I principi e le competenze fondamentali al servizio della digital compliance aziendale

Si chiede spesso al diritto di inseguire la tecnologia digitale che in questo periodo sta compiendo passi da gigante. E **ogni novità, dall'intelligenza digitale alla blockchain sino al metaverso, si porta dietro insistite richieste di regolamentazione**, perché i rischi che l'innovazione tecnologica porta con sé non sarebbero sostenibili e metterebbero in discussione la stessa nostra esistenza.

Lungi dal voler affrontare l'arduo compito di comprendere come le nuove tecnologie possano sconvolgere (in bene o in male) le nostre esistenze, mi limiterò a fornire una **breve guida su come procedere in punto di diritto**, in modo di evitare di chiedere al legislatore ciò che è bene che non faccia, così da consentire, magari, a professionisti preparati in ottica interdisciplinare di procedere con consapevolezza lungo i binari delle regolamentazioni già esistenti e tracciare finalmente un quadro solido per l'innovazione che vogliamo portare avanti per il nostro Sistema Paese.

Effettivamente, come vedremo insieme, **il diritto** – a livello legislativo – **deve e dovrebbe rimanere regolamentazione di fattispecie astratte, lasciando a noi interpreti il compito delicato di adattare alla realtà mutevole**, che oggi caratterizza la nostra esistenza, **i principi generali** che si sono stratificati lungo centinaia di anni. E questo significherebbe sostanzialmente **dare piena attuazione al fondamentale principio** – di ispirazione common law – **dell'accountability** che contraddistingue le regolamentazioni europee più recenti in materia di mercati digitali e libera circolazione dei dati.

Elemento dirimente per noi professionisti, attenti interpreti di una realtà che sta vertiginosamente cambiando, **è comprendere come vadano correttamente usate le risorse** che abbiamo a disposizione e in queste rientra senz'altro l'evoluzione tecnologica. Ciò nell'ottica di non scivolare e magari rovinare in adempimenti ad uso esclusivamente burocratico.

I rischi insiti nello sviluppo di tecnologie digitali

Ovviamente **la realtà digitalmente mutevole** che riguarda noi tutti va osservata con attenzione per poter **essere con pazienza regolamentata in modo concreto e proattivo**. E, ciò che oggi è certo, è che qualsiasi direzione – più o meno metaversica e più o meno intelligente – dovesse prendere la tecnologia digitale, **il cuore pulsante dell'evoluzione sarà costituito dalla gestione di enormi database profilatissimi** in modo compatibile con i nostri diritti fondamentali. Quindi, in una società evidentemente datificata, assicurare la pienezza del valore alle proprie informazioni digitali dovrebbe risultare un'ovvietà per qualsiasi ente (pubblico o privato). Appare pertanto inevitabile, per chi si occupa di sviluppare dei processi innovativi, avere come fine ultimo di ogni sua azione **il perseguimento costante dei principi della security e della privacy by design (e by default)**.

Del resto, avere in pancia del proprio sistema aziendale dati e informazioni manipolabili e accessibili a chiunque credo che oggi non convenga a nessuno e rischierebbe di compromettere il valore di qualsiasi processo di digitalizzazione, oltre che incrinare irrimediabilmente la propria reputation. Infatti, come ribadisce il **considerando 75 del GDPR** (Regolamento (UE) 2016/679 del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati), **qualsiasi trattamento di dati personali può comportare rischi specifici per gli interessati a quei trattamenti**[1]. E la possibile esposizione a

1. Secondo il considerando 75 "I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano l'origine

specifici rischi per i diritti e libertà degli interessati comporta per qualsiasi ente che sviluppa progetti di innovazione digitale una particolare e indispensabile attenzione alla compliance normativa in materia IT, salvo rischiare di esporsi a pesantissime sanzioni e/o richieste di risarcimento danni da parte di interessati violati nei loro diritti e libertà fondamentali.

Il valore del dato

Per qualsiasi ente pubblico o privato è quindi oggi indispensabile **perseguire strategie organizzative per gestire e custodire i propri dati. Garantire la qualità, la corretta accessibilità, l'interoperabilità, l'integrità, l'immodificabilità, quindi, la sicurezza e l'autenticità al proprio patrimonio informativo è fondamentale**: raggiungere **un modello corretto di compliance** sui propri dati (personali e non[2]) deve entrare così nelle corde di qualsiasi società o pubblica amministrazione. Vanno, pertanto, governati e custoditi i propri dati rilevanti, attraverso **accurate analisi del rischio** che assicurino adeguate misure di sicurezza a protezione di ogni asset informativo.

Le registrazioni affidabili costituiscono, del resto, i documenti del nostro presente digitale ed essi possono essere assicurati nel loro valore solo da un corredo di metadati che abbia una logica anche archivistica. E per un qualsiasi ente gli stessi data breach – ormai entrati prepotentemente nella cronaca dell'ultimo periodo – non possono essere valutati solo come personal data breach, così come **i DPO (Data Protection Officer e Digital Preservation Officer) devono trovare un ruolo che sia di presidio complessivo del patrimonio informativo pubblico o privato**.

L'accountability nella gestione efficace di database e archivi digitali

Nella necessaria tutela dei propri patrimoni informativi e documentali si intersecano normative diverse con obiettivi ultimi spesso coincidenti. In particolare, **i principi di esattezza, affidabilità, integrità, immodificabilità, autenticità, trasparenza e accessibilità riecheggiano nelle normative generali** che regolamentano la materia, come il **Codice dell'amministrazione digitale**[3] (che si occupa proprio di delineare i presidi fondamentali della gestione e conservazione del proprio patrimonio informativo e documentale), o il già citato **GDPR** (in materia di protezione dei propri database) e il **D. Lgs. 33/2013** (su open data, trasparenza e pubblicità legale online). A queste normative andrebbero aggiunti i vari regolamenti europei in vigore che oggi si occupano di delineare un quadro uniforme per favorire lo sviluppo dei mercati digitali[4].

Per concretizzare tali principi **occorre predisporre quindi processi, metodologie e regole** per un records management che sia finalizzato a **mantenere custodito nel tempo il contesto di dati (anche strutturati), informazioni e documenti (anche e soprattutto nativi) digitali rilevanti** per gli enti pubblici e privati attraverso altresì una regolamentazione contrattuale consapevole. E per raggiungere tali obiettivi non occorre partire dalla scelta tecnologica (scelta

razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati".

2. Ci troviamo oggi infatti in una dimensione di completa digitalità, quindi – come già riferito – di esistenza "datocentrica" e inevitabilmente sfumano i codici ontologici che ci permettono di separare concettualmente in modo netto il dato personale da quello non personale, il documento dall'informazione, la firma dall'identità. In altre parole, siamo noi stessi assurti a "valore di riferibilità" in relazione ai dati rilevanti, personali e non, che ci riguardano.

3. Decreto legislativo 82/2005.

4. Faccio riferimento ai regolamenti UE noti agli studiosi della materia e conosciuti con gli acronimi eIDAS, DSA, DMA, DGA, o anche DORA e NIS.

che deve essere invece l'esito di una valutazione ponderata e responsabile), ma è indispensabile operare delle **costanti verifiche sulla propria compliance legale e organizzativa**, quindi dedicarsi **a definire con attenzione competenze, ruoli e responsabilità interdisciplinari**, prima dell'avvio di qualsiasi progetto con impatto digitale.

Come garantire la digital compliance?

La digital compliance è un processo a tappe, di trasparente mappatura, prima di tutto, e che comporta una visione a 360° tra discipline diverse in grado di presidiare materie così complesse e affascinanti. Infatti, i vari **documenti e contratti** che le diverse discipline normative prevedono (e che corredano l'accountability dei processi di digitalizzazione) **devono a loro volta "parlarsi tra loro"**. E tali documenti devono quindi essere frutto di una **coordinata mappatura e un'analisi del rischio portate avanti da team interdisciplinari**, come appunto la normativa prevede.

La necessità di favorire lo sviluppo di team interdisciplinari per poter cavalcare l'innovazione digitale

Progetti che perseguano l'assioma del "Digital First" hanno bisogno di **interdisciplinarità, quindi di "interferenze" tra professionalità molto diverse** che siano capaci di confrontarsi su obiettivi comuni, focalizzandosi su una corretta mappatura sia dei flussi informativi e documentali e sia dell'intera organizzazione (fatta di tecnologie e risorse umane) a presidio degli stessi. Da tale trasparente mappatura si può ricavare una **verifica puntuale delle soluzioni applicative**, anche per assicurare una **coerente applicazione dei (tante volte citati) principi della privacy by design e della privacy by default, come individuati nell'art. 25 del GDPR**.

In particolare, secondo il **considerando 78 del GDPR** "in fase di sviluppo, progettazione, selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati personali o che trattano dati personali per svolgere le loro funzioni, i produttori dei prodotti, dei servizi e delle applicazioni dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati allorché sviluppano e progettano tali prodotti, servizi e applicazioni e, tenuto debito conto dello stato dell'arte, a far sì che i titolari del trattamento e i responsabili del trattamento possano adempiere ai loro obblighi di protezione dei dati. I principi della protezione dei dati fin dalla progettazione e di default dovrebbero essere presi in considerazione anche nell'ambito degli appalti pubblici".

In estrema sintesi, **la tecnologia rimane uno strumento indispensabile di sviluppo per aziende pubbliche e private**, ma per essere volano di crescita, senza rischiare di calpestare diritti e libertà fondamentali, **ha estremo bisogno di presidi organizzativi** in grado anche di **dare concretezza e documentare in modo affidabile alcuni principi fondamentali** su cui si fonda oggi il nostro intero ordinamento giuridico.

Andrea Lisi
segreteria@studiolegalelisi.it

Il contributo è apparso originariamente sul numero di giugno-luglio di "Cybermagazine", la rivista curata da Assintel, dedicata alla cybersecurity e alla tecnologia digitale.