Impresa sociale e privacy

Appunti per un corretto approccio al principio di Accountability

Gianna Vignani, | 06 giugno 2022

Introduzione

Quando parliamo di privacy e protezione dati capita spesso di cogliere nell'interlocutore, salvo che non si tratti di operatore del settore, un istintivo irrigidimento nei confronti di una materia che è percepita quasi come una nebulosa, priva di chiari riferimenti e punti fermi. Più o meno sulla stessa lunghezza d'onda si collocano le imprese, che nel comune sentire vivono spesso gli adempimenti connessi alla regolamentazione europea dettata dal Regolamento UE 2016/679 (GDPR) come inutili appesantimenti burocratici imposti in nome di un principio di matrice unionale, quello di *accountability*, esso stesso di difficile comprensione e spesso anche di difficile integrazione all'interno delle singole organizzazioni. Il mondo della cooperazione sociale ha ben presente queste difficoltà, che si esprimono sia sotto il profilo dell'integrazione con la cultura dell'organizzazione, condizionata non poco dal rapporto committente-fornitore con le pubbliche amministrazioni, sia sotto il profilo delle forme tradizionali di erogazione dei servizi, fortemente basate sulla relazione umana[note]Queste note raccolgono il lavoro di ricerca svolto da UP Umanapersone R&S, in particolare dal Gruppo di progetto Privacy, coordinato da Gianna Vignani e di cui fanno parte: Barresi Giuliana, D'Aniello Alessio, De Luca Benedetta, Meiattini Sacha, Pacella Nicla, Ragazzo Nicolò, Receputi Valentino, e altri.[/note].

La scelta di UP Umanapersone R&S

A distanza di quattro anni circa dall'entrata in vigore della normativa europea, l'impressione è che continui a perdurare la fatica di interiorizzare certi concetti e di integrare nei processi certi approcci. Tuttavia, già prima dello scoppio della pandemia, all'interno della rete di imprese UP Umanapersone R&S si è posta l'esigenza di condividere con le organizzazioni aderenti un cammino di crescita su tali tematiche. Terreno di elezione è costituito dai progetti regionali, nazioni ed europei per la sperimentazione delle **tecnologie assistive** nell'ambito dei contesti in cui vengono erogati servizi alla persona (prevalentemente servizi domiciliari per persone con disabilità e anziani fragili)[note]Vedasi in tal senso l'area operativa denominata Digitalizzazione e Tecnologie Assistive.[/note] che ha visto impegnate sul campo le imprese associate.

In particolare, è stato costituito un gruppo di progetto, composto dai soggetti referenti interni alle cooperative e dagli esperti consulenti esterni, avvocati ed ingegneri, gruppo ormai stabile ed operativo dal 2020. Scopo principale quello di presidiare gli aspetti di privacy e protezione dei dati connessi allo svolgimento delle attività progettuali, ma anche quello di coltivare competenze nuove attraverso l'esperienza concreta che possano essere divulgate all'interno delle organizzazioni.

Il percorso

Nella prospettiva di attuazione del GDPR, in questi anni si è registrata maggior difficoltà a dar seguito a quegli adempimenti che richiedono l'attivazione di cambiamenti organizzativi permanenti, quali ad esempio processi interni volti a garantire la minimizzazione dei dati trattati (ossia trattare solo i dati strettamente necessari in relazione alle finalità) ed il rispetto del principio di conservazione dei dati limitato nel tempo. Si tratta invero di obiettivi che per essere effettivi richiedono la revisione dei processi, o quantomeno la loro integrazione, con altre funzioni aziendali, destinate auspicabilmente ad operare in modo stabile e trasversale rispetto all'intera organizzazione. Viceversa, esistono adempimenti che possono essere assolti *una tantum* ovvero ciclicamente ma non costantemente – si pensi ad esempio alla nomina della figura del Responsabile per la Protezione dei Dati, DPO, oppure alla predisposizione delle informative sul trattamento dati – rispetto ai quali risulta esservi

una maggiore responsività[note]Ciò sembra in linea con una survey condotta a maggio 2018 da Oracle Community for Security, in collaborazione con Protoviti, Clusit, Aused ed Europrivacy, i cui risultati sono consultabili e scaricabili dal web. [/note].

In generale, un adeguamento reale ed efficace, ossia che dia concreta attuazione ai principi ivi contenuti, comporta dei costi diretti (es: nuove nomine) ed indiretti (es: formazione personale, adeguamento processi) e questo rappresenta di per sé un fattore di resistenza per organizzazioni, sottoposte a contrazione di risorse legate agli affidamenti pubblici.

I driver digitalizzazione e pandemia

C'è da dire che la spinta alla digitalizzazione, autonoma come nel caso di UP Umanapersone R&S, o indotta dall'emergenza sanitaria, ha incentivato percorsi di crescita ed una presa di coscienza, almeno parziale, in ordine ai rischi derivanti dalla violazione dei dati personali connessi all'uso delle tecnologie, comprese quelle più semplici (tablet, smartphone, smartwatch, sensoristica, ecc.).

Non vi è dubbio che una più chiara e realistica percezione del rischio in ordine alle conseguenze e agli impatti, in termini economici, operativi e finanche reputazionali che possono derivare da una violazione dei dati personali, condizioni significativamente la valutazione del rapporto costi-benefici di cui sopra. Molto però dipende dal livello di consapevolezza, maturità e sensibilità che un'organizzazione e le persone che la compongono possiedono sul tema.

È bene precisare che quando si fa riferimento alle persone, si intendono livelli differenti delle funzioni aziendali: da quella più strettamente operativa e di coordinamento, che dovrà assumere una confidenza consapevole rispetto all'uso di quei mezzi tecnologici a supporto della presa in carico dell'utenza (anche alla luce del delicato ruolo di "facilitazione" all'uso della tecnologia da parte degli utenti che sta emergendo dall'esperienza concreta)[note]Toccafondi L., Vignani G., "Innovazione tecnologica e servizi sociosanitari e assistenziali", *Prospettive Sociali e Sanitarie* n. 2 - Primavera 2022, p. 15 e ss.[/note]; a quella direzionale e strategica per le ragioni che verranno accennate nel prosieguo. Per questo, la corretta e realistica percezione del rischio è uno degli snodi centrali su cui si è concentrata una significativa parte del lavoro di UP Umanapersone R&S, sia sul campo che mediante appositi momenti formativi.

Valutare lo stato dell'arte

Per settare il punto di partenza si è partiti dalla replica di una survey condotta su larga scala dal Clusit[note]Clusit, Associazione Italiana per la Sicurezza Informatica.[/note], contenuta nel Rapporto 2021[note]Tratta da Rapporto Clusit 2021 sulla sicurezza ICT in Italia e scaricabile da questo link.[/note] e intitolata "*La percezione delle aziende e organizzazioni italiane in merito alle minacce informatiche, all'impatto degli attacchi e alla capacità di difesa*". I risultati più significativi, emersi dalla survey di Clusit condotta su un campione di 304 aziende, per lo più medio-piccole, erano i seguenti: *(i)* il 23% delle aziende dichiara di aver subito nel corso del 2020 un attacco informatico; *(ii)* nel 60% dei casi i danni si sono rivelati di grave o media entità (esfiltrazione/perdita di dati, danni di natura economica, danni di immagine, danni infrastrutturali, danni derivanti della interruzione di continuità operativa); *(iii)* il 41% delle aziende ritiene di essere poco o per niente in grado di difendersi in caso di attacchi informatici; *(iv)* il 48% delle aziende ritiene altamente probabile il rischio di subire un attacco; *(v)* il 43% delle aziende dichiara di avere poca o nessuna consapevolezza circa le conseguenze di un potenziale attacco; *(vi)* il 46% delle organizzazioni dichiara di non aver predisposto una formazione mirata su tali tematiche; *(vii)* il 95% delle aziende ritiene molto utile l'attivazione di una formazione mirata; *(viii)* il 56% delle aziende non opera alcuna verifica in ordine ai requisiti di sicurezza di terze parti fornitrici.

Ebbene, ciò che è emerso dalla parallela survey riproposta internamente si pone in linea, tenuto conto delle opportune proporzioni, con i risultati descritti, che delineano in buona sostanza un deficit di alfabetizzazione tecnologica di base. In questo senso, per far capire il concetto di ***rischio privacy***, sulla base della nostra esperienza risulta essenziale chiarirne la relazione con quelli di protezione dei dati e sicurezza.

Evidenziare le differenze: Privacy, protezione dei dati e sicurezza

Tecnicamente evocano aspetti differenti, ma basti sapere che la prima si realizza attraverso misure volte a garantire **tre fondamentali proprietà dei dati:** confidenzialità, integrità e disponibilità. Poiché tuttavia la compromissione di una di queste proprietà può dipendere anche da un incidente di sicurezza (si pensi ad es. ad una campagna di *phishing* delle credenziali di account aziendali che consente ad un extraneus di avere accesso ai dati sensibili di utenti) è fondamentale tenere in considerazione questi fronti tra loro strettamente interconnessi. Peraltro, di sicurezza del trattamento si parla espressamente all'art. 32 GDPR[note]Il quale recita: "tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche al rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento ed il responsabile del trattamento mettono in atto misure tecniche ed organizzative adeguate per garantire il livello di sicurezza adeguato al rischio, che comprendono, se del caso:….".[/note].

Dalla disposizione emergono una serie di elementi significativi. Innanzitutto, il contesto specifico in cui un'organizzazione opera, e i limiti di risorse che la stessa ha, sono variabili da tenere in considerazione per individuare le misure di sicurezza più adeguate al rischio a cui si è esposta.

In secondo luogo, la norma non impone soluzioni preconfezionate, valide per tutti - il c.d. approccio "a checklist" -, né di sostenere costi per soluzioni standardizzate. Al contrario, richiede di attivare processi di analisi, valutazione e ponderazione interni che conducano l'ente alla definizione dell'insieme di soluzioni più adatte a sé stesso. In questo senso, con l'espressione "se del caso", la norma elenca anche una serie di soluzioni possibili ma lascia aperto un ampio margine di operatività demandata evidentemente al soggetto che deve compiere le scelte.

Leggere l'accountability alla luce della strategia di impresa

È su questo punto che si coglie maggiormente il valore più profondo della nozione di *accountability*.

Come si diceva in apertura la nozione è complessa, ma sotto questa prospettiva viene tendenzialmente ricondotta al concetto di responsabilizzazione dell'ente in ordine alle scelte fatte. Non c'è dubbio che tale forma di responsabilizzazione imponga un notevole sforzo di autoanalisi, essendo questo preliminare e necessario alla definizione del set di misure adeguate, ma è evidente come il punto di tenuta dell'*accountability* non si giochi tanto sotto il profilo della quantità, quanto piuttosto sotto il profilo della qualità dell'investimento fatto. Con questo approccio, è davvero possibile che il GDPR possa diventare uno strumento di miglioramento ed anche una leva di vantaggio competitivo.

Le iniziative di formazione interne a UP Umanapersone R&S sono state fortemente centrate sul far crescere culturalmente le organizzazioni al fine di promuovere processi interni di cambiamento. In particolare, l'approccio al rischio ha meritato e merita la profusione degli sforzi maggiori per le realtà cooperativistiche, in quanto risulta ad oggi fortemente depotenziato. In direzione opposta, il percorso di UP Umanapersone R&S ha incentivato le imprese sociali a orientarsi verso segmenti di mercato, quali quello privato, a domanda individuale o collettiva, quello della finanza d'impatto, ovvero verso nuove forme di modelli di servizio, rispetto ai quali, inevitabilmente, è necessario assumere approcci differenti.

E qui veniamo al tema della **strategia di impresa**. Stando ai dati, si registra in taluni casi un ritorno di investimento[note]CISCO, Data Privacy Benchmark study, 2020.[/note] rispetto ai costi sostenuti per l'adeguamento e la crescita nei settori della protezione dei dati e della privacy in termini di: apertura di nuovi segmenti di mercato; attivazione di nuove partnership commerciali; aggiudicazione di nuove commesse o maggior attrattività presso investitori. Questo significa che l'allocazione delle risorse in questo settore deve essere concepita anche come investimento strategico, demandato alla competenza dell'organo direzionale e con un suo convinto *engagement*, da comunicare efficacemente all'interno dell'organizzazione e al panorama degli stakeholder.

L'approccio strategico nasce in particolare dalla presa di coscienza che i dati sono veri e propri *asset* aziendali ed hanno valore, non solo etico-legale, ma anche economico, in quanto consentono di orientare in maniera capillare e personalizzata il

servizio o la prestazione offerti, per non parlare del valore predittivo dei Big Data e dell'intelligenza artificiale.

L'obiettivo della personalizzazione del servizio, così come la customizzazione dei prodotti di consumo, mostra come le imprese sociali che offrono servizi alla persona godano di un patrimonio informativo di inestimabile valore, non per mere finalità lucrative, ma per migliorare quantità e qualità dell'offerta. Questi dati meritano pertanto di essere sfruttati e, ancora prima, opportunamente presidiati da tutti gli attori che intervengono nel loro ciclo di vita, un'unica filiera, di imprese sociali e pubbliche amministrazioni, che non sempre dimostrano un livello di maturazione adeguato.

Le varie declinazioni dell'accountability

Si è accennato alla capacità di comunicare sia internamente che esternamente il valore di certe scelte e delle attività svolte sul tema della protezione dei dati. Ciò rinvia alla seconda importante dimensione in cui si declina il concetto di accountability, quella che viene solitamente accostata al concetto di trasparenza e che si concretizza nella capacità di tracciare e dare opportunamente conto del percorso decisionale svolto, delle scelte fatte e delle ragioni poste a fondamento di suddette scelte.

Anche questa dimensione passa attraverso una realizzazione spesso onerosa ma è per molti versi il logico completamento della precedente.

Conclusioni

Il concetto di accountability merita di essere attentamente considerato non solo come mera fonte di oneri rendicontativi, bensì come potenziale leva strategica di sviluppo e competitività, basata sulla consapevolezza che i dati hanno un valore.

Non considerare questa seconda prospettiva per mera mancanza di alfabetizzazione digitale o resistenza al cambiamento può rappresentare un rischio concreto per le scelte strategiche che l'ente è chiamato a compiere nei prossimi anni.

L'esperienza di UP Umanapersone R&S dice di soffermarsi e prendere in seria considerazione i risvolti prospettati, approfondendoli eventualmente anche con l'ausilio di esperti e calandoli attentamente all'interno dello specifico contesto di riferimento, poi permette di assumere decisioni in piena consapevolezza[note]Un utile riferimento è la Guida di ENISA, Guidelines for SMEs on the security of personal data processing, 2016.[/note].