Il trade-off sullo stato di attuazione del Gdpr in Italia e le prospettive dei temi strategici legati alla dominanza digitale

Author : Sergio Guida

Date : 28 Giugno 2019

L'accountability è prima di tutto volta alla ricerca del corretto bilanciamento tra diritti, libertà e altri beni giuridici primari, che si inviluppano un una dialettica continua e richiedono l'applicazione del principio di proporzionalità.
Lo testimoniano le esperienze di questi ultimi anni che rendono sempre più urgente affrontare temi quali la democrazia nella società digitale e gli effetti distorsivi della profilazione e del nudging*, sia sul piano commerciale che su quelli delle relazioni sociali e pubbliche.*

Il nostro Garante nazionale persegue l'obiettivo di rispondere alle sfide poste dai nuovi modelli economici fondati in maniera sempre più invasiva sullo sfruttamento dei dati e, specularmente, alle accresciute esigenze di tutela dei diritti fondamentali delle persone, onde assicurare **un'adeguata protezione dei loro dati**.

D'altronde, il 2018 ha rappresentato una tappa di grande importanza con l'entrata nella sua piena applicazione del **GDPR** che ha irrobustito la tutela dei diritti per gli individui (*natural person*) e dilatato le responsabilità per i soggetti che trattino i dati.

Come emerge dalla Relazione sull'attività recentemente pubblicata, gli interventi sono stati polarizzati sulle rilevanti novità normative e sulle grandi questioni legate alla tutela dei diritti e delle libertà delle persone nel mondo digitale: si pensi ad es. alle **implicazioni etiche** della tecnologia alle grandi piattaforme; ai *big data*; agli algoritmi ad uso sociale; alla pervasività nella raccolta dei dati, nella *profilazione* online, talvolta anche pensando alle possibilità di orientare la pubblica opinione; alla *cybersecurity*; all'Internet delle cose.

Proprio nel 2018 si sono verificati **fatti clamorosi** che hanno messo a rischio la sicurezza informatica di milioni di persone in tutto il mondo, tanto che sotto il profilo dei possibili utilizzi illeciti dei dati personali sulle piattaforme *social*, sono emersi due casi paradigmatici: il primo è stato il caso *Cambridge Analytica*, sul quale l'Autorità è intervenuta non solo per accertare le responsabilità ma soprattutto per aumentare la consapevolezza sui rischi che forme distorte di influenza possono rappresentare per la libertà delle persone. Nel secondo, a *Facebook* il

Garante ha vietato l'ulteriore trattamento dei dati degli utenti italiani, riservandosi di valutare l'iter verso un eventuale procedimento sanzionatorio.

In tema di **tutele per i minori** per le attività online, il lavoro si è concentrato sui possibili rischi insiti negli *smart toys* e, per combattere il fenomeno del *cyberbullismo,* il Garante ha potuto, alla luce dei nuovi compiti, prescrivere misure e procedure per la rimozione dei contenuti offensivi, siglando inoltre un protocollo di intesa con la Polizia postale e con alcuni Co.Re.Com. onde realizzare una vera e propria rete per la protezione delle giovani vittime che possa effettivamente agire in maniera coordinata e tempestiva.

Non sono mancate indicazioni sull'uso dei **droni** a scopo ricreativo e su come difendersi dai software dannosi, in particolare dal *ransomware*, software malevoli diffusi per bloccare un dispositivo elettronico (pc, tablet, smartphone, smart tv), o criptare i dati in esso contenuti (foto, video, file) allo scopo di ottenere un riscatto per sbloccarlo.

Nel mondo del **lavoro** sono state indicate le garanzie per la raccolta delle impronte digitali per i dipendenti pubblici a fini di lotta all'assenteismo; fissate regole per la *geolocalizzazione* dei lavoratori e vietati i controlli massivi su email e smartphone dei dipendenti, così come prassi di valutazione lesive della dignità del lavoratore.

Sul fronte ***cybersecurity**,* l'attività di vigilanza e intervento è stata molto intensa, procedendo d'ufficio o a seguito di specifiche segnalazioni relative a violazioni di dati personali (*data breach*), alcune gravi; fornendo prescrizioni dettagliate per la messa in sicurezza di una piattaforma di partecipazione politica; rafforzando la cooperazione con l'*intelligence* in ordine ai trattamenti di dati per fini di sicurezza nazionale e alle garanzie da assicurare ai cittadini; prescrivendo i criteri per l'esercizio del diritto all'oblio e per la sua tutela al di là dei confini UE.

Sulle delicate questioni di **trasparenza** online della P.A., le amministrazioni sono state richiamate a rispettare canoni di proporzionalità e di scrupoloso bilanciamento fra obblighi di pubblicità degli atti e dignità delle persone. Inoltre è stata bloccata la diffusione online, su siti di amministrazioni pubbliche, di dati sensibili delle persone; sono state fissate precise regole per l'esercizio del diritto di accesso civico; sono state chieste garanzie riguardo al nuovo censimento permanente, che prevede l'integrazione di banche dati e l'uso massivo dei dati dell'intera popolazione; sono state intraprese azioni per aumentare il livello di sicurezza della P.A. digitale e per rafforzare le garanzie per i cittadini nell'attuazione dello *Spid*.

Per quanto riguarda il **sistema fiscale**, il Garante ha individuato i presupposti e le condizioni necessari affinchè l'Agenzia delle entrate avviasse il nuovo obbligo della fatturazione elettronica, in particolare sulle tutele per evitare trattamenti sproporzionati dei dati personali dei contribuenti; ha prescritto misure tecniche relative all'accesso alla dichiarazione dei redditi precompilata da parte di contribuenti, Caf e soggetti autorizzati, nonchè alla messa in sicurezza delle grandi banche dati pubbliche, *in primis* quella dell'Anagrafe tributaria.

Per la tutela dei **consumatori** sono state dettate regole per il trattamento dei dati effettuato attraverso i totem pubblicitari nelle stazioni ferroviarie, proseguendo il contrasto al ***telemarketing* aggressivo** con l'applicazione di pesanti sanzioni agli operatori che utilizzano i

dati degli abbonati senza il loro consenso; accertando rilevanti illeciti da parte di società di telefonia; svolgendo ispezioni presso diversi call center e suggerendo l'opportunità di modifiche normative per rafforzare le garanzie dei cittadini.

Naturalmente è stata costante l'azione di supporto a imprese e pubbliche amministrazioni e di formazione in vista della definitiva applicazione del GDPR.

Nel periodo 2012-2018 sono state riscosse **sanzioni** per l'importo complessivo di 31.322.754 Euro.
Nel solo 2018 sono stati adottati 517 provvedimenti collegiali.

Sono stati riscontrati oltre 5.600 quesiti, reclami e segnalazioni in diversi settori: marketing telefonico e cartaceo; centrali rischi; credito al consumo; videosorveglianza; concessionari di pubblico servizio; recupero crediti; settore bancario e finanziario; assicurazioni; lavoro; enti locali; sanità e servizi di assistenza sociale.

I 130 ricorsi, decisi fino all'applicazione del Regolamento UE, hanno riguardato soprattutto editori; datori di lavoro pubblici e privati; banche e società finanziarie; P.A. e concessionari di pubblici servizi; fornitori telefonici e telematici.

Sono stati resi 28 pareri al Governo e al Parlamento (di cui 5 su norme di rango primario) e hanno riguardato, *inter alia*, l'attività di polizia e sicurezza nazionale; il casellario giudiziale; i trattamenti di dati a fini di polizia; le misure antiassenteismo e la raccolta delle impronte digitali dei dipendenti pubblici; il Programma statistico nazionale; il "bonus cultura"; il Fascicolo sanitario elettronico; la carta di identità elettronica; il Registro tumori; l'Archivio dei rapporti finanziari; l'Anagrafe nazionale dei vaccini; il fisco.

Le comunicazioni di **notizie di reato** all'autorità giudiziaria sono state 27, in particolare per mancata adozione di misure minime di sicurezza a protezione dei dati e illecito controllo a distanza dei lavoratori.

Sono state contestate 707 violazioni amministrative, quasi tutte per trattamento illecito di dati; mancata adozione di misure di sicurezza; violazioni di banche dati; omessa o inadeguata informativa agli utenti sul trattamento dei loro dati personali; omessa esibizione di documenti, mentre sono state riscosse sanzioni amministrative per oltre 8 milioni 160 mila euro (+115% in più rispetto al 2017).

Le 150 ispezioni, effettuate anche con il contributo del Nucleo speciale tutela privacy e frodi tecnologiche, hanno riguardato numerosi e delicati settori:

- *nell'ambito privato*: trattamenti effettuati da istituti di credito; da società per attività di *rating* sul rischio e sulla solvibilità delle imprese; dalle aziende sanitarie locali e poi trasferiti a terzi per il loro utilizzo a fini di ricerca; da società che svolgono attività di telemarketing; da società di "money transfer". Particolare attenzione è stata rivolta ai trattamenti di dati svolti da società assicuratrici attraverso l'installazione di *"scatole nere*" a bordo degli autoveicoli e da società che offrono servizi medico-sanitari tramite

app;
- *nel settore pubblico*: enti pubblici, soprattutto Comuni e Regioni, che svolgono trattamenti di dati personali mediante app per smartphone e tablet (con particolare attenzione all'eventuale profilazione e geolocalizzazione degli utenti); sulle grandi banche dati; sul sistema della fiscalità, con speciale riguardo alle misure di sicurezza e al sistema degli *audit*; sul sistema informativo dell'Istat e sullo *Spid*.

Per quanto riguarda l'attività di relazione con il pubblico, sono stati riscontrati quasi 23.000 quesiti, relativi agli adempimenti legati all'applicazione del Regolamento Ue, seguiti dalle questioni legate alle telefonate, mail, fax e sms promozionali indesiderati; a Internet; alla videosorveglianza; al rapporto di lavoro; ai dati bancari.

A livello internazionale, la nostra Authority ha svolto un ruolo rilevante nel contesto che a livello Ue è stato caratterizzato soprattutto dalla definitiva applicazione del nuovo Regolamento in materia di protezione dei dati (GDPR), il 25 maggio 2018.

Con esso l'Advisory Board, che riuniva le Autorità dei 28 Paesi Ue, è stato sostituito dal "*Comitato europeo per la protezione dei dati*", che ha acquisito un ruolo non solo consultivo, ma anche decisionale e il Garante italiano ha continuato a fornire i propri contributi riguardo all'elaborazione di importanti *Linee guida* sull'interpretazione e l'applicazione delle disposizioni del GDPR, tra le quali quelle sul consenso; sulla trasparenza; sui registri dei trattamenti; sulla profilazione e le decisioni automatizzate; sull'adeguatezza del Paese terzo in caso di trasferimenti di dati extra Ue; sui *data breach*.

La nostra Authority partecipa ai meccanismi di cooperazione (**"sportello unico"**) e coerenza previsti dal Regolamento, attraverso scambi quotidiani di informazioni e documentazione: in particolare, dal 25 maggio 2018, è operativa la sezione GDPR della **Piattaforma IMI** *(Internal Market Information System),* utilizzata da tutte le autorità di controllo per garantire una coerente tutela dei dati personali all'interno dell'Unione europea. Inoltre, del 24-25 settembre 2018 il *Comitato europeo per la protezione dei dati* ha assegnato all'IMI *help desk* una funzione non solo di supporto tecnico ma anche di complessivo monitoraggio del sistema.

Così, attraverso IMI, le autorità possono ora contare su uno strumento trasparente, flessibile e sicuro per diverse finalità, quali ad esempio identificare l'autorità capofila nel caso di trattamenti transfrontalieri per poi contribuire all'elaborazione di un progetto di decisione condiviso fra l'autorità capofila e le autorità interessate (cd. *meccanismo dello sportello unico* o *one stop shop*) oppure assicurare assistenza reciproca attraverso lo scambio di informazioni o condurre indagini e misure di contrasto congiunte.

Infine, allo scopo di favorire un'**applicazione coerente del GDPR** in tutta l'Unione, la piattaforma verrà utilizzata per consentire alle autorità di controllo di consultare il *Comitato europeo per la protezione dei dati* al fine di raccoglierne un parere, ad esempio per questioni di applicazione generale o che producono effetti in più di un Paese membro oppure per ottenere una decisione vincolante del Comitato che componga eventuali conflitti fra le stesse autorità di controllo.

Il Garante ha continuato la collaborazione con le altre Authority europee in ordine all'istituzione di meccanismi per la certificazione della protezione dei dati personali. I lavori hanno riguardato in particolare la stesura dei documenti concernenti, rispettivamente, l'identificazione di criteri comuni per accreditare gli organismi di certificazione e i requisiti aggiuntivi per l'accreditamento, ai sensi dell'art. 43, par. 1, lett. *b*), del GDPR, e quelli aventi ad oggetto l'identificazione di criteri comuni per la certificazione dei trattamenti, che hanno portato all'elaborazione delle *Guidelines 4/2018* e *1/2018.* Il decreto legislativo n. 101/2018 ha poi individuato in Accredia l'*organismo nazionale di accreditamento deputato all'accreditamento degli organismi di certificazione*.

Altre rilevanti **attività sovranazionali** del Garante italiano sono state espletate per il Consiglio d'Europa, che - attraverso il Comitato presieduto da una rappresentante del Garante italiano - ha portato a termine i lavori tesi alla "modernizzazione" della Convenzione 108 del 1981 sulla protezione dei dati, nonché nell'ambito di gruppi internazionali (quali la *Global Privacy Enforcement Network, GPEN*) preposti a interventi congiunti e mirati di verifica del rispetto della normativa in materia di protezione dei dati.

Looking ahead, dal cospicuo "bilancio" presentato si può trarre la misura di come la nostra Autorità Garante rappresenti ormai il fulcro al centro del *framework* teso alla modernizzazione del Paese attraverso il potenziamento delle sue infrastrutture digitali, affinché possa effettivamente aver luogo nel rispetto dei diritti individuali e delle libertà fondamentali dei cittadini.

Articolo a cura di **Sergio Guida**