IL GARANTE PRIVACY DEL FUTURO: IDEE PER IL PROSSIMO COLLEGIO 2019-2026

Le proposte dell'Istituto Italiano per la Privacy e la Valorizzazione dei Dati

Roma, 1 aprile 2019

L'imminente rinnovo del Collegio del Garante per la Protezione dei Dati Personali (o Garante Privacy, come chiamato da molti informalmente) ci offre l'opportunità per ragionare sul futuro di questa cruciale Autorità, i cui compiti sono essenziali per assicurare libertà e diritti fondamentali agli individui nell'era digitale. **A cavallo tra primavera ed estate del 2019, infatti, scadrà il termine per l'elezione dei nuovi componenti del Collegio del Garante**.

Dall'osservatorio dell'**Istituto Italiano per la Privacy e la Valorizzazione dei Dati**, esterno ma, da ormai tanti anni, in stretto e costante contatto scientifico e professionale con tutta la comunità, istituzionale e non, che si occupa di questa materia, possiamo affermare che il Collegio uscente ha guidato l'Autorità con saggezza, in un periodo storico irripetibile e di difficile transizione (con l'avvento del Regolamento 2016/679/UE - GDPR, *in primis*). Abbiamo constatato la capacità di ascolto degli *stakeholder*, il bilanciamento degli interessi come missione, l'attenzione impeccabile alla **tutela dei più deboli**, dei singoli e "piccoli" esseri umani alle prese con violazioni e abusi privacy più o meno gravi perpetrati da imprese ma anche da enti pubblici. Un approccio, uno stile e un tono fermi e, tuttavia, mai autoritari, tecnicistici o "professorali" nei confronti dei Titolari e dei Responsabili del trattamento di dati, sempre aperto all'ascolto e al confronto. Queste sono **virtù da riconoscere al settennato che va a concludersi nel 2019**, che porteremo con noi come un buon ricordo. Senza contare la conferma del fatto che i Dirigenti e i Funzionari dell'Ufficio del Garante erano, sono e resteranno straordinariamente competenti, fini sul piano giuridico, attenti al minimo particolare nelle loro delicatissime attività istruttorie. Un faro, per gli operatori del diritto dei dati, che ci conforta anche in termini di **costanza giurisprudenziale**.

Nel mentre, **il GDPR ha rafforzato enormemente i poteri e i compiti delle Autorità di controllo privacy nei vari Stati**. Il legislatore italiano, con il D.Lgs. 101/2018, ha a sua volta modificato il Codice incrementando ulteriormente, a livello nazionale, il perimetro di poteri, competenze e compiti riconosciuti al **Garante, che ormai può dirsi emancipato dal ruolo di mero "supervisore" e trasformato in vero e proprio regolatore generale ed astratto *ex ante***. I poteri sanzionatori e di intervento *ex post* sono poi, come noto, estremamente estesi e incisivi, tanto da avere effetti dissuasivi e preventivi anche nei confronti di grandi colossi digitali e non. Intanto, qualcuno dice che i dati personali siano divenuti il nuovo petrolio; da anni questo è un luogo comune da cui, peraltro, dissentiamo come dissentono in tanti: il petrolio ha valore soprattutto in virtù della sua scarsità, mentre i dati sono ovunque e ce ne saranno sempre di più. **Ci convince maggiormente un'altra suggestiva metafora: che i dati personali siano il "quinto elemento"** del mondo in cui l'essere umano esiste e vive, dopo terra, aria, fuoco e acqua. Ecco, per il futuro settennato 2019-2026 sarebbe forse necessario pensare a un Garante del "quinto elemento".

Il futuro, dicevamo. **Cosa ci aspettiamo dal nuovo Collegio 2019-2026? Di che cosa avrebbe bisogno il Garante Privacy, nei prossimi sette anni – che sono un'era lunghissima – per essere ancora più utile e forte**? In pochi punti, non esaustivi e che rappresentano solo un "là" per il confronto, ecco qualche nostra idea e suggestione, qualcosa che a nostro parere servirebbe davvero. L'ordine delle idee non ne indica necessariamente il grado di priorità.

Le proposte per il settennato 2019-2026 del Garante per la Protezione dei Dati Personali:

1. **Cooperazione stretta con le altre Autorità, ma non fusione**

   In questi mesi, in Italia, si è svolto un vivace dibattito sulla stampa, a proposito di idee di **fusione tra Garante Privacy e Autorità per le Garanzie nelle Comunicazioni** (AgCom), in quanto autorità indipendenti accomunate da materie "limitrofe", come quelle riguardanti l'abuso e la protezione dei dati e delle informazioni degli utenti *on line*. Abbiamo inoltre assistito a un progressivo e obiettivo avvicinamento

dell'Autorità Garante della Concorrenza e del Mercato (Agcm) su terreni che sono, fisiologicamente, anche di competenza del Garante Privacy (per l'abuso commerciale e concorrenziale dei dati personali dei consumatori). Ragionando per "fusioni successive", in virtù della prossimità di campo, si dovrebbe auspicare, appunto, perfino un'unione di Garante Privacy e AgCom con AGCM: ma non si finirebbe più di fondere, per arrivare a una "*reductio ad unum*" di sapore omeopatico. È vero che si potrebbero mantenere Dipartimenti separati all'interno di un'unica maxi-Autorità, ma il Collegio sarebbe comunque uno solo. Senza contare che il Garante Privacy mira a proteggere valori, diritti e libertà fondamentali e inviolabili degli individui, ben distinti da quelli oggetto di tutele da parte delle "Autorità cugine". Anche il peso nei confronti delle grandi piattaforme globali non basta come argomento a favore della fusione: esso può ben derivare dall'entità delle sanzioni e dei poteri di limitazione o inibitori, quand'anche esercitati da più Autorità separatamente. In tal senso, crediamo che un più intenso coordinamento tra le varie Autorità sarebbe senz'altro necessario ed opportuno, anche **senza procedere a fusioni, prevedendo invece per legge l'integrazione eventuale dei procedimenti e alcune forme di "cooperazione rafforzata" in tutti i casi necessari**;

2. **Internazionalità**

   È banale, ma abbiamo bisogno di **componenti del Collegio che conoscano le lingue** e si muovano agevolmente nell'arena naturale, senza confini geografici nel confronto sulla materia, che è discussa **su scala globale** e che è regolamentata, ora più che mai, almeno a livello europeo. Occorre una **robusta capacità di comprendere la dimensione internazionale**, europea e mondiale, e di affrontarla direttamente con competenze (intese proprio come "*skill*" personali dei componenti del Collegio). È essenziale che i 4 nuovi componenti del Collegio possano muoversi con sicurezza di sé, nell'elaborare e portare posizioni e proposte al tavolo del Comitato Europeo della Protezione dei Dati e agli altri tavoli internazionali di cooperazione e dialogo tra autorità, istituzioni, *stakeholder*. **Non basta avere personale tecnico da delegare, per quanto bravo**: spesso è fondamentale che la "partita di tennis" sia giocata in diretta

dal vertice, per far pesare e passare idee innovative e non scontate. Funziona così al Consiglio della UE, e funzionerà sempre di più in questo modo anche nel Comitato Europeo della Protezione dei Dati e in altre sedi analoghe, o nel confronto con le grandi aziende multinazionali;

3. **Competenza e professionalità**

   I componenti del Collegio non siano solo dei politici o degli 'appassionati' di innovazione. **Occorrono veri esperti, professionisti e studiosi apprezzati dalla comunità accademica, forense, scientifica**. Non basta avere letto libri sull'Intelligenza Artificiale o sui *Big Data* o sull'Internet delle Cose o sulle *smart city*: un buon componente del Collegio, almeno come lo immaginiamo noi, dovrebbe avere sperimentato direttamente questo genere di progetti e di sviluppi, nella ricerca, nella professione e nell'impresa. Diversamente, non sarà in grado di comprendere il senso reale e profondo di princìpi – molto predicati, poco praticati – quali la *data protection-by-design* e la *data protection-by-default*, e non sarà abile nel discernere il mero formalismo dalla sostanza delle tutele;

4. **Aperti al mercato e al progresso tecnologico**

   Da quanto indicato sopra, discende il fatto che i nuovi componenti non dovrebbero essere teorici assertori di principi svincolati dalla realtà, quanto piuttosto **figure aggiornate alle tendenze globali del mercato e dell'innovazione tecnologica**, per calare appieno i principi di proporzionalità e ragionevolezza nell'applicazione concreta del diritto dei dati personali: questo significa avere competenza ed esperienza in materia di nuovi diritti digitali e, a monte, in materia di mercati digitali. Presenti e futuri. Come si può pensare ad **un Garante che protegga i diritti delle persone, nel rispetto della libertà di iniziativa economica, della libertà di espressione, dell'innovazione e della ricerca scientifica**, se non conosce a fondo come funziona il mercato e dove porta l'inarrestabile cammino dell'uomo verso la conoscenza e lo sviluppo tecnologico? Ignorare o negare la realtà corrente, nel nome del diritto formale ed astratto, non potrebbe rafforzare le tutele concrete;

5. **Un'azione trasparente**

   Indipendenza ma non chiusura. L'apertura al dialogo e la trasparenza dovrebbero trovarsi nel DNA del Garante Privacy. Anche in assenza di una norma di legge che preveda **obblighi di riscontro agli interpelli preventivi, formulati al di fuori di un procedimento**, sarebbe opportuna l'adozione di un Regolamento interno che prevedesse un'equivalente procedura: potenziando l'URP dell'Autorità, ma anche responsabilizzando periodicamente l'Ufficio nella risposta a quesiti frequenti, per iscritto, pubblicando gli orientamenti – un po' come accade con le circolari interpretative e con le risposte scritte a quesiti da parte dell'Agenzia delle Entrate. Le imprese e gli enti hanno fame e sete di orientamento, e il ruolo degli avvocati e della dottrina non può bastare. **Più risposte saranno date prima, con possibilità di legittimo affidamento da parte di Titolari e Responsabili, meno procedimenti sanzionatori ci potranno essere poi**;

6. **Maggiore comprensibilità e certezza del diritto**

   Chiarezza "a prova di stupido" nelle linee guida e nei provvedimenti generali. Il GDPR e la restante normativa privacy nazionale sono spesso vaghi, intrisi di princìpi generali, causano incertezza del diritto negli operatori istituzionali e di mercato. Il problema è che non si scherza con le conseguenze di un inadempimento, che possono essere gravissime per le imprese, gli enti e le persone che ci lavorano. Alla violazione di alcuni provvedimenti del Garante, dallo scorso 19 settembre 2018, sono perfino ricondotte fattispecie penali (artt. 167 e 170 del Codice Privacy). Questo dovrebbe portare l'Autorità a **esemplificare il più possibile, a non dare per scontato nulla, a dettagliare ogni "millimetro" di quanto atteso in termini di conformità da parte di Titolari e Responsabili del trattamento di dati**. La vaghezza, di leopardiana memoria, affascina il giurista, ma è veleno di incertezza per chi deve applicare le regole e valutare i rischi;

7. **Canali di contatto e reclamo per bambini**

   Con la legge 71/2017, il Garante è stato investito di importanti poteri d'intervento per il contrasto al **cyberbullismo**. È però indispensabile che l'Autorità dedichi **un'intera sezione del suo portale proprio ai minori** – ai quali si riferisce la normativa anti-cyberbullismo – con contenuti chiari, coinvolgenti e comprensibili. Allo stesso modo, sarà necessario investire in campagne educative e di orientamento destinate ai bambini, anche in collaborazione con il MIUR, per accrescere le competenze di autodifesa e di prudenza nell'uso delle tecnologie dell'informazione da parte degli studenti.

   Serve un "**Garante a colori**" per i bambini, che si ponga come sportello amico e consultorio per le vittime di cyberbullismo (ma anche per i cyberbulli) e di altri abusi privacy, perpetrati spesso anche da adulti, con un volto adatto ai più giovani. Un Garante che si doti anche di un servizio di sostegno psicologico, per accompagnare al meglio le vittime nel corso dei procedimenti, al di là del "freddo" e per certi versi inevitabile approccio giuridico e tecnico nella gestione dei reclami;

8. **Sanzioni destinate a un fondo per le vittime**

   Paradossalmente, **il Garante "rischia" di diventare inutilmente ricco nei prossimi anni**. Infatti, le sanzioni previste a norma dell'art. 166 del Codice Privacy e dell'art. 83 del GDPR (fino a 10 milioni o 20 milioni di euro o, nel caso di imprese, fino al 2% o al 4% del fatturato mondiale totale dell'anno precedente, se superiore) dovrebbero entrare per il 50% nelle casse dell'Autorità: tuttavia, il Garante potrebbe non sapere che farsene. L'organico dell'Autorità è fissato *ex lege* in 162 unità, come previsto dall'attuale formulazione dell'art. 152 del Codice. Anche avesse in cassa 100 milioni di euro – cifra stellare ma non fantascientifica, vista la "potenza di fuoco" sanzionatoria riconosciutagli dal GDPR – il Garante non potrebbe assumere altri dipendenti, senza prima far modificare la legge. Cosa fattibile e certamente auspicabile, anno dopo anno, vista la rilevanza di questa materia e il numero di reclami (in fase di vera e propria esplosione già nel primo anno di vigenza del Regolamento UE) ma anche, chiaramente, ben poco elastica ed efficiente. Un'opzione sarà l'affidamento di parte delle attività,

per sostenere la mole di procedimenti, a consulenti esperti esterni, con tutte le connesse problematiche, però, in termini di potenziali conflitti di interessi. L'alternativa sarebbe forse **trasformare questa Autorità in un ente di investimento e gestione immobiliare, per non disperdere l'enorme tesoro via via accumulato attraverso le nuove sanzioni?** Avrebbe senso e sarebbe etico per un'autorità pubblica? Naturalmente no. Dunque, ciò che si propone per ovviare, almeno in parte, a questo paradosso è che l'Autorità istituisca – se del caso anche grazie ad una piccola modifica legislativa *una tantum* – **un fondo per le vittime di violazioni e abusi privacy**, tramite il quale prevedere indennizzi in tutti i casi nei quali si riconosca, a valle di un reclamo o d'ufficio, che una violazione impattante sui diritti degli interessati si è effettivamente verificata. Stiamo o non stiamo parlando di diritti fondamentali e inviolabili degli individui? Se sì, l'istituzione di un fondo per le vittime è la strada giusta;

9. **Niente multe per chi notifica le violazioni**

Il GDPR consente un importante margine di manovra alle singole Autorità, nel commisurare le sanzioni amministrative pecuniarie. Tra gli elementi che possono essere valutati, a norma del paragrafo 2 lettera h) dell'art. 83 GDPR, vi è "*la maniera in cui l'autorità di controllo ha preso conoscenza della violazione, in particolare se e in che misura il titolare del trattamento o il responsabile del trattamento ha notificato la violazione*". Ebbene, con proprio regolamento, il Garante italiano potrebbe applicare una regola: **per le prime notifiche operate dai Titolari del trattamento, con riferimento a violazioni dei dati che si verificano per la prima volta, dovrebbero escludersi sanzioni amministrative pecuniarie** o limitarsi l'importo alla mera copertura dei costi vivi del procedimento;

10. ***Advisory Board***

Istituzione di **un comitato scientifico o *advisory board***, come già previsto dalla regolamentazione interna del Garante. Poteva essere fatto in passato, non è stato fatto. Ma sarebbe servito e quella previsione regolamentare era anzi intelligente: proprio per restare al passo coi tempi, per diventare sempre più bravi e "sul pezzo" dell'evoluzione

galoppante degli scenari tecnologici, economici e giuridici, **dotarsi di una "*sounding board*" qualificatissima, non solo italiana ma a composizione internazionale, sarebbe una scelta illuminata**. Non vi sarebbe pericolo di sovrapposizione di poteri: il Collegio avrebbe e manterrebbe tutto il potere decisionale, semplicemente si ritroverebbe meglio orientato, otterrebbe punti di vista d'avanguardia, qualche volta dovrebbe tollerare – in stile anglosassone, ma non morirebbe nessuno – delle posizioni pubbliche di cosiddetto "*Not In My name*" da parte di uno dei membri del comitato scientifico, ma bene così, il confronto intellettuale fortifica e genera fiducia, non ha senso temerlo;

11. Un Garante digitale

Occorre interpretare il proprio ruolo come **Garante della libertà degli esseri umani nell'era digitale**. Un ruolo meta-costituzionale, sovraordinato all'ordinario esercizio dei poteri amministrativi e di derivazione sovranazionale, direttamente previsto da GDPR e Trattati UE. In grado di assicurare la difesa del cittadino, del contribuente, del consumatore, di tutti noi dai possibili abusi e soprusi causati e imposti (impersonalmente, automaticamente, silenziosamente) da regole informatiche che avranno progressivamente più peso delle norme di legge. In ogni caso, oggi e domani ancora di più, occuparsi di tutela dei diritti alla protezione dei dati personali e alla riservatezza significa **occuparsi di algoritmi, decisioni automatizzate, Intelligenza Artificiale e sostituzione/integrazione del pensiero umano**. La commistione tra fisico e virtuale – trattamenti di dati che generano effetti materiali, fisici, da un lato, e fenomeni fisici che generano dati, dall'altro – trasformerà la protezione dei dati personali in "**protezione degli effetti personali**". Nel 2026 questo sarà pane quotidiano per l'Autorità, probabilmente ben prima. La consapevolezza e l'esercizio attivo di questo ruolo saranno determinanti per il valore e l'efficacia dell'azione del nuovo Collegio.

ISTITUTO ITALIANO
PER LA PRIVACY E LA
VALORIZZAZIONE DEI DATI

Le proposte che abbiamo messo in fila, in questo sintetico documento, vogliono servire ad **avviare un dibattito costruttivo, anche e soprattutto in Parlamento nella primavera del 2019,** quando la Camera dei Deputati e il Senato della Repubblica saranno chiamati a valutare le candidature per eleggere, rispettivamente, 2 componenti del Collegio del Garante Privacy. Lo speriamo. **Solo attraverso un vero confronto pubblico, che induca alla dialettica e alla condivisione delle idee, potremo contare su future istituzioni veramente aperte, responsabili, trasparenti ed equilibrate.**

Luca Bolognini
Presidente dell'Istituto Italiano per la Privacy e la Valorizzazione dei Dati
l.bolognini@istitutoprivacy.it

Roma, 1 aprile 2019