Privacy digitale e protezione dei dati personali tra persona e mercato".

Persona, diritti fondamentali, innovazione: un primo bilancio di un ventennio di attività del Garante

Intervento di Antonello Soro

Il ventennale della legge sulla tutela dei dati personali cade a cavallo tra l'entrata in vigore e l'applicazione del pacchetto protezione dati, dunque nella fase di più intensa riforma della disciplina di questa materia.

Il ciclo evolutivo che ha caratterizzato il diritto alla protezione dati dalla direttiva madre al "pacchetto"- come anche nei 20 anni di attività del Garante- delinea in chiaroscuro non soltanto il contenuto ma anche le potenzialità, la funzione democratica, la sua indispensabilità per mantenere ancora "umano" un tempo altrimenti ostaggio di tecnologia e potere.

Nel corso della sua evoluzione, questo diritto e la sua cornice normativa si sono dimostrati lungimiranti e duttili quanto necessario per comprendere al loro interno una realtà costantemente e inevitabilmente in mutamento.

E laddove si è avvertito il bisogno di "costituzionalizzare" la nuova dimensione della privacy- proiettandola oltre il profilo statico dell'inviolabilità della sfera privata- è soccorso il legislatore (europeo).

La Carta di Nizza, già nel 2000, ha infatti sancito l'autonomia della protezione dati dalla più tradizionale riservatezza, entrambe costitutive di quella dignità che apre la Carta in quanto "diritto ad avere diritti".

Si sanciva così il passaggio dalla dimensione della "libertà da" verso quella della "libertà per", riconoscendo alla persona il diritto di svolgere un ruolo attivo nella costruzione della propria identità, sempre più insidiata dalla capacità delle nuove tecnologie di influenzare modi di essere e comportamenti.

Con il Regolamento la protezione dati si emancipa quindi dalla dimensione riduttiva del mercato interno (cui anche nella direttiva "madre" si riteneva funzionale), in favore del più ampio approccio di tutela di un diritto fondamentale, caratterizzato dai principi di precauzione e prevenzione e da un'anticipazione della soglia di tutela sin dalla fase anteriore al trattamento: ad esempio con la valutazione d'impatto e misure di protezione fin dalla progettazione o per impostazione predefinita.

La protezione dati si arricchisce di nuovi contenuti: da un lato, diritto alla portabilità -che consente la ricomposizione delle tessere del mosaico dei nostri dati, proteggendo anche la concorrenza da fenomeni di "lock-in"; dall'altro, l'oblio, che consente equilibrio tra storia individuale e memoria collettiva, contro il rischio della "biografia ferita" e di riduzionismo della complessità dell'io in un dettaglio che lo distorce o non lo rappresenta più.

Di questo diritto il Regolamento valorizza anche la funzione sociale, coniugandolo con gli interessi individuali e collettivi di volta in volta meritevoli di bilanciamento e rendendolo fattore di competitività e responsabilità per le stesse imprese.

Nel corso di tale evoluzione, la protezione dati ha dimostrato una progressiva forza espansiva, anche per l'impossibilità di circoscrivere in ragione della nazionalità gli utenti di una realtà globale, qual è appunto la dimensione digitale, per sua natura aterritoriale e per questo refrattaria ai confini di leggi e giurisdizioni..

Circostanza apparsa chiarissima nella sentenza Schrems (e prima Weltimmo), che invalidando l'accordo per il trasferimento dei dati dei cittadini europei negli Usa- per le scarse garanzie lì accordate- ha tra l'altro indotto il legislatore americano a riforme, sia pure parziali, che hanno rafforzato le misure di tutela.

Questa direzione si è poi consolidata con il Regolamento, che ha esteso il proprio ambito di applicazione a qualsiasi trattamento svolto anche da soggetti stabiliti al di fuori dell' Unione, purché inerente l'offerta di beni o servizi o il monitoraggio dell'attività di interessati che si trovino al suo interno.
Con questo criterio di applicazione la norma europea, con una sorta di ultrattività, supera lo schermo dei confini, per assicurare ai cittadini europei idonee garanzie rispetto a qualsiasi trattamento, in particolare a quelli altrimenti attratti in ordinamenti fondati sulla prevalenza delle ragioni della sicurezza o del mercato sui diritti individuali.

E del resto un diritto, quale quello alla privacy, nato per garantire libertà e autonomia, non può conoscere confini e discriminazioni per nazionalità.
Non a caso, non solo in Europa, esso è considerato diritto fondamentale, come tale da riconoscere a prescindere dal requisito della cittadinanza (*vds. il considerando 2 del GDPR).*
Peraltro, la stessa scelta del legislatore europeo di ricorrere in questa materia allo strumento regolamentare- proprio al fine di garantire a chiunque si trovi nell'Unione un paniere uniforme di diritti -è solo il primo passo di una delle sfide più importanti che il legame tra tecnologia, nuovi diritti e prevenzione pone alle nostre democrazie: il riconoscimento universale del diritto alla protezione dati, quale primo presupposto di libertà nella società digitale.

Questo percorso- che dalla direttiva madre, passando per la Carta di Nizza e per decisioni storiche della Corte di giustizia, sarebbe giunto al Regolamento- ha consentito al diritto di non smarrire il senso del limite dinanzi alla "volontà di potenza" della tecnica.
Mai come in questa materia, del resto, il rischio più forte per il diritto è l'anacronismo o la subalternità al "nuovo" per mera rinuncia al tentativo di normarlo.
Disciplinare le forme del governo di ciascuno sui propri dati vuol dire infatti, anche, essere al passo con l'evoluzione scientifica e tecnologica, comprenderla e ricondurla, pur con la sua fluidità, nella cornice, inevitabilmente fissa, delle norme, per impedire che la legge ignori la vita, nella sua concretezza.
Vuol dire, in altri termini, coniugare tecnologia e umanità, libertà e sicurezza, trasparenza del pubblico e riserbo del privato, informazione e dignità, iniziativa economica e autonomia individuale, scienza e libertà dal determinismo.

E' questo, del resto, l'orizzonte su cui si è mossa l'Autorità nei vent'anni trascorsi nello sforzo costante di interpretare il cambiamento -sociale, tecnologico, di costume- riportandovi al centro la persona e cogliendo le sfide poste, di volta in volta, dall'innovazione, che si è potuta così misurare anche secondo i criteri della sostenibilità sociale e dell'ammissibilità etica, prima ancora che giuridica.

I mutamenti affrontati non sono, del resto, marginali: internet non è più soltanto, come nelle origini, uno strumento di comunicazione, ma- nel bene e nel male - il più grande spazio pubblico che l'umanità abbia conosciuto.
In un'epoca di crisi dei tradizionali sistemi di intermediazione, ai giganti della rete è riconosciuto in campi sempre più rilevanti (dall'oblio all'apologia del terrorismo, dall'hate speech al cyberbullismo) un potere di bilanciamento, sia pure in prima istanza, tra beni giuridici fondamentali (dignità, libertà di espressione, sicurezza).
E sarà interessante seguire l'attuazione dell'accordo siglato a Ischia tra i Ministri dell'interno dei Paesi del G7, con particolare riferimento ai sistemi di filtraggio preventivo dei contenuti filo-jihadisti.
Se, infatti, è doveroso impedire che la rete diventi un mezzo (anzi, il principale) di radicalizzazione, è altrettanto doveroso escludere ogni forma di sistematico monitoraggio preventivo, da parte dei provider, delle informazioni scambiate sul web, come del resto ribadisce la stessa direttiva antiterrorismo (541/2017).

In senso più generale, la responsabilizzazione dei grandi protagonisti del web è certamente un processo positivo, una scelta ineludibile, ma, dobbiamo ribadirlo con assoluta chiarezza, non si può assolutamente incoraggiare - con una comoda quanto ingenua delega all'algoritmo di funzioni squisitamente pubbliche- una marginalizzazione del ruolo dello Stato e delle istituzioni democraticamente legittimate nella composizione di diritti e libertà.

Un'ulteriore innovazione che caratterizza il contesto attuale concerne trattamenti, quali quelli svolti su big data, che si snodano lungo una catena dagli anelli infiniti, rispetto ai quali un istituto, quale quello del consenso informato, su cui sinora ha ruotato la disciplina privacy, relativizza molto la sua funzione. Per questo, in tali campi soprattutto, è indispensabile anticipare la soglia della tutela alla fase della progettazione dei sistemi, come prevede del resto il Regolamento.

Per altro verso dopo l'11 settembre, ma anche dopo il Datagate, il rapporto tra libertà e sicurezza si modula su equilibri ben diversi da quelli di vent'anni fa.
Il contesto su cui oggi ci muoviamo è, dunque, assai diverso da quello in cui si inseriva il Garante al momento della sua istituzione.
Ma, nonostante le differenze di contesto, quella della protezione dati è ora- come e più di allora- la frontiera su cui si gioca molta parte del futuro delle società.
E lo è più di allora perché oggi, assai più che vent'anni fa, non vi è attività privata o pubblica che non si fondi su tecnologie "alimentate" da dati personali.
Dati che costituiscono non tanto e non solo il fondamento, quanto piuttosto l'intima essenza della nostra stessa persona e che per questo, per restituirne una rappresentazione integrale e non riduzionista, devono poter essere ricomposti nella loro interezza e complessità.
E se la vita on-line è reale- anche ai fini della responsabilità giuridica- esattamente come quella off-line e se i dati costituiscono la proiezione digitale delle nostre persone, proteggere quei dati vuol dire proteggere la nostra persona, nella sua libertà, dignità, autonomia.
E' il portato inevitabile della trasformazione del tutto (parole, immagini, coordinate spazio-temporali, relazioni sociali) in informazione digitale: la registrazione totale della vita, la "datificazione" dell'esistenza.

Il cosiddetto capitalismo "estrattivo" ha mutato paradigma: sono i dati personali- ceduti senza costi nell'ignoranza del loro valore- la fonte di ricavi impensabili per le grandi imprese del digitale.
E l'incolmabile disparità di potere -non solo contrattuale- tra chi detiene i dati di pressoché l'intera popolazione mondiale e chi quei dati cede per ottenere servizi spesso essenziali, determina uno squilibrio nei rapporti sociali, istituzionali, politici, persino ordinamentali, suscettibile di correzione soltanto ripensando le nostre democrazie, nel segno della centralità della persona e dei diritti.

A partire, appunto, da quello alla protezione dati, che rischia di soggiacere agli imperativi del profitto e del mercato e che deve invece essere garantito quale presupposto di libertà e autonomia, condizione necessaria del libero sviluppo della persona.

La privacy è dunque anche condizione necessaria della democrazia, in quanto rende possibile per i cittadini il pensiero autonomo e critico, l'autodeterminazione: in una parola la libertà, altrimenti insidiata dalla sorveglianza operata dal potere pubblico e privato e dalla massificazione indotta dalla profilazione e dalla "schedatura" di
consumi e bisogni.

La società uniforme, l'assenza di ogni possibilità di dissenso, il controllo di ogni manifestazione di sé, sono del resto sempre stati gli obiettivi di ogni regime illiberale, così come l'argomento del "niente da nascondere" la giustificazione per la sorveglianza totale.

Il compito dello Stato di diritto - nell'era dei big data soprattutto - è, dunque, promuovere la protezione dati quale condizione di democrazia e valorizzazione della persona, in un contesto in cui altrimenti sarebbero i detentori del potere economico (che è appunto essenzialmente informativo) a stabilire regole e fini: della vita pubblica e non solo.

Questo diritto possiede infatti– come ha già dimostrato - una straordinaria funzione di redistribuzione del potere informativo e ha, almeno in parte, corretto le asimmetrie che hanno caratterizzato il rapporto tra dignità umana e iniziativa economica, per riprendere il binomio dell'articolo 41 della Costituzione.
Garantire il diritto alla protezione dati significa, dunque, impedire l'esercizio di poteri incontrollati, fondati sullo sfruttamento di quanto di più privato abbiamo, riequilibrando almeno in parte il rischio di rifeudalizzare i rapporti sociali.
Paradigmatica, in questo senso, l'affermazione, nella sentenza Costeja, della primazia di un diritto fondamentale, quale appunto quello alla tutela dei dati personali, sul mero profitto dei giganti della rete. Primazia progressivamente ostacolata dalle insidie sottese alla combinazione tra big data, internet degli oggetti, tecniche di profilazione sempre più avanzate.

Il "pedinamento digitale" reso possibile dalle tracce che affidiamo ai dispostivi elettronici, il caleidoscopio di identità formatesi sul web (spesso a nostra insaputa) a partire da singoli dati o immagini, la moltiplicazione delle informazioni resa possibile dall'utilizzo sempre più frequente dei big data e dall'espansione di ambienti connessi dove anche gli oggetti dialogano tra loro: tutto questo, unitamente ad algoritmi capaci di automatismi decisionali sempre più sofisticati, accresce in maniera esponenziale i rischi (incrementali perché legati ad attività continue) connessi alla profilazione.

Rischi inerenti non soltanto
-l'opacità dei sistemi automatizzati e i criteri- non sempre fondati sull'imparzialità algoritmica- sottesi alle categorizzazioni (spesso foriere di conseguenze dirimenti sulla vita professionale, sociale, individuale delle persone),
-ma anche possibili discriminazioni derivanti da analisi predittive fondate su inferenze "spurie" o dati non rappresentativi;
-l'omologazione indotta da pubblicità mirata sul profilo di utente attribuito a ciascuno;
-la normalizzazione derivante dall'inibizione della libertà di espressione causata dal timore di stigmatizzazione di comportamenti "non allineati".

Tali rischi sono poi accresciuti dall'intervento sempre più prossimo dell'intelligenza artificiale, la cui capacità di autoapprendimento rischia di espungere del tutto dal processo decisionale il fattore umano.

Cogliendo queste sfide, il Regolamento insiste sulla contestabilità e la trasparenza del processo decisionale automatizzato, dei suoi criteri e delle sue conseguenze, esigendo il filtro dell'uomo, contrastando la delega incondizionata al cieco determinismo dell'algoritmo.

Cautele meno stringenti, ma comunque significative, sono previste dalla direttiva sul trattamento per fini di contrasto, rispetto all'uso, ancora più rischioso, di tecniche di polizia predittiva (si pensi alla profilazione razziale svolta dalla polizia americana dopo l'11.9).

Il ricorso alle nuove tecnologie per fini investigativi rischia, infatti, di riproporre il Panopticon come modello di governo dei fenomeni sociali, con un pericoloso scivolamento dallo Stato di diritto allo Stato di prevenzione.
E', quella della tecnologia, la dimensione in cui oggi, più di ogni altra, il rapporto tra libertà e sicurezza assume forme nuove e costringe a ricercare di volta in volta il limite che ne garantisca la sostenibilità giuridica e politica.

In questi anni ci siamo chiesti tante volte quanto controllo possa sopportare una democrazia e il grado di libertà cui si possa rinunciare, senza divenire schiavi del terrore e senza neppure soccombere.

Ci ostiniamo a pensare che la strada da seguire sia quella di un'intelligence capace di operare una raccolta non "a strascico" ma selettiva di dati, governata dall'ineludibile "fattore umano", capace esso solo di dare senso e forma a masse di informazioni, altrimenti prive di significato.

Evitando tra l'altro raccolte massive che rischierebbero di accrescere "la superficie d'attacco" di fronte alle diverse minacce cibernetiche, di cui pure si è molto discusso nel recente vertice di Ischia.

Del resto, se la resilienza delle democrazie è la più efficace strategia di contrasto, la reazione alla minaccia terroristica deve saper essere efficace ma rispettosa dei diritti e delle libertà fondamentali.

E questo è ancora più necessario in un ordinamento, quale quello europeo, in cui il diritto alla sicurezza è sancito, nella stessa disposizione, accanto al diritto alla libertà, per realizzare appunto quello "spazio di libertà, sicurezza e giustizia" cui alludono i Trattati.

Non a caso, la Corte di giustizia ha costruito l'architrave del rapporto tra prevenzione, tecnologia e dignità proprio sul principio di proporzionalità tra esigenze investigative e protezione dati, al punto da mutare la stessa natura della data retention, da misura massiva in mezzo di ricerca della prova individualizzante (sentenza Tele2).
Nella consapevolezza, già propria della Corte tedesca, che la coscienza di essere soggetti a controllo è già, essa stessa, limitazione della libertà.
Come in Foucault, l'esercizio del potere diviene, nel sorvegliato, coscienza inquieta della propria visibilità.

Il diritto alla protezione dati si intreccia, dunque, con il destino delle nostre libertà e la tenuta delle democrazie, insidiate oggi più che mai dalla tentazione di cedere alla logica dell'uomo di vetro e, con essa, alla rinuncia a diritti e libertà in cambio di una illusoria quanto tirannica idea di sicurezza.
Quando invece la garanzia dei diritti è essa stessa la prima forma di sicurezza.

Anche rispetto alla sfida posta dal terrorismo "immanente" di oggi- con il rischio, che comporta, di normalizzare l'emergenza e, con essa, la conseguente compressione dei diritti - la protezione dati si dimostra un insostituibile presidio di libertà, di prevalenza dello Stato di diritto sulla ragion di Stato.

"Prendere sul serio" questo diritto, in ogni campo della vita privata e pubblica, è allora la sfida che ci attende: come Paese, come Autorità e come cittadini.