CYBERSECURITY E DATA PROTECTION: UN INSCINDIBILE BINOMIO[*]

Carla Cosentino[**]

Digital first: questo è il principio che muove la legge 7 agosto 2015 n. 124 in materia di innovazione e riorganizzazione della Pubblica Amministrazione.

La finalità del legislatore è incentivare la fruizione dei servizi pubblici in modalità digitale ogni qual volta non sia strettamente necessario recarsi fisicamente negli uffici a ciò preposti. L'ammodernamento della Pubblica Ammistrazione deve tradursi nel trasferimento dallo spazio fisico a quello digitale.

Non è casuale quindi che la digitalizzazione della P.A. sia tra le componenti cui sono destinate buona parte delle risorse economiche stanziate nel Piano nazionale di ripresa e resilienza (PNRR).

In tale prospettiva ben si comprende come non possa che essere la sicurezza informatica il presidio utile e indispensabile a garantire il processo di ammodernamento in corso, se solo si rifletta sulla circostanza che più il servizio pubblico è digitale, maggiore è il rischio cyber al quale risulta esposto. Ed infatti l'art. 1 della l. n. 124/2015, rubricato "Carta della cittadinanza digitale", individua tra i criteri direttivi del provvedimento legislativo, la necessità di approntare "strumenti per definire il livello minimo di sicurezza, qualità, fruibilità, accessibilità e tempestività dei servizi on line delle amministrazioni pubbliche".

La sicurezza digitale figura al primo posto della lista dei criteri redatta nel testo legge.

Nel 2022 i primi bandi del PNRR rivolti a digitalizzazione, innovazione e sicurezza della Pubblica Amministrazione si sono concentrati sulla necessità di approntare un idoneo sistema di cybersecurity dei servizi pubblici.

Il leit motiv di tali bandi è stata l'analisi della c.d. "postura di sicurezza", ossia l'esame della sicurezza cibernetica nella quale si trova la P.A. Quest'ultima va, a sua volta, definita in relazione al "Framework nazionale per la Cybersicurezza e la Data Protection", predisposto a febbraio del 2019 dal CIS-Sapienza Research Center of Cyber Intelligence and Information Security presso l'Università Sapienza di Roma e dal CINI (Consorzio Interuniversitario

[*] Relazione del 27 ottobre 2023, svolta in occasione dell'evento annuale di presentazione del Jean Monnet Module "Digital Education and Consent to Data Processing", dal titolo "Pubblica amministrazione e protezione dei dati personali", presso l'aula consiliare del Consorzio di bonifica integrale – comprensorio di Sarno, Nocera inferiore (SA).

[**] Ricercatore di Diritto privato comparato presso il Dipartimento di Scienze Giuridiche dell'Università degli Studi di Salerno.

Nazionale per l'Informatica) Cybersecurity National Lab con il supporto dell'Autorità Garante per la protezione dei dati personali e del Dipartimento delle informazioni per la sicurezza della Presidenza del Consiglio dei ministri. ll rischio legato al verificarsi di attacchi informatici, che possano compromettere la sicurezza di informazioni o operazioni, è una realtà con cui tutte le organizzazioni pubbliche e private, operanti nei più disparati settori produttivi, devono confrontarsi.

Il Framework Nazionale per la Cybersecurity e la Data Protection rappresenta un punto di riferimento adottato da realtà fortemente eterogenee (dalla grande P.A. alla piccola impresa) come strumento per l'organizzazione della propria strategia di difesa rispetto alle minacce cibernetiche.

Tale Framework, racchiude tutte le indicazioni in materia di privacy dettate dal relativo Regolamento sulla protezione dei dati (reg. UE 2016/679), entrato in vigore nel 2018.

Digitalizzazione è quindi data protection che per il legislatore europeo significa, in linea teorica, la ricerca di un continuo bilanciamento tra circolazione dei dati e protezione dei soggetti titolari dei dati medesimi.

Il Gdpr costituisce una sorta di Giano bifronte, un compromesso tra due opposte istanze: da un lato il fenomeno circolatorio fortemente voluto dall'Unione Europea, che mira a promuovere lo sviluppo economico e tecnologico attraverso la costituzione di un mercato digitale, dall'altro l'esigenza di tutelare l' eccessiva esposizione dei dati personali.

E qui veniamo al *puntum dolens*.

Il bilanciamento, auspicato dalla legislaziona europea, risulta di difficile attuazione: spesso si assiste infatti ad un sacrificio del consenso dell'interessato per necessità considerate prevalenti e quindi ad una esposizione dei suoi dati personali, prescindendo da un atto di volontà, in omaggio alla primaria esigenza di circolazione degli stessi.

Ed infatti la base del trattamento non è più esclusivamente consensocentrica, ben potendo collocarsi su un un altro "legittimo fondamento previsto dalla legge", come recita l'art. 6 del Regolamento, il quale nello specificare che la liceità del trattamento è subordinata ad almeno una delle condizioni *ivi* previste, le parifica tra loro, ponendole tutte sul medesimo piano, senza che il consenso possa essere considerato regola e le altre eccezioni alla stessa.

Si pensi al legittimo interesse del titolare del trattamento, a titolo esemplificativo, che può motivare il trattamento dei dati, purchè non prevalgano gli interessi o i diritti o le libertà fondamentali dell'interessato (in special modo se si tratta di un minore), tenuto conto delle

ragionevoli aspettative dello stesso in base alla relazione con il titolare del trattamento (Considerando n. 47 del Gdpr).

Si rammenta che i dati di cui parliamo costituiscono espressione dell'identità dei soggetti cui si riferiscono, soprattutto con riguardo ai dati sensibili, si tratta cioè dell'estrinsecazione della personalità degli individui.

Il Garante europeo e quello italiano hanno in più occasioni messo in guardia sulla pericolosità di consentire il trattamento di dati personali alla stregua della cessione di una comune merce.

E tuttavia la prospettiva emergente già nei Considerando del Gdpr è quella circolatoria, come si legge nel n. 5 secondo il quale "L'integrazione economica e sociale conseguente al funzionamento del mercato interno ha condotto ad un considerevole aumento dei flussi transfrontalieri di dati personali e quindi anche dei dati personali scambiati, in tutta l'Unione tra attori pubblici e privati, comprese persone fisiche, associazioni e imprese. Il diritto dell'Unione impone alle autorità nazionali degli Stati membri di cooperare e scambiarsi dati personali per essere in grado di svolgere le rispettive funzioni o eseguire compiti per conto di un' Autorità di un altro Stato membro". Rimarcata dall'art. 4 del Gdpr per il quale "Il trattamento dei dati personali dovrebbe essere al servizio dell'uomo. Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità".

Oggi la realtà è in effetti orientata in tal senso.

Basta navigare pochi minuti in Internet per rendersi conto che la maggior parte dei contenuti sono accessibili ormai solo mediante il consenso al trattamento dei dati, che tra l'altro viene accordato con un semplice click.

Viceversa, il rifiuto può determinare l'impossibilità dell'accesso e, anche laddove non sia così, accettare solo alcune condizioni della informtiva richiede tempo e sforzo, due limiti che mal si sposano con la celerità e la semplicità della realtà digitale.

Sebbene la protezione dei dati costituisca uno dei due poli su cui ruota il Gdpr, appare sacrificabile ad una maggiore legittimazione del mercato degli stessi.

A conferma di siffatta lettura è intervenuta anche la giurisprudenza nostrana, la quale in una recente pronuncia (TAR Lazio, 10 gennaio 2020, n. 260) dichiara che la raccolta e lo sfruttamento dei dati degli utenti a fini remunerativi si configurano come controprestazione del servizio offerto dal social network, perché dotati di valore commerciale. Ed infatti si legge nella motivazione

della sentenza che sebbene si ritenga che: "… l'unica tutela del dato personale sia quella rinvenibile nella sua accezione di diritto fondamentale dell'individuo, … tuttavia, tale approccio sconta una visione parziale delle potenzialità insite nello sfruttamento dei dati personali, che possono altresì costituire un "asset" disponibile in senso negoziale, suscettibile di sfruttamento economico e, quindi, idoneo ad assurgere alla funzione di controprestazione in senso tecnico di un contratto. A fronte della tutela del dato personale quale espressione di un diritto della personalità dell'individuo, e come tale soggetto a specifiche e non rinunciabili forme di protezione, quali il diritto di revoca del consenso, di accesso, rettifica, oblio, sussiste pure un diverso campo di protezione del dato stesso, inteso quale possibile oggetto di una compravendita, posta in essere sia tra gli operatori del mercato che tra questi e i soggetti interessati".

I dati personali, dunque, rientrano a pieno titolo in un'area di mercato e di necessità occorre abbandonare l'ottica che li considera esclusivamente nel contesto dei diritti assoluti, proprio allo scopo di offrirgli il più ampio ventaglio di tutele possibili.

Va osservato che la loro modalità di circolazione rappresenta ancora un terreno parzialmente esplorato, rispetto al quale occorre abbandonare soluzioni ancorate a preconcetti schematismi ed affidarsi ad una prospettiva ricostruttiva ancora tutta in divenire.

Certamente il regolamento UE 2016/679 costituisce il primo passo.

Il regolamento ha consolidato il quadro dei diritti in materia con l'introduzione di nuove facoltà come la portabilità dei dati, il diritto di opposizione e il diritto all'oblio.

L'individuazione del principio dell'accountability è poi un passo particolarmente significativo nella politica di data protection dell'Unione.

Il termine accountability può essere tradotto con responsabilità e, insieme, prova della responsabilità. Esso è correlato da un obbligo di rendicontazione e consiste nella necessità di conformarsi a certe previsioni e poterne dare prova tangibile.

L'accountability si esprime su due livelli: un primo livello obbligatorio e un secondo volontario. Il primo comprende due elementi: l'attuazione di misure e/o procedure di protezione e la conservazione delle relative prove. Questo primo livello può essere integrato da disposizioni specifiche.

Il secondo livello include invece sistemi di responsabilità di natura volontaria eccedenti le norme di legge minime, in relazione ai principi fondamentali di protezione dei dati (tali da fornire garanzie più elevate di quelle prescritte nel Gdpr) e/o in termini di modalità di attuazione o di garanzia dell'efficacia delle misure.

Evidentemente l'accountability assume caratteristiche differenti nei due diversi casi.

Nel primo consiste nell'obbligo di attuare alcune specifiche misure di sicurezza e di formalizzare le procedure accolte.

Nel secondo caso si traduce nella facoltà di adottare misure di protezione dei dati personali ulteriori rispetto a quelle previste dalla normativa vigente.

Lo scopo è promuovere l'utilizzo di sistemi che concretamente mettano in pratica i principi generali della protezione dei dati.

Il titolare del trattamento è infatti tenuto a garantire l'efficacia delle misure adottate e a dimostrare, su richiesta, di aver intrapreso tali azioni. Ma la sua responsabilità non si esaurisce con la valutazione e l'adozione delle suddette. È necessaria, altresì, un'attività di continuo monitoraggio, per verificare che siano proporzionate e adeguate ai rischi in continuo mutamento. Si tratta di una tutela della privacy in una visione preventiva quindi, la c.d. "privacy by default", che si declina poi in una complessa attività di valutazione (tecnica, giuridica e organizzativa), un'analisi dei rischi e dei costi, una scelta sulle misure di sicurezza da adottare, l'istituzione di un presidio, l'emanazione di una policy interna e per finire di un'attività di monitoraggio continuo ("privacy by design").

Certamente, una più solida protezione dei dati sarebbe stata possibile con regole *ad hoc*, che implicassero un ribaltamento dell'ottica prospettica: consentire l'accesso al digitale senza accettazione al trattamento dei dati, fuorchè in determinati e sporadici casi attraverso un consenso necessariamente ed esplicitamente richiesto.

Questa opzione è tuttavia di difficile attuazione e ne è intuibile la ragione.

Resta il fatto che probabilmente una regolamentazione più attenta e severa in tema di trattamento dei dati e ancora prima di consenso al trattamento è indispensabile per evitare un eccessivo sbilanciamento tra mercato e persona, tutto a vantaggio del primo, ad eccessivo discapito della seconda.