizzo dei dati come alternativa al pagamento (esempio "paywall" su cui è in corso un'istruttoria da parte del Garante rispetto ad alcune testate giornalistiche online);[28] 3) il legittimo interesse, che non prevede una manifestazione di volontà preventiva. L'utilizzo di questa base giuridica può essere il varco per il bilanciamento tra il diritto alla protezione dei dati personali e altri interessi e può essere visto come base di

[27] 'Fidelity card' e garanzie per i consumatori. Le regole del Garante per i programmi di fidelizzazione - 24 febbraio 2005
[1103045]
[28] Cfr. Comunicati stampa del Garante per la Protezione dei Dati Personali del 18 ottobre 2022, 21 ottobre 2022 e 12 novembre 2022.

sostenibilità e di "riciclo" del dato. È emerso però che devono essere poste delle condizioni per il suo utilizzo; 4) la contrattualizzazione. Si va oltre l'utilizzo del dato per la stretta necessità del servizio e possono esserci due ipotesi che prevedono: a) un'obbligazione dalla parte del titolare del trattamento, il quale si obbliga a fare qualcosa con i dati (ad esempio, il personal shopper a cui si chiede di conoscere le preferenze del cliente); b) la possibilità per l'interessato di mettere a disposizione la licenza per l'utilizzo dei suoi dati personali. Quest'ultima soluzione è quella che si avvicina alla monetizzazione in senso stretto ed è anche la più rischiosa.

Tutti gli schemi sopra indicati mettono in pericolo il diritto alla protezione dei dati personali. Non si suggerisce, quindi, una disponibilità assoluta, ma una sorta di "fisarmonica di indisponibilità relative", le quali vanno bilanciate. Si dovrebbero poi prevedere restrizioni più pesanti o leggere a seconda dei casi. La sensazione è che nella valorizzazione siano presenti una serie di modelli verticali di business (in relazione alla base giuridica prescelta) che devono essere guardati separatamente, identificando rischi e opportunità per identificare per ciascun modello il rischio accettabile. Inoltre, non dovremmo liberarci di un approccio caso per caso, oltre a quello modello per modello. Dal confronto, è emerso che il modello che fa riferimento alla valorizzazione del dato personale attraverso l'utilizzo di diverse basi giuridiche, sopra descritto, potrebbe essere complesso e idoneo ad essere applicato ai grandi player, ma non ai piccoli. Una soluzione proposta per rendere il modello un punto di riferimento per tutti i soggetti è quella di introdurre degli schemi standard (sull'esempio delle SCC) in cui, per determinati scenari di basi giuridiche relative a modelli verticali (tra quelli elencati sopra), vengono date delle indicazioni per i player più "piccoli".

La standardizzazione dovrebbe presentare degli scenari minimi immutabili, rimanendo però aperta a varianti che si scostino dallo standard, nel rispetto del principio di accountability. Tale soluzione aperta a varianti, però, potrebbe non raggiungere l'efficacia delle SCC il cui punto di forza risiede proprio nell'immodificabilità. Un altro aspetto critico è stato rinvenuto nell'utilizzo del legittimo interesse e nell'individuazione del limite entro il quale il

bilanciamento può essere considerato adeguato.[29] In ogni caso, la soluzione proposta è concreta e parte da strumenti già presenti nel nostro ordinamento.

Il limite dell'autonomia negoziale delle parti nella costruzione di un rapporto tra la fornitura di servizi in cambio di dati personali

Anche rispetto a quest'ultimo tema occorre partire dagli strumenti che l'ordinamento mette già a disposizione, i quali in parte funzionano e in parte no. Si ritiene opportuno mantenere le due fattispecie: monetizzazione (l'interessato dà i dati verso il pagamento) e valorizzazione del dato (che avviene già). Valorizzazione e monetizzazione, pertanto, vanno tenute distinte. Inoltre, un punto fermo che ha visto tutti i partecipanti del panel d'accordo è stato l'esclusione della monetizzazione del diritto. Dal confronto è emerso un possibile parallelo con l'art. 97 della legge sul diritto d'autore con riferimento allo sfruttamento del diritto all'immagine. Infatti, il diritto resta in capo al soggetto mentre l'immagine viene utilizzata. Rispetto ai limiti relativi alla riutilizzazione del dato personale, è stato discusso che la stessa non può essere impedita quando va a tutelare interessi superiori (es. pubblici o collettivi).

Sul punto, i partecipanti al panel si sono trovati d'accordo nell'affermare che ci dovrebbero essere norme di diritto positivo che pongano dei limiti. È stato ribadito inoltre che il diritto alla protezione dei dati è un diritto fondamentale, come sancito dall'art. 8 della Carta dei diritti fondamentali dell'Unione Europea e la chiave per la valorizzazione dei dati è il bilanciamento. Il dato ha un valore economico ed è innegabile; tuttavia, ad oggi non esiste una norma di diritto positivo che ponga il dato come sinallagma[30]. Occorre, pertanto, prestare attenzione sia a dare al singolo il controllo dei propri dati personali, sia a bloccare la circolazione degli stessi; dunque, è necessario trovare un bilanciamento tra le due esigenze poiché il rischio di porre delle "barricate" altissime ha come contraltare che le stesse non vengano rispettate.

[29] Si ricordi il caso VoetbalTV in cui il Garante olandese ha detto che lo scopo di lucro non può essere considerato un legittimo interesse, posizione questa criticata dalla Commissione europea.

[30] Nel dibattito è stato preso in considerazione anche l'art. 135-octies, co. 4, del Codice del consumo «*Le disposizioni del presente capo si applicano altresì nel caso in cui il professionista fornisce o si obbliga a fornire un contenuto digitale o un servizio digitale al consumatore e il consumatore fornisce o si obbliga a fornire dati personali al professionista, fatto salvo il caso in cui i dati personali forniti dal consumatore siano trattati esclusivamente dal professionista ai fini della fornitura del contenuto digitale o del servizio digitale a norma del presente capo o per consentire l'assolvimento degli obblighi di legge cui e' soggetto il professionista e quest'ultimo non tratti tali dati per scopi diversi da quelli previsti.*»

PARTECIPANTI AI TAVOLI

Tavolo 1 – Strategia digitale dell'UE

TAVOLO 1	Strategia Digitale dell'UE
Coordinatore: Perri - Conduttori: Bruschi, Diomede, Orofino	
Claudio Ardagna	Professore di Informatica UNIMI – Direttore Laboratorio CINI Big Data
Simone Bonavita	Head of IT Law - Perani Pozzi Associati - EXC Director at ISLC - UNIMI
Danilo Bruschi	Professore di Informatica UNIMI - Direttore Laboratorio di Sicurezza e Reti
Diego Dimalta	Co-fondatore Privacy Network
Nicla Ivana Diomede	Direttore del Dipartimento di Cybersecurity e Sicurezza di Roma Capitale
Giulia Escurolle	Avvocato – DPO - Dottore di Ricerca – Research Fellow ISLC
Simona Klimbacher	Avvocato - General Counsel BSVA - Studio Legale Associato - Research Fellow ISLC
Paulina Kowalicka	Assegnista di ricerca in Informatica Giuridica UNIMI - Research Fellow ISLC
Gianluigi Marino	Partner, Head of Digitalisation Osborne Clarke Italia
Francesco P. Micozzi	Professore di Informatica Giuridica UNIPG - Leader Modulo Jean Monnet CIBER (2020-2023)
Juri Monducci	Partner Fondatore MPSLAW Monducci Spedicato e Associati - DPO
Mattia Monga	Professore di Informatica UNIMI
Marco Orofino	Professore di Diritto Costituzionale – Dip. Studi Internazionali, Giuridici, Storici e Politici UNIMI
Pierangela Samarati	Professoressa di Informatica UNIMI - Direttore Laboratorio Sicurezza e Protezione Dati
Onofrio Signorile	Capo Ufficio Tecnologie e Innovazione - Direzione Regionale Piemonte Agenzia delle Entrate

TAVOLO 1	Strategia Digitale dell'UE
Federico Marengo	Senior Consultant White Label Consultancy
Stefano Petrussi	Partner Floreani Studio Legale Associato
Tommaso Stranieri	Partner Risk Advisory Corporate, Public & Private Market Leader Deloitte
Stefano Zanero	Professore di Cybersecurity POLIMI - President & Founder Secure Network
Alessandro Trivilini	Head of SUPSI Digital Forensics Lab

Tavolo 2 – Ruolo e poteri delle Autorità di controllo

TAVOLO 2	Ruolo e poteri delle Autorità di controllo
Coordinatore: Imperiali - Conduttori: Faggioli, Fulco, Rigoni, Vintiadis	
Antonio Bianchi	Docente universitario diritto delle imprese – Università Suor Orsola Benincasa
Cristina Cabella	Head Data Protection Compliance & Group DPO UniCredit
Carlo Rossi Chauvenet	Managing Partner CRCLEX - Professore Aggiunto di Privacy & Protezione Dati UniBocconi
Nicola Fabiano	Founder Studio Legale Fabiano - Prof. a c. UniOstrava - Già Presidente Garante privacy San Marino
Gabriele Faggioli	CEO P4I & Co-CEO Gruppo Digital360 - Presidente CLUSIT - Professore a contratto UniPavia
Umberto Fantigrossi	Avvocato Studio Legale Fantigrossi
Carolina Foglia	Head of Activity for Legal Coordination EDPB Secretariat
Carmelo Fontana	Senior Regional Counsel Google - Docente & MCE Digital Economy, Legal e Tax SDA Bocconi
Diego Fulco	Partner netforLegal - Professore a contratto IULM
Giovanni B. Gallus	Partner Array Law - Membro Commissione Surveillance CCBE - Fellow Nexa Center for Internet & Society
Corrado Giustozzi	Partner Fondatore Rexilience - Professore Aggiunto in Security presso LUISS
Giovanni Guerra	Founder Studio Legale Avvocati Guerra Ricchiuto
Laura Liguori	Partner Portolano Cavallo
Cristiana Luciani	Funzionario Autorità Garante per la Protezione dei Dati Personali
Andrea Monti	Founder Studio Legale Monti - Professore a contratto Università degli Studi di Chieti
Enrico Pelino	Partner Grieco Pelino Avvocati
Andrea Rigoni	Government and Public Services Global Cyber Leader Deloitte

TAVOLO 2	Ruolo e poteri delle Autorità di controllo
Fabrizio Vigo	Co-Founder e CEO presso SevenData
Marianna Vintiadis	CEO di 36Brains

Tavolo 3 – Soggetti vulnerabili ed effettività delle tutele

TAVOLO 3	Soggetti vulnerabili ed effettività delle tutele
Coordinatore: Ziccardi - Conduttori: Egitto, Sala, Stefanelli	
Sergio Aracu	Partner Fondatore Area Legale
Marcello Bergonzi Perrone	Avvocato Studio Legale Bergonzi Perrone
Rossella Cerchia	Professore di Diritto Privato Comparato UNIMI - Of Counsel DLA Piper
Chiara Ciccia Romito	Avvocato e PhD Candidate LSI, Fondazione Marco Biagi
Luca Egitto	Partner IP & Technology RP Legal&Tax Studio Associato - Research Fellow ISLC
Riccardo Giannetti	Presidente Inveo Group - Docente di corsi Auditor EPE e Maestro Privacy - DPO
Silvia Gorlani	DPO Mediamarket
Matteo Giacomo Jori	Avvocato - Professore a contratto di Legge IT e Informatica Giuridica UNIMI
Licia Liguori	Senior Legal Counsel UK&I and Data Privacy Specialist Avanade
Francesca Marinelli	Professoressa Diritto del Lavoro UNIMI
Giulio Messori	Managing Director - Sweet Legal Tech
Andrea Michinelli	Avvocato Studio Legale d'Ammassa & Partners - Of Counsel 42 Law Firm
Massimiliano Nicotra	Senior Partner QUBIT Law Firm - Digital Lawyer - Co-Founder Legal Hacker Roma
Giulia Pesci	Assegnista di ricerca in Informatica Giuridica UNIMI - Research Fellow ISLC
Fabio Rastrelli	Avvocato - Intesa San Paolo
Gianluigi Maria Riva	Avvocato, Data Protection Specialist - PhD in Privacy, Etica e Nuove Tecnologie UC Dublin
Marianna Sala	Avvocato fondatore Studio Legale Sala - Presidente Corecom Lombardia
Alessandra Salluce	Avvocato specializzato in protezione dei dati personali - DPO - Research Fellow ISLC

TAVOLO 3	Soggetti vulnerabili ed effettività delle tutele
Andrea Stanchi	Managing Partner Stanchi Studio Legale - Avvocato di diritto del lavoro
Samanta Stanco	Avvocato, Assegnista di ricerca in Informatica Giuridica UNIMI - Research Fellow ISLC
Silvia Stefanelli	Senior Partner Studio Legale Stefanelli&Stefanelli - Docente

Tavolo 4 – Monetizzazione del dato

TAVOLO 4	Monetizzazione del dato
Coordinatore: Cataleta - Conduttori: Panetta, Pastorella, Pavone	
Ernesto Belisario	Senior Partner E-Lex Studio Legale
Rebecca B. Aspetti	Research Officer European Centre on Privacy & Cybersecurity Maastricht University
Luca Bolognini	Partner Fondatore ICTLC - Presidente Istituto Italiano Privacy e Valorizzazione dei Dati
Vincenzo Colarocco	Capo Dipartimento Compliance, Media e Tecnologia, e Capo Dipartimento Diritto della Proprietà Intellettuale, Diritto di Internet e concorrenza sleale - Studio Previti
Fernanda Faini	Research Fellow e Professoressa a.c. UniPisa e UniCatt – Funzionario legislativo-legale Regione Toscana
Ada Fiaschi	General Counsel & Compliance ITA Airways
Camilla Giannecchini	Senior Legal Counsel TikTok
Arianna Greco	Senior Vice President Head Global Commercial Legal Alnylam Pharmaceuticals
Anna Paola Lenzi	Group DPO & Head Compliance TeamSystem
Melissa Marchese	Counsel Gianni & Origoni
Gianluca Marmorato	Avvocato Studio Legale Boglione
Massimiliano Masnada	Partner Hogan Lovells
Luigi Neirotti	Avvocato e DPO, Senior Legal Counsel, IT Law & Data Protection Law Leader, EYLaw
Giangiacomo Olivi	Partner presso Dentons – Europe Co-Head IP, Data and Technology
Valentina Pagnanelli	Avvocato, Privacy Officer e Consulente Privacy - Docente Diritto informatico - PhD candidate - Università di Firenze
Rocco Panetta	Founder & Managing Partner Panetta Studio Legale - Country Leader Italia IAPP - DPO
Giulia Pastorella	Deputata della Repubblica Italiana - PhD London School of Economics

TAVOLO 4	Monetizzazione del dato
Layla Pavone	Coordinatrice Board Innovazione Tecnologica e Trasformazione Digitale Comune di Milano Presidente Onorario IAB Italia e ConDirettrice e Professoressa del Master Digital Communication Almed-UniCatt
Chiara Petruzzo	Data Protection Officer ARERA - Member of Board of appeal on the EU Agency for the Cooperation of Energy Regulators (Acer)
Lucio Scudiero	Avvocato Legance - Direttore Generale Lex Digital

ALLEGATO 1 – Sondaggio ed esiti

Ritieni che il legislatore europeo stia sviluppando un quadro coerente di governo dei dati?

		Answers	Ratio
Si, perché la regolamentazione di diversi settori sta crescendo in maniera uniforme.		24	42.11%
No, perché la produzione è tale da renderla ormai impossibile da seguire nelle sue evoluzioni.		28	49.12%
Non saprei.		5	8.77%
Non risponde		0	0%

Dal tuo punto di vista, è corretto fissare sempre più obblighi in capo alle piattaforme?

		Answers	Ratio
Si, perché su di esse risiede il potere di intervenire.		39	68.42%
No, perché si rischia di frenare l'innovazione.		14	24.56%
Non saprei.		4	7.02%
Non risponde		0	0%

Come giudichi l'approccio c.d. human in the loop tipico della strategia digitale dell'UE?

		Answers	Ratio
Corretto, perché mette in primo piano i diritti degli individui.		42	73.68%
Non corretto, perché già altre norme potrebbero essere invocate per evitare discriminazioni o altri effetti negativi sugli individui.		8	14.04%
Non saprei.		7	12.28%
Non risponde		0	0%

I diversi assessment che le norme o le interpretazioni delle autorità preposte impongono in capo ai produttori di tecnologie o ai titolari dei trattamenti hanno una ricaduta effettiva sulla tutela dei diritti?

		Answers	Ratio

Si, perché consentono di comprendere i punti di forza e i punti di debolezza di una determinata attività.		25	43.86%
No, perché vengono condotti in maniera poco accurata semplicemente per ottemperare a un obbligo.		30	52.63%
Non saprei.		2	3.51%
Non risponde		0	0%

Il GDPR può ancora rappresentare il testo di riferimento per la protezione dei dati personali, oppure è un testo di legge ormai datato?

		Answers	Ratio
Si è ancora attuale, per cui è corretto che i testi successivi della digital strategy europea vi facciano rimando.		43	75.44%
No è ormai superato, per cui bisognerebbe aggiornarlo al fine di evitare incongruenze o vuoti legislativi.		12	21.05%
Non saprei.		2	3.51%
Non risponde		0	0%

Ritieni che le autorità indipendenti attualmente presenti siano sufficienti, come numero e come competenze, a sorvegliare il rispetto delle norme rientranti nella strategia digitale dell'UE?

		Answers	Ratio
Si, perché molte competenze sono già in capo alle autorità esistenti e non si dovrebbe correre il rischio di sovrapposizioni.		43	75.44%
No, perché si correrebbe il rischio di creare concentrazioni di potere su singole autorità.		6	10.53%
Non saprei.		8	14.04%
Non risponde		0	0%

In tema di strategia digitale, ritieni che il processo legislativo seguito, che prevede anche la partecipazione della società civile mediante lo strumento della consultazione pubblica, sia adeguato o vada perfezionato?

		Answers	Ratio
Si, è adeguato perché consente a diversi attori di intervenire ed è quindi estremamente trasparente.		24	42.11%

No, non è adeguato perché il settore richiede una formazione delle leggi agile, mentre adesso il processo di approvazione è eccessivamente lungo.		29	50.88%
Non saprei.		4	7.02%
Non risponde		0	0%

La sovranità digitale deve essere davvero un tema centrale delle politiche UE?

		Answers	Ratio
Si, perché solo tramite essa si possono raggiungere gli effetti positivi, sia da un punto di vista dell'innovazione sia dal punto di vista della crescita economica, legati ai dati.		44	77.19%
No, perché è una forma di protezionismo che rallenta il mercato globale e crea diversi problemi di conformità agli operatori.		10	17.54%
Non saprei.		3	5.26%
Non risponde		0	0%

Nella strategia digitale dell'UE, si dà abbastanza risalto alle competenze digitali dei cittadini?

		Answers	Ratio
Si, perché i programmi educativi vengono ormai costruiti intorno a queste competenze.		5	8.77%
No, perché non si fa ancora abbastanza in termini di alfabetizzazione digitale.		51	89.47%
Non saprei.		1	1.75%
Non risponde		0	0%

Le politiche di riuso dei dati a livello europeo:

		Answers	Ratio
Sono corrette, perché solo così il dato può creare il massimo del suo valore.		34	59.65%
Non sono corrette, perché c'è il rischio che questi dati non siano sufficientemente protetti.		12	21.05%
Non saprei.		11	19.3%

Non risponde		0	0%

L'istituzione del Garante privacy è prevista dalla Carta dei Diritti Fondamentali dell'UE e dai Trattati. Gli atti legislativi della strategia UE sui dati prevedono l'istituzione di ulteriori Autorità Indipendenti lasciando libertà agli Stati di accorparle anche in capo ad Autorità già esistenti. Sei favorevole a questa moltiplicazione di Istituzioni amministrative?

		Answers	Ratio
Sì, perché ogni tema in ambito digitale ha bisogno di un presidio specifico.		9	15.79%
No, perché si rischia una situazione confusa con sovrapposizione di competenze.		46	80.7%
Non saprei.		2	3.51%
Non risponde		0	0%

L'eventuale accorpamento di compiti in materia di dati in capo all'Autorità Garante è secondo te preferibile?

		Answers	Ratio
Sì, perché si ha un governo omogeneo di materie strettamente connesse a beneficio anche della certezza del diritto.		38	66.67%
No, si rischiano conflitti di interesse ed il conferimento di poteri eccessivi e di varia natura in capo ad un'unica Istituzione.		15	26.32%
Non saprei.		4	7.02%
Non risponde		0	0%

La gestione dei dati personali ha risvolti anche in materia di tutela dei consumatori, tutela della concorrenza e tutela delle comunicazioni con il coinvolgimento delle pertinenti Autorità Indipendenti. Ritieni che il livello di cooperazione tra queste Istituzioni sia attualmente soddisfacente?

		Answers	Ratio
Sì, si registra già un buon livello di sinergia e cooperazione.		9	15.79%
No, non mi sembra che le autorità tengano in debita considerazione i profili di competenza di altre istituzioni omologhe.		43	75.44%

Non saprei.		5	8.77%
Non risponde		0	0%

Talvolta le Autorità hanno il compito di dirimere le controversie promosse dagli interessati, in aggiunta alla possibilità per gli stessi di adire l'Autorità giudiziaria. Ritieni che questo abbia facilitato l'esercizio del diritto di agire in giudizio in questo ambito?

		Answers	Ratio
Sì, i procedimenti dinanzi alle autorità sono generalmente più semplici, rapidi, meno formali e onerosi.		33	57.89%
No, la soluzione delle due vie procedurali, solo parzialmente alternative, aggiunge complessità ed incertezza.		17	29.82%
Non saprei.		7	12.28%
Non risponde		0	0%

In alcuni atti legislativi in materia di dati, in caso di violazioni è previsto l'ammonimento in alternativa all'irrogazione di sanzioni pecuniarie. Pur nel rispetto dei principi di effettività, efficacia e dissuasività delle misure di contrasto, ritieni preferibile interventi di ammonimento con obbligo di ripristino di comportamenti conformi?

		Answers	Ratio
Sì, anche a fini di moral suasion, occorrerebbe un maggiore bilanciamento tra provvedimenti ammonitori con obblighi di conformità e irrogazione di sanzioni pecuniarie.		44	77.19%
No, la diffusa non conformità e il divario culturale tra prassi e protezione dei dati richiede necessariamente l'adozione di sanzioni proporzionate, efficaci e dissuasive.		10	17.54%
Non saprei.		3	5.26%
Non risponde		0	0%

La potestà nomofilattica è rimessa al legislatore; tuttavia, si assiste alla produzione di linee guida e provvedimenti individuali ad opera delle Autorità con valore di precedenti cogenti di carattere generale. Ritieni che sussista il rischio di auto-referenzialità delle Autorità?

		Answers	Ratio

Sì, troppo spesso le autorità a fondamento delle proprie decisioni fanno riferimento a precedenti loro provvedimenti o linee guida prive di efficacia vincolante verso tutti.		32	56.14%
No, è normale e giusto che le autorità traccino percorsi interpretativi sulle materie di propria competenza. Questo rientra anche fra le specifiche competenze loro assegnate.		20	35.09%
Non saprei.		5	8.77%
Non risponde		0	0%

Nella società dell'informazione, il trattamento dei dati è normalmente transfrontaliero con impatti su più Stati. Nonostante specifiche regole di cooperazione tra le Autorità previste dalle leggi UE, il sistema solleva critiche sia riguardo al funzionamento del meccanismo di cooperazione sia nei casi in cui l'Autorità nazionale si consideri competente esclusiva. Sei d'accordo su questa soluzione di equilibrio tra cooperazione e competenza territoriale?

		Answers	Ratio
Sì, perché è un giusto bilanciamento che consente, da un lato, all'azienda pan-europea di interfacciarsi con una sola autorità capofila e, dall'altro, al singolo di rivolgersi alla propria autorità nazionale.		31	54.39%
No, perché il meccanismo di cooperazione tra le autorità è farraginoso e incide negativamente sulle effettive tutele dei singoli.		17	29.82%
Non saprei.		9	15.79%
Non risponde		0	0%

Molti atti legislativi europei sulla Strategia dei dati prevedono sanzioni solo per il massimo edittale in percentuale del fatturato globale dell'azienda che trasgredisce. La misura specifica è determinata talvolta applicando criteri definiti dal legislatore ma anche in tal caso vi è molta incertezza sulla misura della pena da applicare. Ritieni che questa modalità sia condivisibile per rispondere al principio di dissuasività della sanzione?

		Answers	Ratio
Sì, perché risponde sia all'esigenza di dissuasività sia a quella di determinare la misura della sanzione in modo proporzionale alla gravità della violazione e alle condizioni economiche del trasgressore.		22	38.6%

No, perché nonostante la definizione dei criteri di determinazione della misura della sanzione, si lascia troppo discrezionailità a chi le irroga.		32	56.14%
Non saprei.		3	5.26%
Non risponde		0	0%

Gli interventi correttivi delle Autorità possono essere promossi tramite reclami o d'ufficio. Nel caso di interventi d'ufficio c'è il rischio di accuse di protagonismo da parte dell'Autorità. Sei d'accordo?

		Answers	Ratio
Sì, sebbene spesso le Autorità pubblichino i temi oggetto di ispezioni programmate, gli interventi d'ufficio dipendono pur sempre da criteri ancora poco noti.		27	47.37%
No, gli interventi delle Autorità nei rispettivi ambiti di pertinenza soddisfano sempre criteri basati sul livello di effettiva rilevanza degli stessi.		19	33.33%
Non saprei.		11	19.3%
Non risponde		0	0%

In alcuni Stati, la potestà di irrogare sanzioni non è di competenza delle Autorità ma degli organi giudiziari cui le Autorità si rivolgono in caso di violazione accertata. Da noi, le sanzioni irrogate dalle Autorità possono essere impugnate dinanzi all'Autorità giudiziaria. Ritieni preferibile il nostro sistema?

		Answers	Ratio
Sì, il sistema dei due binari - quello amministrativo e quello giudiziario - è un giusto compromesso che tiene conto del diritto fondamentale della difesa in giudizio.		41	71.93%
No, il sistema dei due binari (amministrativo/giudiziario) crea confusione e penalizza la certezza del diritto: non è infrequente che per lo stesso oggetto, Autorità e giudice siano su posizioni differenti.		15	26.32%
Non saprei.		1	1.75%
Non risponde		0	0%

A tuo avviso, nel testo del GDPR e del Codice Privacy, la tutela garantita nei confronti dei soggetti più deboli e vulnerabili (ad esempio: minori, consumatori, anziani, vittime di reati), è:

		Answers	Ratio
Articolata e particolarmente efficace.		19	33.33%
Non la si percepisce né appare efficace.		32	56.14%
Non saprei.		6	10.53%
Non risponde		0	0%

Nel testo del GDPR, con riferimento all'uso dei termini e alle previsioni contenute, le disposizioni a tutela dei minori (e dei loro dati) sono:

		Answers	Ratio
Ben specificate ed efficaci.		19	33.33%
Non specificate né efficaci.		26	45.61%
Non saprei.		12	21.05%
Non risponde		0	0%

Se spettasse a te, come affronteresti la tutela dei soggetti deboli?

		Answers	Ratio
Interverrei rendendo il minore più consapevole.		30	52.63%
Interverrei incrementando i diritti e/o i poteri del minore.		23	40.35%
Non saprei.		4	7.02%
Non risponde		0	0%

Cosa pensi del ruolo delle associazioni degli interessati/utenti/consumatori nelle leggi sui dati e del loro impatto nella vita quotidiana degli interessati?

		Answers	Ratio
È un elemento eccellente di garanzia e difesa.		34	59.65%
Sono previste troppe tutele, che generano rischi impossibili da gestire per le organizzazioni che utilizzano i dati.		9	15.79%
Non saprei.		14	24.56%

Non risponde		0	0%

Ritieni giusto che l'interessato possa esercitare direttamente i propri diritti con modalità automatizzate e su larga scala? (ad esempio: i casi italiani che hanno riguardato Google Analytics nel pubblico e nelle scuole)

		Answers	Ratio
Sì, sono strumenti legittimi e molto efficaci a tutela dell'interessato.		29	50.88%
No, rischiano di essere strumenti illeciti che possono costituire abuso dei diritti, reati, tentativi di estorsione o spam.		24	42.11%
Non saprei.		4	7.02%
Non risponde		0	0%

Ritieni che il ruolo del DPO (soggetto indipendente che vigila sulla conformità al GDPR) sia anche quello di strumento/ruolo/funzione per la tutela dell'interessato?

		Answers	Ratio
Sì, il DPO deve poter essere a difesa dell'interessato anche contro la stessa organizzazione che utilizza i dati.		31	54.39%
No, il DPO deve soprattutto tutelare la governance dei dati nella realtà dell'organizzazione che utilizza i dati.		22	38.6%
Non saprei.		4	7.02%
Non risponde		0	0%

Recentemente si è assistito a una modalità di raccolta del consenso per l'uso dei dati basata sul "prendere o lasciare": vedi ad esempio i cookie walls degli editori, cioè se vuoi leggere devi accettare i cookie. Ritieni che questa modalità sia corretta?

		Answers	Ratio
Sì, è giusto adattare il consenso all'evoluzione tecnologica e monetizzare anche il semplice accesso ai siti web.		19	33.33%
No, sono consensi raccolti con costrizione, quindi sono illegali e questa pratica va sanzionata.		34	59.65%
Non saprei.		4	7.02%
Non risponde		0	0%

Il livello di sicurezza delle aziende più piccole lascia spesso a desiderare, permettendo casi di data breach altrimenti evitabili. Ritieni che le aziende maggiori all'interno della filiera debbano farsi carico dei livelli di sicurezza delle aziende minori?

		Answers	Ratio
Sì, le aziende maggiori, qualsiasi sia il loro ruolo, dovrebbero prendersi carico anche della sicurezza delle aziende minori che hanno accesso ai dati di loro pertinenza.		21	36.84%
No, ciascuna azienda, grande o piccola che sia, è responsabile del livello di sicurezza sui dati che attua nella propria organizzazione.		35	61.4%
Non saprei.		1	1.75%
Non risponde		0	0%

Ritieni sia adeguata l'attenzione dell'Autorità Garante italiana nei confronti delle piccole e medie imprese, sia a livello di attività ispettiva, sia di sanzioni irrogate?

		Answers	Ratio
Sì, è più che adeguata; peraltro il Garante dovrebbe occuparsi soprattutto delle grandi organizzazioni che utilizzano i dati.		20	35.09%
No, dovrebbe essere maggiore; oggi è marginale e sono oggetto di attenzione del Garante solo quelle casistiche legate a specifici reclami.		33	57.89%
Non saprei.		4	7.02%
Non risponde		0	0%

Ritieni che la tradizionale categoria dei "dati sensibili", ora "particolari" (es. salute e orientamento sessuale) sia sufficientemente specificata e tutelata?

		Answers	Ratio
Sì, a mio avviso l'elencazione dei dati sensibili è chiara e le tutele sono efficaci.		34	59.65%
No, ritengo vi sia ancora molta confusione tra quali dati siano sensibili o meno e questo incide negativamente anche sull'efficacia delle tutele.		20	35.09%
Non saprei.		3	5.26%

Non risponde		0	0%

Ritieni che negli ultimi anni il livello di protezione sui dati personali in ambito UE sia aumentato?

		Answers	Ratio
Sì, le novità normative europee hanno incrementato la tutela di diritti e libertà dei cittadini in relazione ai propri dati.		46	80.7%
No, da cittadino non ho ravvisato alcun incremento di protezione per i miei diritti e libertà riguardo ai miei dati personali.		10	17.54%
Non saprei.		1	1.75%
Non risponde		0	0%

Nel bilanciamento tra libera circolazione dei dati e tutela della riservatezza, ritieni che l'Europa dovrebbe favorire di più la prima?

		Answers	Ratio
Sì, l'Unione Europea dovrebbe ridurre gli obblighi e gli adempimenti per le organizzazioni che utilizzano i dati in modo da favorire una maggiore circolazione dei dati.		27	47.37%
No, gli obblighi e gli adempimenti per le organizzazioni che utilizzano i dati rappresentano garanzie irriducibili per gli individui.		25	43.86%
Non saprei.		5	8.77%
Non risponde		0	0%

Nell'elaborazione degli atti legislativi nell'ambito della strategia UE sui dati, ritieni che il controllo degli interessati sui propri dati debba essere la priorità?

		Answers	Ratio
Sì, solo un effettivo controllo sui dati da parte degli interessati può accrescere la fiducia di questi ultimi e, quindi, rendere efficace la strategia europea per un'economia basata sui dati.		36	63.16%
No, le politiche europee dovrebbero superare il binomio informativa-consenso che costituisce il maggiore ostacolo ad un'economia basata sui dati.		18	31.58%
Non saprei.		3	5.26%

Non risponde		0	0%

I servizi online ci hanno abituato alla prassi della loro fruizione "gratuita", a fronte della raccolta e uso dei dati personali dell'utente. Ritieni che questo scambio possa essere rimesso alla libera scelta del singolo?

		Answers	Ratio
Sì, ciascuno di noi è pienamente in grado di opzionare in libertà le condizioni di questo scambio.		21	36.84%
No, nei fatti il singolo utente non è in grado di operare una libera scelta.		34	59.65%
Non saprei.		2	3.51%
Non risponde		0	0%

Ritieni che a livello europeo si possa parlare di iper-regolamentazione digitale? E che questo sia un problema che rischia di imbrigliare lo sviluppo del mercato digitale?

		Answers	Ratio
Sì, gli operatori economici sono molto ostacolati da una regolamentazione di eccessivo dettaglio che rischia di degradare in mera burocrazia.		30	52.63%
No, le norme europee disciplinano il nuovo mercato digitale che, per un suo ottimale sviluppo, necessita di regole chiare e specifiche.		21	36.84%
Non saprei.		6	10.53%
Non risponde		0	0%

Ritieni che per il mercato digitale siano preferibili discipline basate su principi generali in alternativa a regole di dettaglio?

		Answers	Ratio
Sì, in ambito digitale, gli operatori economici avrebbero maggiori opportunità relazionando i propri comportamenti a principi generali di diritto.		44	77.19%
No, gli operatori necessitano di norme specifiche di dettaglio per sviluppare al meglio il mercato digitale.		9	15.79%
Non saprei.		4	7.02%

Non risponde		0	0%

Ritieni che nel contesto online - caratterizzato da rapporti virtuali e immediatezza delle transazioni - il singolo consenso dell'interessato possa ancora validamente giustificare l'utilizzo dei suoi dati?

		Answers	Ratio
Sì, il consenso dell'interessato rimane ancora la migliore espressione di quel potere di controllo sui propri dati che è alla base del rapporto fiduciario essenziale per un'ottimale sviluppo del mercato digitale.		22	38.6%
No, il fatto che le transazioni virtuali fondate sui dati siano condizionate a singole e specifiche autorizzazioni dei soggetti interessati appare del tutto insostenibile. Quindi, occorre individuare nuove soluzioni più rispondenti al mondo digitale.		35	61.4%
Non saprei.		0	0%
Non risponde		0	0%

Le tecniche di advertising possono oggi essere molto invasive. Ritieni che, in aggiunta alle specifiche leggi, vi sia la necessità di tracciare linee guida e prassi operative in grado di cogliere e disciplinare meglio le particolarità del sistema pubblicitario digitale?

		Answers	Ratio
Sì, linee guida, prassi operative ma anche codici di condotta ed altri strumenti di soft law ben possono coprire adeguatamente quell'ampia area grigia in cui si muove il complesso mercato della pubblicità digitale. Questo approccio favorisce meglio sia il business pubblicitario, sia la tutela dei consumatori.		53	92.98%
No, il mercato della pubblicità digitale è già ampiamente regolamentato.		2	3.51%
Non saprei.		2	3.51%
Non risponde		0	0%

Il cosiddetto web 3.0, basato sull'interoperabilità di sistemi e piattaforme, rappresenta la sfida lanciata in alternativa alle forti concentrazioni di potere delle BigTech. Ritieni che i fenomeni di decentralizzazione, blockchain e del metaverso in generale, che sono alla base di questa sfida, trovino un'adeguata regolamentazione nell'attuale impianto normativo?

		Answers	Ratio

Sì, le sfide rappresentate dal web 3.0 possono trovare soddisfacente disciplina con le regole già esistenti.		10	17.54%
No, l'attuale impianto normativo non è in grado di disciplinare fenomeni innovativi con implicazioni ancora in corso di analisi.		39	68.42%
Non saprei.		8	14.04%
Non risponde		0	0%

Ritieni che i principi delle normative vigenti siano tecnologicamente neutri e sufficientemente flessibili tanto da potersi applicare agli sviluppi futuri?

		Answers	**Ratio**
Sì, i principi delle normative vigenti sono tecnologicamente neutri e hanno un sufficiente grado di flessibilità per potersi applicare anche a prevedibili sviluppi futuri.		28	49.12%
No, il celere sviluppo tecnologico è tale da non permettere al vigente impianto regolatorio di disciplinarne adeguatamente le implicazioni che esso determina sulla società.		26	45.61%
Non saprei.		3	5.26%
Non risponde		0	0%

Officine Dati

ISLC
Information Society Law Center

PRIMA EDIZIONE

GLOBAL DATA CONFERENCE 2023

Finito di stampare il 14/12/2023