Anno 6, n. 11 – LUGLIO 2018
Nuova Etica Pubblica
Rivista dell'Associazione Etica PA

Intervista a Antonello Soro- Presidente del Garante per la protezione dei dati personali

a cura di Vanna Palumbo

Caro Presidente, dal 25 maggio scorso è diventato di piena e diretta applicazione il Regolamento generale sulla protezione dei dati dell'UE (n. 679 del 2016). Cosa cambia per le pubbliche amministrazioni?

Il nuovo Regolamento Europeo, assieme alla direttiva 680 sui trattamenti per fini di polizia e giustizia penale, rappresenta la cornice normativa in cui si giocherà una delle sfide più importanti per i prossimi decenni: quella dell'effettività del diritto fondamentale alla protezione dei dati personali. Questo diritto costituisce ormai una garanzia ineludibile di libertà nella società digitale, in cui si dispiega sempre più la nostra esistenza privata e pubblica.

L'esigenza che ha portato alla revisione delle regole in questa materia, è stata proprio quella di adeguare il diritto a questa nuova realtà in continua evoluzione, perché esposta agli incessanti mutamenti delle nuove tecnologie. Il nuovo quadro giuridico europeo segna quindi, in questo percorso, un momento essenziale: innanzitutto con la scelta della forma regolamentare che, da un lato, fornisce agli Stati membri una disciplina unitaria, volta a superare le asimmetrie riscontrate nel recepimento della direttiva 95/46/Ce; dall'altro, assicura agli individui un livello di tutela omogeneo - fondato sul primato della persona e sul ruolo di garanzia di Autorità indipendenti. Tale approccio di fondo, cui si ispira la nuova disciplina, potrà costituire un modello verso il quale anche gli altri ordinamenti potranno via via convergere, stimolati dall'applicabilità delle regole europee anche a trattamenti svolti al di fuori dei confini dell'Unione, ma che hanno un impatto significativo per gli individui europei, indipendentemente dalla loro nazionalità o residenza. E', insomma, il primo passo verso il riconoscimento universale del diritto alla protezione dati, quale diritto fondamentale dell'uomo.

Tale diritto, però, non costituisce una prerogativa assoluta, ma, nella sua funzione sociale, come recitano i primi considerando del regolamento, va contemperato con altri diritti fondamentali, in linea con il principio di proporzionalità. Nel bilanciamento dovranno necessariamente essere presi in considerazione altri beni giuridici primari, specie nel settore pubblico: la sicurezza pubblica, nazionale e cibernetica, la prevenzione e il perseguimento dei reati, la salvaguardia dell'indipendenza della magistratura e dei procedimenti giudiziari, un mercato concorrenziale, la stabilità economico-

finanziaria, lo sviluppo della scienza e l'avanzamento della medicina, la tutela della salute pubblica e la sicurezza sociale, come pure la trasparenza dei pubblici poteri.

Ma il dato più importante da rilevare concerne la complessiva responsabilizzazione dei titolari del trattamento, delineata dal regolamento quale corollario del mutamento del passaggio da una tutela prevalentemente di tipo remediale, dunque successiva, a una tutela in chiave preventiva. Unitamente alla sostituzione delle misure minime di sicurezza con misure adeguate, il principio dell'*accountability* riflette un'impostazione più sostanzialistica di quello sottesa alla direttiva 95/46/Ce. Tale impostazione valorizza, non tanto la formale osservanza di regole puntuali, quanto l'adozione di una complessiva strategia, nell'organizzazione delle attività istituzionali, fondata sulla minimizzazione del rischio per gli interessati, attraverso tecniche di protezione dei dati fin dalla progettazione e per impostazione predefinita, ma anche sul ricorso alla valutazione d'impatto privacy e alla pseudonimizzazione.

Si tratta di un cambiamento di estrema rilevanza, dal momento che presuppone un ampio margine di discrezionalità, in capo al titolare, in ordine alle scelte da compiere di volta in volta, pur nella rigorosa predeterminazione delle finalità di pubblico interesse perseguite e che mantiene la flessibilità necessaria ad adeguare tali scelte a possibili cambiamenti a seconda del grado di rischiosità del trattamento e del suo impatto sui diritti degli interessati.

In questo quadro, è centrale il ruolo assunto del responsabile della protezione dei dati, figura resa obbligatoria dal regolamento per le Amministrazioni pubbliche, cui spetta il compito di coadiuvare il titolare o il responsabile del trattamento nell'assicurare la piena ed efficace osservanza della disciplina sulla protezione dei dati, verificando costantemente l'adeguatezza e l'efficacia delle misure tecniche e organizzative adottate, anche al fine di prevenire possibili violazioni e mitigare eventuali effetti pregiudizievoli per gli interessati. Questa figura, dotata di una specifica professionalità e di una particolare indipendenza, dovrà essere provvista delle risorse e del supporto necessario per assolvere le sue funzioni, tra cui, quella di "interlocutore privilegiato" dell'Autorità e delle persone interessate dal trattamento.

Peraltro, la violazione del principio di responsabilizzazione (anche nella forma della mancata dimostrazione delle misure adottate per garantire un livello elevato di protezione) integra, al pari dell'inottemperanza agli altri principi, gli estremi di un autonomo illecito amministrativo, per il quale è prevista la sanzione più grave, sino a 20.000.000 euro.

L'Autorità cercherà di guidare questa piccola rivoluzione, nella consapevolezza delle difficoltà, ma anche delle irrinunciabili opportunità che essa comporta, per consentire, anche alle pubbliche amministrazioni, di stare al passo con l'innovazione e con le nuove sfide della società digitale, fondata sull'uso dei dati.

Il Regolamento estende l'obbligo di consultazione preventiva del Garante prevedendo l'acquisizione del parere dell'Autorità non solo per gli atti regolamentari, ma anche per quelli di iniziativa legislativa. Ritiene che in tal modo il ruolo del Garante avrà una maggiore incisività, specie nel valutare la liceità dei trattamenti di dati personali posti in essere in ambito pubblico?

Certo. Il vaglio preventivo del Garante, finora previsto solo con riferimento agli atti di rango regolamentare o amministrativi, contribuisce innanzitutto a evitare possibili contrasti con il diritto europeo, consentendo di modellare la legge nazionale in armonia con i principi fondamentali della protezione dei dati. Ne risulta accresciuto in modo sostanziale anche il livello di garanzia a tutela degli interessati, poiché incorporando la valutazione d'impatto privacy nel processo normativo, i diversi rischi connessi al trattamento possono essere individuati e attenuati in via anticipata. Inoltre, l'introduzione delle garanzie a tutela degli interessati in norme primarie, generali, astratte e valevoli per tutti, assicura la prevedibilità, imparzialità e omogeneità dei comportamenti delle pubbliche amministrazioni, limitandone i margini di discrezionalità, nel rispetto dei diritti fondamentali e, in particolare, di quello alla protezione dei dati personali.

Invero, in questi anni, nonostante si annoverino ancora casi di mancata consultazione obbligatoria del Garante, l'Autorità si è trovata ad essere coinvolta dal legislatore sempre più di frequente nell'elaborazione di fonti di rango primario su materie delicate,sia tramite richieste di parere sulle leggi, che attraverso audizioni alle Camere. Penso, tra gli altri, ai temi dell'amministrazione digitale, della trasparenza,del contrasto all'evasione fiscale,della lotta al terrorismo, dell'immigrazione, del Jobs Act, e del cyberbullismo. Segno di un'evidente consapevolezza che, pur restando legata alla tutela di un diritto fondamentale dell'individuo, la protezione dei dati è un interesse di rilevanza pubblicistica che riguarda l'intera società. Per tale motivo, essa va presidiata non solo a tutela e su richiesta dei singoli interessati,ma anche in via generale e preventiva. La rilevanza dell'attività di monitoraggio continuo, cui il Garante è chiamato, in relazione agli aspetti più

controversi dell'evoluzione della società digitale e dell'innovazione tecnologica, indipendentemente dall'esistenza di concrete attività di trattamento, trova conferma anche in altre previsioni del Regolamento,in base alle quali le Autorità di controllo sono, in generale, tenute a prestare consulenza e supporto costante ad un'ampia platea di soggetti che comprendono oltre che il Parlamento e il Governo, anche altre istituzioni ed organismi nazionali.

Con riferimento a taluni recenti interventi del legislatore che comportano una massiva concentrazione di informazioni personali riferite all'intera popolazione su cui la sua Autorità ha espresso forti perplessità, vorrei chiederle qual è stato l'esito dell'intervento del Garante. Mi riferisco, in particolare, alle iniziative relative alla Piattaforma Digitale Nazionale Dati, affidata in via sperimentale al Commissario straordinario per l'attuazione dell'agenda digitale, alle regole sui nuovi censimenti permanenti che prevedono che le basi di dati di molti enti pubblici,compresa l'Anagrafe tributaria, confluiscano in un grande database dell'ISTAT, nonché all'accordo siglato dalla Presidenza del Consiglio e una società multinazionale per l'utilizzo dei dati sanitari degli italiani finalizzato allo sviluppo di una piattaforma di intelligenza artificiale. Come va valutato in questi casi l'interesse pubblico e in quali casi può prevalere su interessi e diritti delle persone coinvolte?

Le prime due iniziative le abbiamo portate all'attenzione di Parlamento e Governo, sollecitandone il ripensamento, in quanto queste, ove attuate, secondo le previsioni del legislatore, potrebbero pregiudicare l´assetto delle garanzie assicurate fino a oggi dai soggetti pubblici nel trattamento dei dati personali, con un impatto senza precedenti sulla vita privata dei cittadini italiani. Parimenti, abbiamo manifestato profonde perplessità in merito al progressivo processo di centralizzazione e integrazione a fini statistici di archivi amministrativi riferiti all'intera popolazione: il rischio è che simili operazioni si traducano in schedature permanenti degli individui, con grave compromissione dei diritti degli interessati.

E' mia convinzione che la pur necessaria valorizzazione del patrimonio informativo pubblico non deve avvenire a discapito della tutela dei diritti fondamentali e con possibili ricadute anche in termini di sicurezza nazionale. L'Autorità, pertanto, eserciterà con responsabilità il suo ruolo affinché tali iniziative non comportino per i cittadini italiani un arretramento dell'effettività dei principi europei su cui si fonda la salvaguardia dei dati personali, presidio di libertà nei Paesi democratici.

Riguardo al caso Watson, ne abbiamo seguito gli sviluppi, sottolineando la necessità di definire meglio gli aspetti fondamentali del trattamento dei dati dei pazienti, anche alla luce dei compiti istituzionali che spettano alla Regione e della corretta qualificazione del ruolo di IBM, anche in relazione ai possibili impieghi dei risultati conseguiti all'esito della ricerca. E' stato altresì evidenziato che in questo contesto, in cui si sperimentano tecniche innovative basate sull'intelligenza artificiale, coinvolgendo una cospicua parte della popolazione, non si può prescindere da una ponderata valutazione di impatto sulla protezione dei dati, in linea con quanto richiedono le nuove regole europee.

L'impiego delle nuove tecnologie nel campo della ricerca medico-scientifica è anzitutto un fattore di sviluppo e di benessere collettivo e, come tale, va promosso, senza però rinunciare al pieno rispetto dei diritti delle persone e ad un'adeguata salvaguardia degli aspetti più intimi della loro esistenza. Per tale ragione, vanno tenute nella massima considerazione non soltanto le implicazioni giuridiche, ma anche quelle sociali ed etiche dell'uso dei *big data* specie se riferiti a informazioni così delicate, come quelle sulla salute.

Questi temi ci riportano ad una delle grandi sfide di oggi. In quale modo, va affrontata la rivoluzione digitale che con le promesse dei big data seduce l'amministrazione, senza un vero dibattito sull'impatto sociale del cambiamento, specie sui diritti e sulle libertà fondamentali degli individui? Ricordo che il Garante ha avviato, d'intesa con l'Autorità garante per la concorrenza e il mercato e l'Autorità per le garanzie nelle comunicazioni, un'indagine conoscitiva congiunta dedicata al tema dei big data. L'attività è ancora in corso, ci sono delle prime indicazioni?

Siamo in un'epoca in cui l'uso dei dati è oramai indispensabile nei processi decisionali non solo delle imprese, ma anche delle istituzioni pubbliche e sempre di più dei singoli individui. Al crescere della dimensione, della varietà e della disponibilità dei dati, aumenta anche l'esigenza di investire in tecnologie sofisticate di acquisizione, archiviazione ed analisi degli stessi. Così i *big data* sono diventati un fattore strategico non solo nella competizione dei mercati, ma anche nelle innovazioni di importanti settori pubblici. D'altro canto, l'incessante progresso dell'innovazione tecnologica, che ha generato un livello senza precedenti di raccolta e di elaborazione dei dati, è destinato a subire una nuova

espansione con le nuove applicazioni dell'Internet delle cose, della robotica, dell'intelligenza aumentata.

In particolare, l'utilizzo di tecniche di analisi di *big data* permette agli enti pubblici di migliorare prodotti e servizi offerti alla cittadinanza, rendendoli più rispondenti ai loro bisogni e in grado di aumentare il benessere collettivo. I progressi nella potenza di calcolo e nella produzione di algoritmi sempre più raffinati svolgono infatti un ruolo cruciale per la capacità di estrarre dai dati, anche in tempo reale, informazioni significative e di acquisire nuove conoscenze - anche sulla base di valutazioni predittive dei comportamenti di singoli cittadini - in grado di fornire soluzioni efficaci a problematiche complesse, a beneficio dell'intera collettività. Cresce così il numero di soggetti interessati a sfruttarne le potenzialità: attori pubblici e privati, piccoli e grandi, dagli istituti di ricerca agli enti governativi e agli organismi di sicurezza, dalle banche alle compagnie assicuratrici.

Ma i progressi incessanti di questi cambiamenti sollevano interrogativi ineludibili. La raccolta continua e massiva, la trasmissione istantanea ed il riutilizzo dei dati, accompagnati dalla -crescente e generalizzata- tendenza alla centralizzazione e integrazione delle banche dati nel settore pubblico, ci espone a nuovi rischi. E, poiché i dati rappresentano la proiezione digitale delle nostre persone, aumenta anche la nostra vulnerabilità. D'altra parte, l'espansione delle attività governative di monitoraggio dei contenuti in rete, per esigenze di sicurezza, dinanzi alla minaccia criminale e terroristica, favorisce nuove forme sottili e pervasive di controllo che noi stessi alimentiamo, più o meno consapevolmente, per l'incontenibile desiderio di connessione e condivisione. Diventa inoltre strutturale l'asimmetria informativa tra coloro che forniscono i dati e coloro che li sfruttano, disponendo degli *standard* tecnologici dominanti. E si afferma una nuova gerarchia dei poteri in cui un numero esiguo di attori possiede un patrimonio di conoscenza gigantesco, in grado di attuare raffinati meccanismi di persuasione verso ciascuno di noi, non solo come consumatori, ma in quanto cittadini e possibili elettori.

In questo scenario, le tre Autorità hanno avviato un'indagine conoscitiva, al fine di cogliere appieno possibili sinergie e identificare gli strumenti più appropriati per eventuali interventi regolamentari. Nel corso dell'indagine, che ha prodotto talune evidenze preliminari, sono stati approfonditi i radicali cambiamenti derivanti dai *big data* sui singoli individui che forniscono i dati e, in via più generale, sui mercati e sulla società, attraverso tre prospettive diverse e complementari, valorizzando competenze ed esperienze giuridiche, tecnologiche e delle scienze sociali.

Innanzitutto, a fronte della progressiva difficoltà a mantenere un effettivo controllo sui dati a causa dell'opacità delle modalità di raccolta, dei luoghi di conservazione e dei criteri di selezione e di analisi, vanno promosse garanzie di trasparenza dei processi. Ma queste devono tener conto anche del *gap* di conoscenze tecnologiche che può rendere difficoltoso agli individui comprendere appieno queste informazioni ed operare su tali basi scelte consapevoli. Ad ogni modo, in questo processo, non si può prescindere da un generale dibattito pubblico sull'uso etico e responsabile dei *big data* che coinvolga non solo le Autorità di protezione dei dati, ma anche i governi e la popolazione, in una piena e rinnovata consapevolezza di tutti i beni giuridici in gioco.

Un ultimo punto è quello dei rapporti tra trasparenza, alla luce in particolare del nuovo accesso civico (il FOIA italiano) e la tutela dei dati personali. Tenuto conto della prassi formatasi in più di un anno di applicazione della disciplina e dei vari pareri resi in materia dal Garante, quali sono, a suo avviso, i punti di frizione maggiore tra le due normative?

In generale - e l'Autorità ha avuto modo di ribadirlo in più di un'occasione - la privacy non contrasta, ma anzi può contribuire a valorizzare la trasparenza dell'azione amministrativa, mediante un'adeguata selezione delle notizie davvero funzionali all'esercizio del controllo diffuso sull'esercizio dei pubblici poteri. Quello che invece non può essere consentito è che, in nome di un dilatato e malinteso concetto di trasparenza, si comprimano ingiustificatamente i diritti fondamentali degli individui, sostituendo alla trasparenza dell'amministrazione la trasparenza delle persone, trasformandola così in un pericoloso strumento di demagogia.

Ciò che è in discussione, infatti, non è l'affermazione della trasparenza come strumento essenziale di democrazia partecipativa e forma principale dell'agire amministrativo e dell'organizzazione dei pubblici poteri, bensì la necessità di vagliare con attenzione le sue concrete modalità di realizzazione.

Purtroppo la normativa italiana, anche a seguito dell'introduzione dell'istituto dell'accesso civico generalizzato, non è stata in grado di superare l'approccio burocratico che aveva caratterizzato il precedente impianto normativo, basato sulla moltiplicazione indiscriminata di una serie di obblighi di pubblicità indifferenziati, finendo così paradossalmente con il risultare disfunzionale rispetto allo stesso scopo perseguito di contrastare i fenomeni corruttivi. Come ha sottolineato il Consiglio di Stato

nel parere reso sul decreto FOIA, l'eccesso incontrollato di informazioni può provocare quella "*opacità per confusione*" che della trasparenza costituisce l'esatto contrario.

Riguardo all'accesso civico generalizzato, l'assenza di motivazione delle istanze di accesso e la lacunosità dei parametri offerti dalla legge, ai fini della valutazione delle richieste, ha reso evidente il rischio di un'applicazione della nuova disciplina, oscillante tra un'eccessiva rigidità interpretativa e, all'opposto, una dilatazione ingiustificata della nozione di trasparenza. A tali rischi hanno tentato di ovviare le indicazioni fornite con le linee guida dell'Anac adottate - pur in un testo sicuramente perfettibile - con l'intesa del Garante e suscettibili di revisione dopo un anno di applicazione. Al momento però le Linee guida non risolvono del tutto i dubbi interpretativi posti dal nuovo istituto che, essendo basato sul meccanismo del cd. "test del danno", costringe le amministrazioni ad operare di volta in volta una difficile e complessa attività valutativa volta a determinare se l'ostensione del dato o del documento richiesto possa danneggiare concretamente uno o più interessi pubblici o privati, individuati dal legislatore quali limiti all'accesso.

L'applicazione del FOIA richiede un impegno costante e notevole all'Autorità, che con il proprio parere sul ricorso o il riesame, avverso il diniego o il differimento dell'accesso per ragioni di tutela della riservatezza, svolge il ruolo di garante della congruità del bilanciamento, in concreto, rispetto alle caratteristiche del singolo caso, tra trasparenza, da un lato, e protezione dei dati, dall'altro. I molti casi esaminati, sui quali siamo stati chiamati a pronunciarci - peraltro, in tempi ristrettissimi - stanno consentendo di consolidare un indirizzo interpretativo particolarmente rilevante in ordine alla necessaria ponderazione degli interessi in gioco.

In particolare, abbiamo sottolineato che, nel valutare l'esistenza di un possibile pregiudizio concreto alla riservatezza dei controinteressati, occorre tenere in considerazione l'amplificato regime di pubblicità che caratterizza i dati o i documenti ottenuti a seguito di un'istanza di accesso civico, i quali divengono pubblici e chiunque ha diritto di conoscerli, di fruirne gratuitamente e di riutilizzarli, sia pure nel rispetto dei limiti derivanti dalle regole sulla protezione dei dati personali. In questo contesto, va escluso l'accesso civico a qualsiasi informazione da cui si possa desumere, anche indirettamente, la malattia oppure una condizione di invalidità o di disabilità di una persona, o anche una situazione di disagio economico-sociale, così come dati riferiti a soggetti vulnerabili, come i minori.