GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Regolare il futuro

La protezione dei dati per un'innovazione antropocentrica

Relazione del Presidente Pasquale Stanzione
2023

Roma, 3 luglio 2024

1. Il “cuore antico” del futuro

Signor Presidente della Camera, Autorità, Signore e Signori,

la presentazione, oggi, della Relazione annuale del Garante avviene in una congiuntura alquanto particolare. Il forum intergovernativo del G7 si è da poco interrogato sull’impatto dell’intelligenza artificiale sulla politica, sulle relazioni internazionali, sulla vita individuale e collettiva. Il 17 maggio scorso, il Consiglio d’Europa ha adottato la prima Convenzione internazionale, giuridicamente vincolante, che impegna gli Stati aderenti (non solo europei) al rispetto di alcune essenziali garanzie per i diritti umani, la democrazia e lo Stato di diritto nell’utilizzo dei sistemi di intelligenza artificiale.

Poco prima, l’Unione europea aveva approvato, in conclusione di legislatura, la prima disciplina al mondo, di taglio organico e non settoriale, dell’intelligenza artificiale, segnando una primazia che non è, affatto, soltanto cronologica ma è, soprattutto, assiologica. L’*Ai Act* – tanto più se inscritto all’interno del complessivo quadro regolatorio del digitale, definitosi nei suoi ultimi tasselli con il *Data Act* – rappresenta, infatti, assieme a ciò che fu il GDPR otto anni fa, il tentativo più avanzato dell’Europa di delineare una strategia antropocentrica di governo della tecnica.

Nel promuovere un’innovazione sostenibile sotto il profilo delle garanzie giuridiche, dell’equità sociale, della dignità personale, l’Europa ha, infatti, investito sul terreno del digitale la propria identità come Comunità di diritto, marcando la propria specificità tanto rispetto alla d*eregulation* o

alla settorialità dell'approccio americano (di cui l'*Executive Order* di ottobre 2023 è espressione), quanto rispetto all'autoritarismo sino-coreano.

E pur con l'inevitabile asincronia del diritto rispetto alla tecnica, con la sua velocità incessante, i tempi della regolazione sono significativi. L'attenzione – soprattutto, ma non soltanto europea - nei confronti delle neotecnologie esprime, infatti, la consapevolezza dell'ormai piena integrazione dell'intelligenza artificiale nella nostra vita privata e pubblica. Il 2023 è stato l'anno della diffusione massiva dell'intelligenza artificiale, così estesa e veloce da aver addirittura indotto, nel marzo di quell'anno, mille esponenti delle *big tech* a suggerire, con una lettera aperta, una moratoria sullo sviluppo di questa neotecnologia, ritenuto eccessivamente rapido.

Pur limitandoci a pochi dei molti esempi che si potrebbero fare, si consideri che circa il 65% dei ragazzi utilizza oggi l'intelligenza artificiale per svolgere i compiti; due studenti su tre avrebbero preparato l'esame di maturità ricorrendo a *Chat Gpt* che peraltro, a quanto pare, non sarebbe riuscita a tradurre correttamente il Minosse, o Della legge, attribuito a Platone.

L'intelligenza artificiale è riuscita persino ad arricchire, con effetti visivi e sonori straordinari, la Turandot rappresentata alla Scala. Un' impresa su quattro, nel nostro Paese, ha già integrato l'intelligenza artificiale nei propri processi produttivi ed entro un anno – si stima – il 60% delle aziende la utilizzerà nei procedimenti assunzionali.

Si ritiene, inoltre, che l'intelligenza artificiale potrebbe sostituire, nei prossimi anni, circa 85 milioni di posti di lavoro creandone, tuttavia, 97 (milioni) di nuovi, sebbene con un rischio di nuove, ulteriori diseguaglianze, evidenziato con preoccupazione dal Fondo monetario internazionale. E non

si tratta, del resto, di un rischio così peregrino, se si considerano le profonde diseguaglianze che, anche sul terreno del lavoro, il capitalismo digitale ha prodotto, rispetto ai lavoratori "invisibili" della *gig economy.*

In ambito sanitario sono moltissime e sempre più significative le applicazioni di intelligenza artificiale a fini diagnostici, sperimentali, terapeutici. Secondo una recente ricerca, le molecole farmacologiche scoperte mediante l'intelligenza artificiale mostrerebbero un tasso di successo, nella prima fase clinica, pari a circa l'80-90%: una promessa importante per la cura di molte malattie. E a dimostrazione delle straordinarie potenzialità delle neotecnologie, basti pensare che si ricorre già al Metaverso per effettuare visite mediche a detenuti, così da coniugare il diritto alla salute – che neppure in carcere può ammettere limitazione – ed esigenze di sicurezza (è il progetto della colonia penale di Mamone).

Questi esempi – e molti altri che si potrebbero addurre – dimostrano come effettivamente l'intelligenza artificiale sia ormai entrata a far parte del nostro orizzonte quotidiano di vita e sempre più ne sarà elemento costitutivo, con effetti della cui portata (in senso lato antropologica) non siamo, forse, del tutto consapevoli.

Il diritto ha il compito di colmare questo vuoto di consapevolezza, fornendoci gli strumenti per capire come porre realmente al servizio dell'uomo ciò che può rappresentare tanto uno straordinario fattore di sviluppo, benessere, promozione del pubblico interesse quanto anche, se non ben governato, una fonte di rischi tutt'altro che trascurabili, per la persona, la società, la democrazia. La sfida principale che si delinea all'orizzonte è tutta nel rendere l'evoluzione tecnologica davvero mimetica e non soltanto protesica (capace cioè di simulare l'uomo e la sua razionalità, prima e oltre che colmarne le carenze) un fattore di progresso

non solo tecnico ma sociale, temperando – per riprendere le parole del Pontefice – con l'algoretica gli eccessi dell'algocrazia.

Agli algoritmi e alla loro pretesa neutralità si affidano, infatti, decisioni sempre più significative, assecondando per ciò la svolta ingiuntiva della tecnica, sempre più demiurgica, predittiva e quindi performativa. Tra gli opposti estremi, entrambi scorretti, del soluzionismo tecnologico scientista e del neoluddismo, si delinea dunque l'obiettivo del prossimo futuro: un governo democraticamente sostenibile della tecnica, che tracci il confine oltre il quale, per riprendere Nietzsche, non si può fare tutto ciò che *si può* fare, ponendo limiti a una volontà di potenza che, altrimenti, non ne conoscerebbe e che, anzi, tenderebbe a spostare sempre più in là la frontiera delle possibilità. Va, dunque, delineato quel "cuore antico" del futuro (parafrasando Carlo Levi) che àncori l'innovazione a un limite giuridico, politico, sociale, prima ancora etico di sostenibilità.

2. Il momento Oppenheimer

La persistenza della guerra, ai confini d'Europa e, da ottobre scorso, anche nel cuore del Mediterraneo, offre all'intelligenza artificiale un drammatico terreno di sperimentazione in contesti bellici, dove la potenza geometrica dell'algoritmo rischia di amplificare senza limiti la capacità offensiva dei conflitti, sottraendo all'uomo il controllo della violenza.

Si tratta non tanto e non soltanto dei droni - cui si è fatto ampio ricorso nel contesto russo-ucraino - quanto di sistemi, come Lavender, utilizzati nel conflitto israelo-palestinese per identificare i *target,* tuttavia con un ampio margine di tolleranza delle "*casualties*" (vittime collaterali): emblematico ossimoro del dramma della guerra. Secondo alcune fonti

citate da *The Guardian*, infatti, l'alto numero di civili rimasti vittime dei bombardamenti sulla striscia di Gaza sarebbe imputabile all'uso indiscriminato dell'intelligenza artificiale. Quella stessa intelligenza artificiale che, paradossalmente, Mosab Alì utilizza come terapia per i traumi subiti dai bambini della Striscia.

E se Lavender contempla ancora una decisione finale umana, seppur meramente estrinseca, sull'indicazione proposta dall'algoritmo, si stanno sperimentando strumenti offensivi capaci anche di prescinderne, come si è chiarito alla Conferenza internazionale di Vienna di aprile. Si ritiene, non a torto, che le armi autonome possano rappresentare la nuova bomba atomica, per gli effetti dirompenti e l'assenza di regole che ne potranno caratterizzare l'utilizzo, tanto da qualificare quello attuale come un nuovo "momento Oppenheimer".

E, anche oltre il contesto bellico in senso stretto, l'intelligenza artificiale alimenta quella "cognitive warfare" – realizzata con la manipolazione e monopolizzazione dell'informazione, su cui lo stesso Presidente della Repubblica ha stimolato una riflessione – capace di rappresentare, secondo alcuni, la nuova guerra fredda, spintasi in quello che la Nato ha definito il sesto dominio della conflittualità.

La stessa vice-Presidente della Commissione UE ha espresso preoccupazione rispetto all'utilizzo massivo e con metodi algoritmici, a fini di competizione geopolitica, dei dati personali da parte di alcuni Stati: il bando statunitense dei prodotti Kaspersky è, del resto, in tal senso significativo. Essa ha infatti sottolineato come i "tempi nervosi" in cui viviamo inducano a una crescente domanda di sicurezza da parte dei cittadini, che va dunque – aggiungiamo - filtrata e analizzata, dalla politica,

con la necessaria lungimiranza, tanto più alla luce delle potenzialità dell'intelligenza artificiale, per essere più efficaci, non meno liberi.

La continua espansione ed evoluzione dell'intelligenza artificiale impone dunque di tracciare (e questo è il massimo compito della politica) un limite di sostenibilità, delle colonne d'Ercole da non varcare perché il progresso non divenga, paradossalmente, socialmente regressivo.

Si pensi, a titolo meramente esemplificativo, ai progetti di utilizzo dell'intelligenza artificiale in campo neuroscientifico, con la realizzazione di *decoder* "semantici" dell'attività neurale, combinando scansione cerebrale e database di modelli linguistici, come quelli usati da *Chat Gpt*. A gennaio, negli Stati Uniti, è stato applicato per la prima volta, a un paziente tetraplegico, un dispositivo in grado di decodificare i segnali neurali per far eseguire a un robot ciò che i suoi arti non possono fare.

Si tratta di un'innovazione potenzialmente rivoluzionaria, capace di apportare benefici senza precedenti per la cura di stati neurodegenerativi e, per ciò, meritevole di sviluppo, purché tuttavia non si giunga alla trasparenza del pensiero: il più illiberale e pericoloso degli esiti possibili. La possibilità di traduzione dell'attività neurale in impulsi algoritmici è, infatti, una conquista preziosa a condizione che non venga utilizzata per leggere il pensiero, rendendo dunque accessibile anche quel foro interno la cui riservatezza è presupposto necessario per la libertà di coscienza.

Quello del limite e dello scopo (o, meglio, di uno scopo diverso dalla mera volontà di potenza) è, dunque, il principale obiettivo da perseguire nel governo della tecnica, perché l'uomo non divenga, paradossalmente, egli stesso strumento della macchina anziché suo d*ominu*s, al "servizio della manovella", come nell'icastica immagine pirandelliana di Serafino Gubbio operatore.

3. Territorio di frontiera

Se il Garante è potuto intervenire su molti sistemi di intelligenza artificiale (nell'ultimo anno *ChatGPT*, *Sora, Replika*) è perché la disciplina di protezione dei dati regola (e continuerà a farlo anche dopo l'*AI Act*) il fulcro dell'intelligenza artificiale: il trattamento di dati personali funzionale a processi decisionali automatizzati e all'addestramento dell'algoritmo.

Rispetto a questo nucleo fondativo dell'intelligenza artificiale, la disciplina di protezione dei dati ha introdotto infatti, non da ora, alcune garanzie essenziali: dal principio di conoscibilità al divieto di discriminazione algoritmica; da un generale principio di trasparenza, che impone precisi obblighi informativi nei confronti dell'utente a un criterio di qualità ed esattezza dei dati da utilizzare, particolarmente rilevante per evitare i *bias* propri di un addestramento dell'algoritmo sulla base di informazioni inesatte o non sufficientemente rappresentative.

Le garanzie particolari accordate nel trattamento dei dati dei minori si sono, inoltre, rivelate determinanti nell'assicurare il controllo sull'accesso degli infraquattordicenni ad alcuni dei contenuti offerti da sistemi di intelligenza artificiale generativa e *chatbot* tra cui *Replika* e *ChatGpT*, spesso inadeguati (ad esempio perché sessualmente espliciti) per il corretto sviluppo cognitivo, etico, personologico dei minori. L'attenzione posta dal Garante sulle carenze di *chatbot* come *ChatGpT* ha stimolato, peraltro, anche il Comitato europeo per la protezione dei dati a trattare il tema ad ampio raggio e su scala appunto europea, con una *task force* costituita *ad hoc*.

Particolare rilievo assume anche il provvedimento sul *webscraping*, recante alcune garanzie essenziali (e, per converso, adempimenti a carico

dei titolari) per impedire che le nostre vite si traducano – come si è detto - in alimento per gli algoritmi. I limiti del *webscrapin*g sono stati sottolineati anche rispetto alla riforma fiscale, nel cui ambito il ricorso all'intelligenza artificiale esige requisiti stringenti di affidabilità ed esattezza dei dati utilizzati per la profilazione del contribuente. Se addestrato su dati anche soltanto parzialmente inesatti, infatti, l'algoritmo restituirà risultati errati in proporzione geometrica, con *bia*s che dalla base informativa si propagano lungo tutto l'arco della decisione algoritmica. Per questo, ad esempio, nel parere sul decreto legislativo, sul concordato preventivo, è stato richiesto di espungere un riferimento che avrebbe potuto legittimare analisi del rischio fiscale fondate anche sul *webscraping*.

Basare le procedure accertative su informazioni "rastrellate" dal web – come tali in larga misura inesatte – è, infatti, estremamente rischioso, potendo avere effetti fortemente distorsivi sulla corretta rappresentazione della capacità fiscale dei contribuenti. Le garanzie di protezione dei dati rappresentano quindi, anche in quest'ambito, presupposti di efficacia dell'azione di contrasto dell'evasione fiscale.

Riguardo al settore sanitario, caratterizzato dal ricorso qualitativamente e quantitativamente crescente all'intelligenza artificiale, con lo specifico "decalogo" adottato lo scorso ottobre si è inteso rimarcare i principi che presiedono al corretto utilizzo dei dati personali mediante sistemi d'intelligenza artificiale, riconducibili in estrema sintesi ai principi di trasparenza e supervisione dei processi decisionali automatizzati, nonché di non discriminazione algoritmica.

La disciplina del GDPR sulla decisione algoritmica è funzionale anche ad evitare che il legittimo controllo del territorio, a fini di sicurezza, degeneri, sia pur preterintenzionalmente, in sorveglianza massiva. Per

questo, ad esempio, si è inteso verificare la legittimità del sistema di videosorveglianza "intelligente" adottato dal Comune di Trento, la cui incidenza sui diritti e le libertà dei cittadini avrebbe comportato l'adozione di garanzie significative.

Queste iniziative (e molte altre che si potrebbero richiamare) dimostrano la ragione per cui l'*AI Act*, nel delineare il sistema di g*overnance* dell'intelligenza artificiale, sancisca una specifica riserva di competenza in favore delle Autorità di protezione dei dati, in particolare in settori (immigrazione, attività di contrasto, giustizia, processi democratici) nei quali la potenza algoritmica rischia di amplificare la strutturale asimmetria del rapporto in cui si inscrive o le vulnerabilità proprie, per condizione soggettiva o circostanza, degli interessati. Ed è anche questa la ragione per cui, come rappresentato più volte al Parlamento e al Governo, l'individuazione nel Garante dell'Autorità competente per l'*AI Act* sarebbe la più coerente con l'incidenza, profonda e trasversale, dell'intelligenza artificiale, sui diritti fondamentali (cui, significativamente, si rivolge la stessa valutazione d'impatto prescritta per i sistemi ad alto rischio). Essa suggerisce, infatti di attribuirne la competenza ad Autorità caratterizzate da requisiti d'indipendenza, in ragione dei "limiti e delle aporie" che la regola maggioritaria presenta, come insegnava Norberto Bobbio, di fronte a quel "territorio di frontiera" rappresentato dai diritti di libertà; la sfera dell'indecidibile, appunto.

4. La giustizia e il digitale

L'anno trascorso è stato determinante per la piena realizzazione del processo di digitalizzazione della giustizia, cui il Garante ha fornito un

contributo significativo soprattutto in sede consultiva, rispetto sia al processo (ordinario) telematico, sia alla costituzione delle infrastrutture digitali per le intercettazioni. I flussi informativi funzionali alla giurisdizione presentano, infatti, caratteristiche tali da esigere cautele peculiari e garanzie rafforzate nella loro utilizzazione, per la tutela dei soggetti interessati e degli stessi interessi pubblicistici sottesi (si pensi, per tutti, al segreto investigativo o all'autonomia e indipendenza della magistratura).

Ma con questi presidi offerti, anche, dalla disciplina di protezione dei dati, la capacità trasformativa del digitale può rappresentare uno straordinario fattore di progresso e miglioramento dell'attività giurisdizionale, a beneficio di tutti gli attori coinvolti. E' dunque opportuna la valorizzazione, operata tanto dalla riforma Cartabia in entrambi i settori della giustizia ordinaria, quanto dal PNRR, delle risorse digitali in ambito giurisdizionale.

Gli aspetti più delicati, dal punto di vista della protezione dei dati, comuni a questi progetti, pur nella loro diversità, possono ricondursi a due macroaree: la sicurezza e la riservatezza in senso stretto. Con riferimento al primo aspetto, va ricordato - come peraltro rilevato in sede di audizione sul disegno di legge sulla cybersicurezza - che ogni ipotesi di digitalizzazione determina rischi in termini di sicurezza cibernetica. L'esposizione al mezzo telematico comporta, infatti, delle vulnerabilità da cui i dati e i sistemi che li ospitano vanno protetti, per la salvaguardia non soltanto della privacy dei soggetti coinvolti, ma anche della stessa efficienza dell'amministrazione della giustizia, come recenti casi di cronaca dimostrano.

Questo aspetto è centrale nei pareri resi, anche quest'anno, dal Garante sui vari provvedimenti che hanno disciplinato la telematizzazione

di alcuni flussi informativi o la costituzione di nuovi sistemi digitali, con l'esigenza di garantire misure tecniche e organizzative realmente adeguate al grado di rischio connesso al trattamento.

Peraltro, la digitalizzazione non tocca il solo profilo organizzativo e strumentale della giurisdizione, ma anche quello più strettamente processuale, investigativo e probatorio. Soprattutto su questo terreno, il ricorso alla tecnologia e alle sue potenzialità crescenti lascia intravedere l'esigenza di una più puntuale regolazione, come plasticamente emerso in relazione alla *data retention* e ai criptofonini: temi sui quali la giurisprudenza, europea e interna, ha dovuto svolgere un'azione per certi versi di supplenza, per altri di monito al legislatore.

Si dovrebbero, peraltro, rafforzare ulteriormente (secondo direttive già suggerite dal Garante in audizione) le garanzie per le intercettazioni mediante captatore, la cui applicazione sta mostrando tutti i limiti della delega, alla tecnica, di uno strumento potenzialmente "onnivoro" quale il trojan, tanto più se utilizzato "a strascico".

Un altro profilo ricorrente nei processi di digitalizzazione concerne il bilanciamento tra pubblicità degli atti processuali (amplificata esponenzialmente dal mezzo telematico) e garanzia della riservatezza delle parti e dei terzi coinvolti. Un profilo peculiare è emerso a seguito dell'estensione, con la riforma Cartabia del ricorso, nel processo penale, alla riproduzione audiovisiva e fonografica come modalità generale di documentazione, che è destinata ad affiancare il verbale per gli atti del procedimento, quale modalità preferenziale di documentazione dell'interrogatorio di garanzia dell'indagato *in vinculis* o forma di documentazione dell'assunzione dibattimentale dei mezzi di prova.

Tale innovazione - in ragione del suo impatto sul trattamento dei dati personali delle parti e dei terzi coinvolti, a vario titolo, nel procedimento, benché volta a garantire una rappresentazione più accurata dell'atto – ha indotto il Garante a suggerire l'introduzione di un regime speciale di pubblicità degli atti così documentati. Esso dovrebbe, in particolare, bilanciare le esigenze di pubblicità, espressione del principio di cui all'art. 101, I c., Cost., il diritto alla riservatezza e il principio di minimizzazione dei dati trattati.

E' chiaro, infatti, che l'applicabilità a tali atti, documentati digitalmente nella loro integralità, del regime ordinario di pubblicità, potrebbe determinare l'indiscriminata diffusione di dati eccedenti, talora anche appartenenti alle categorie particolari cui l'ordinamento accorda una tutela rafforzata, sino al divieto di diffusione per i dati sanitari, genetici, biometrici. Si tratta, peraltro, di un bilanciamento coerente con quello sotteso anche a innovazioni normative recenti, quali l'oblio per i soggetti destinatari di provvedimenti giudiziali favorevoli (rispetto al quale il Garante ha chiarito doversi operare un bilanciamento tra gli interessi in gioco, senza presunzioni assolute di prevalenza) e le nuove disposizioni sulla trascrizione delle intercettazioni introdotte dal d.l. 105 del 2023. Esse si inseriscono, peraltro, all'interno del più ampio disegno di revisione della disciplina delle intercettazioni – in parte ancora in itinere - volto a rafforzare (ulteriormente rispetto a quanto disposto dalle riforme del 2017 e del 2019 e in linea con le indicazioni del Garante) le garanzie in favore dei terzi, indirettamente intercettati.

Come si è avuto modo di sottolineare in audizione, il ddl governativo, in particolare, rafforza sensibilmente, le garanzie di riservatezza dei terzi e, per altro verso, circoscrive l'ambito circolatorio (endo- ed extra-

processuale) dei contenuti captati, a tutela della privacy di tutti i soggetti (parti e terzi) le cui conversazioni siano acquisite. Se si limita la pubblicabilità delle intercettazioni ai soli contenuti riprodotti dal giudice in propri provvedimenti, si circoscrive notevolmente il novero dei dati suscettibili di circolazione al di fuori del giudizio, ammettendola soltanto per le informazioni rilevanti a fini processuali.

Queste modifiche sottendono, ovviamente, un bilanciamento tra privacy e diritto di (e all') informazione, la cui definizione è riservata alla discrezionalità del legislatore. Ciò che si può auspicare - anche rispetto alla delega legislativa sul divieto di pubblicazione integrale o per estratto dell'ordinanza di custodia in fase di indagini - è che si contenga la tendenza a scambiare l'interesse sociale della notizia con il gossip.

La sfida della democrazia è, infatti, proprio nel coniugare la "pietra angolare" del diritto di (e all') informazione con la dignità personale (di cui la protezione dei dati è peculiare espressione): tanto più in un ordinamento, come il nostro, dalla vocazione intrinsecamente personalista.

5. Biologia e biografia

La sfida della digitalizzazione riguarda anche - e non senza analoga complessità - il settore sanitario, rispetto al quale la protezione dei dati ha dimostrato di poter rappresentare un fattore di efficienza della *governance* sanitaria ma, anche, di fiducia dei cittadini nella sanità. Sulla sinergia tra innovazione, sanità e protezione dei dati si giocherà, infatti, una sfida sempre più determinante per le nostre società, che dobbiamo impegnarci a vincere nel segno, ancora una volta, della centralità della persona e della

sua dignità: quei vincoli che, spiegò Aldo Moro in Assemblea costituente, neppure l'interesse collettivo alla sanità pubblica può superare.

I dati sulla salute sono, infatti, prezioso strumento di garanzia del diritto alla salute e alle cure (che, con lungimirante affermazione, la nostra Costituzione assicura anche "agli indigenti"), anche nella componente solidaristica della destinazione a fini di ricerca ma, al tempo stesso, prezioso frammento della vita più intima di ciascuno, da proteggere da indebite ingerenze o strumentalizzazioni. Non a caso, tra le prime norme dell'ordinamento sulla riservatezza si annoverano proprio quelle inerenti i dati sanitari, da proteggere per evitare fughe dalla diagnosi e dalla terapia, così da costruire, sulla base dell'affidamento riposto nel segreto professionale, il rapporto strettamente fiduciario tra medico e paziente che costituisce l'architrave della disciplina odierna e della giurisprudenza sull'autodeterminazione terapeutica.

Queste garanzie vanno assicurate anche – a maggior ragione – in un contesto di sempre più marcata digitalizzazione della sanità e di promozione della ricerca scientifica che va, tuttavia, inscritta all'interno di un progetto organico e lungimirante di *governance* sanitaria. Esso deve, in particolare, minimizzare i rischi cibernetici e promuovere una condivisione selettiva dei dati, ammettendone anche (come prevede il Regolamento sullo spazio europeo dei dati sanitari) la destinazione solidaristica, anche a fini di ricerca, ma con le dovute cautele per evitare ogni indebita reidentificazione degli interessati e discriminazione per gruppi (rischio tanto più elevato ove i *dataset* sui quali si fonda la decisione algoritmica non siano rappresentativi o sottendano comunque pregiudizi di genere, etnia, condizioni sociali o appunto di salute e così via).

Da questo punto di vista, la recente riforma della disciplina dell'uso dei dati personali a fini di ricerca scientifica, nell'escludere la previa consultazione del Garante anche in assenza del consenso dell'interessato, responsabilizza notevolmente i ricercatori, che saranno tenuti a verificare autonomamente le condizioni di legittimità del trattamento, anche alla luce delle specifiche regole deontologiche, oltre che del parere del comitato etico.

Con riguardo alla digitalizzazione della sanità, sono particolarmente rilevanti le criticità segnalate al Governo rispetto alle difformità riscontrate, tra le varie Regioni, nella realizzazione del FSE 2.0, concepito invece proprio per assicurare omogeneità nelle garanzie di fruizione tra le varie aree del Paese. Diritti fondamentali come quello alla salute – e, per altro verso, la protezione dei dati – non possono, infatti, tollerare garanzie a geometria variabile, con le diseguaglianze *ratione loci* suscettibili di derivarne.

E'quanto, del resto, ha recentemente ribadito la Corte costituzionale nel dichiarare illegittima, per violazione del riparto di attribuzione della potestà legislativa tra Stato e Regioni, una legge regionale volta a legittimare la videosorveglianza nelle strutture di cura, in assenza di norme legislative statali in materia.

Quest'esigenza di uniformità è tanto maggiore in ragione della progressiva integrazione dei sistemi (soprattutto) informativi in ambito sanitario prevista dal Regolamento sullo spazio europeo dei dati sanitari. Esso, infatti, pur promuovendo la destinazione a fini solidaristici dei dati sanitari (in linea con l'idea dei dati come beni comuni sottesa già al *data altruism* del *Data Governance Act*), introduce tuttavia significative garanzie anche per la c.d. *group privacy*, con specifici divieti di utilizzo

discriminatorio dei dati sanitari nei confronti di singoli o gruppi di persone, anche per quanto riguarda offerte di lavoro o condizioni contrattuali.

Analoga esigenza non discriminatoria è sottesa alla disciplina dell'oblio oncologico, condivisa – anche in fase attuativa – con il Garante, volta a impedire che la persona sia risolta nella sua malattia e che la biografia sia schiacciata, ineludibilmente, sulla biologia.

Non del tutto dissimile, almeno nel suo significato più profondo, l'esigenza di riservatezza che ha indotto il Garante ad intervenire, anche sul piano sanzionatorio, rispetto alla vicenda del "cimitero dei feti", ovvero dell'indicazione dei nomi delle donne che avevano praticato un'interruzione volontaria di gravidanza su targhette apposte sulle sepolture dei feti presso un cimitero romano.

In gioco qui vi erano non tanto e non "soltanto" dati sulla salute come, pure, sono quelli sull'aborto quanto, piuttosto, informazioni rilevantissime (e per ciò soggette alla massima riservatezza) su scelte di ordine esistenziale, etico, per certi aspetti persino religioso, tra le più delicate. Come spesso accade, anche in questo caso una questione che coinvolge il corpo giunge, ben al di là - dalla biologia alla biografia, appunto - al cuore di quelle "scelte tragiche" che meritano il massimo riserbo.

6. Asia e le altre

La vicenda di Asia, la ragazza insultata in rete perché (!) malata, così come quella, di pochi mesi precedente, della ristoratrice toltasi la vita per non aver retto alla "condanna" dello spietato tribunale di internet, simboleggiano, drammaticamente, le aberrazioni cui può giungere l'odio digitale.

Preoccupa l'uso offensivo del web, la diffusione anche tra i giovani di messaggi istigativi, discriminatori nei confronti, generalmente, di minoranze, delle donne o di chiunque sia percepito come "altro-da-noi", con rivendicazioni identitarie in forma aggressiva. Le stesse caratteristiche socio-tecniche (c.d. *affordances*) delle piattaforme sono, spesso, non neutrali rispetto al genere e tali, dunque, da agevolare o, quantomeno, normalizzare atteggiamenti sessisti.

E se la rete esprime la morfologia sociale dell'oggi, questa sua degenerazione non può non interrogarci con la drammaticità dei problemi epocali, a partire dagli episodi, susseguitisi la scorsa estate e sui quali il Garante è più volte intervenuto, di diffusione sui social di immagini di stupri commessi da ragazzi, in gruppo, su ragazze, sole. Le interrelazioni tra il web e la violenza sono, infatti, più profonde e ambivalenti di quanto una drammatica contabilità delle loro aberrazioni possa restituire.

La rete mostra infatti – accanto a innegabili, straordinarie, potenzialità di progresso anche sociale – sempre più un lato oscuro, un suo prestarsi a logiche di sopraffazione che finiscono con il tradirne l'originaria promessa inclusiva. Internet rappresenta così non soltanto il "teatro" della violenza (e di violazioni varie come l'impersonificazione e le frodi, oggi in netto aumento) ma anche, spesso, un suo fattore propulsivo, capace di mutarne, profondamente, forme di manifestazione e implicazioni, per persistenza, pervasività, emulazione, difficile contenibilità del danno.

Si pensi al *revenge porn*, rispetto a cui l'indiscriminata pubblicità, lo *shaming effect* indotti dalla diffusione in rete di immagini intime rendono possibile una forma nuova e del tutto singolare di violenza, appunto digitale. Il tradimento della fiducia sottesa a quell'intimità e dell'aspettativa di riservatezza che le è propria, si realizza infatti proprio per effetto

dell'ampia diffusività assicurata dal web ai contenuti che vi sono immessi. L'esercizio, da parte del Garante, della specifica competenza attribuitagli in materia di *revenge porn* (consistente nella decisione sulle istanze di blocco del caricamento non consensuale di contenuti intimi: in quest'anno, 299), ha consentito all'Autorità di verificare la vastità e pervasività del fenomeno, che in tal modo si può almeno in parte arginare.

Ma la violenza digitale assume anche le tragiche vesti della riedizione, *on line*, della violenza inferta *off-line*, nella sua immane concretezza. L'amara cronaca dell'estate scorsa ci ha mostrato come la barbarie degli stupri, commessi da ragazzi - in gruppo - su ragazze, sole, possa superare ogni limite di atrocità venendo filmata, condivisa e irrisa, come fosse il frammento di un'ordinaria quotidianità. La violenza fisica viene così, con se possibile persino maggiore sprezzo, perpetuata nella violenza rappresentata e poi divulgata, con gli effetti drammatici della vittimizzazione secondaria, che il Garante con i suoi interventi ha cercato di contenere.

E vittime e autori di questo dramma sono, troppo spesso, coloro i quali - i ragazzi, appunto – intessono con le nuove tecnologie un rapporto quasi osmotico, ancorché spesso inconsapevole. La micro-celebrità che assicura il web, con il mito di *influencer* seguiti da milioni di *follower*, sembra così poter assicurare l'identità che si fatica altrimenti a costruire, giungendosi al paradosso di voler riprodurre *on line* la propria vita, anche al prezzo di quella degli altri.

Se quest'alienazione dal reale è il frutto della virtualizzazione della vita, dell'intersezione costante, fin quasi alla sovrapposizione, delle dimensioni reale e virtuale, si rischia di confondere la vita con la sua rappresentazione, la persona con l'*avatar*, il corpo con la sua immagine,

riducendo anche la percezione del "male", di cui la rete offre spesso una narrazione pornografica. La stessa diffusione dei *deep fake*, espressiva della capacità della tecnica di rendere imitabile, riproducibile, "falsificabile" ciascuno, induce a sottovalutare l'irripetibile unicità della persona.

Il malinteso anonimato del web, come la defisicizzazione dei rapporti (l'altro ridotto a immagine, profilo, *avatar*) alimentano così, soprattutto nei giovani, quell'aggressività che spesso nella vita *offline* incontra il limite dell'inibizione e la deterrenza del controllo sociale. Ma si può – e si deve - interrompere la mimesi della violenza e illuminare il lato oscuro della rete, rendendola quello strumento di libertà, pluralismo e democrazia che ben potrebbe essere. Per questo, va anzitutto difesa l'unicità della persona (con tutta la sua fragilità e fallibilità) e, con essa, la solidarietà verso l'altro, contro gli effetti deleteri di quella che Lacan definiva, con lucidità, "iocrazia".

In questo percorso è indispensabile – molto più dei divieti - la pedagogia digitale cui il Garante ha dedicato, soprattutto ma non soltanto quest'anno, una parte significativa della propria attività, nella consapevolezza della sua necessità per costruire un futuro democraticamente sostenibile.

7. Lo sguardo presbite del diritto

La promozione, tra i cittadini, di un'adeguata "coscienza digitale" (anche rispetto all'uso di dispositivi IOT o al ricorso alla telemedicina) è una delle funzioni cui il Garante ha riservato, anche nell'anno trascorso, una particolare attenzione. Molte altre e di segno diverso, tuttavia, sono state le iniziative che hanno consentito al Garante di intervenire sui vari ambiti

rimessi alla sua competenza, trasversale e, come tale, tangente ogni ambito della vita e della società. La peculiarità di questa Autorità è, anzi, proprio la poliedricità degli ambiti e delle funzioni che le sono ascritti consentendole così, in una strategia integrata, sul piano interno e internazionale, di offrire una tutela ad ampio spettro a un diritto, come quello alla protezione dei dati, tipicamente "d'avanguardia".

Così, la funzione consultiva consente al Garante di fornire, a Parlamento e Governo - con audizioni o pareri, oltre 70 nell'anno - un contributo utile a delineare, sin dall'origine, norme coerenti con le garanzie richieste dalla disciplina di protezione dei dati. Nel 2023, particolarmente significativa è stata l'attività consultiva svolta rispetto all'attuazione delle riforme processuali o in materia d'istruzione, soprattutto in ragione della piena realizzazione della piattaforma "Unica".

Ancora, nell'ambito dell'istruttoria legislativa, il Garante è stato audito dalle Camere, in varie occasioni, anche (ma non soltanto) sulla disciplina dell'intelligenza artificiale, nella molteplicità delle sue implicazioni, con confronti tanto più proficui quanto più hanno determinato, come spesso accaduto, la revisione dei testi normativi o l'inclusione, nelle relazioni conclusive delle indagini conoscitive, delle indicazioni fornite.

Hanno svolto una rilevante funzione preventiva anche gli "avvertimenti", rivolti ad alcuni titolari di trattamenti suscettibili di determinare – in assenza di tempestive modifiche – violazioni della disciplina di protezione dei dati. Tra i provvedimenti adottati, rileva in particolare l'avvertimento rivolto a *Worldcoin* relativamente al progetto di scansione dell'iride in cambio di cryptovalute, che avrebbe potuto legittimare una raccolta di dati biometrici in assenza delle dovute garanzie e della necessaria consapevolezza da parte degli utenti. Inoltre sul tema, a

questo tangente, dello scambio di servizi contro dati, su cui pure si fonda l'architrave della *data economy*, il Comitato europeo per la protezione dei dati – in linea con la nostra giurisprudenza di legittimità - ha chiarito che il modello "*consent or pay*", per le grandi piattaforme, può ammettersi soltanto in quanto contempli alternative equivalenti non patrimoniali. Perché, appunto, la monetizzazione del consenso non divenga un modo per rendere la privacy un lusso per pochi.

La cooperazione internazionale – realizzata pure attraverso la partecipazione ai lavori del Comitato europeo per la protezione dei dati – ha offerto anche quest'anno l'occasione di confronti particolarmente utili, come quelli funzionali alla decisione di 1.595 procedure "Imi" e quelli che, certamente, si svilupperanno nell'ambito dei lavori del G7 dei Garanti per la protezione dei dati, organizzato per ottobre prossimo proprio dall'Autorità italiana.

La funzione di controllo e decisoria ha consentito anche – ben prima che d'irrogare sanzioni, nel 2023 riscosse per quasi 8 milioni di euro - di ingiungere misure prescrittive o inibitorie, tali da attenuare o, se possibile, prevenire gli effetti pregiudizievoli delle violazioni (soprattutto per i *data breach*, notificati nell'ordine di 2.037). La tutela remediale caratterizza, in modo particolare, l'ambito della libertà di manifestazione del pensiero, rispetto al quale le misure "correttive" rappresentano spesso l'esito elettivo di controversie sui limiti delle esigenze informative o, anche, il particolare ambito del diritto all'oblio.

Rilevante è stata anche, nell'anno trascorso, l'attività funzionale all'approvazione di due importanti codici di condotta, quali quelli, rispettivamente, per le agenzie per il lavoro e sul *telemarketing*. Il primo, in particolare, introduce alcune significative garanzie per i candidati a

posizioni lavorative, volte anche a impedire discriminazioni nell'accesso al mercato del lavoro. Le Agenzie aderenti al Codice si impegnano, in particolare, a trattare soltanto dati strettamente necessari all'instaurazione del rapporto di lavoro, senza svolgere indagini sulle opinioni politiche, religiose o sindacali dei lavoratori o effettuare preselezioni, neppure con il consenso dei candidati, sulla base di informazioni relative a scelte o condizioni di vita come stato matrimoniale, gravidanza, disabilità, non potendo neppure utilizzarsi informazioni su illeciti disciplinari o procedimenti giudiziari.

Il secondo codice di condotta potrà svolgere una funzione rilevante nella promozione del principio di responsabilizzazione, anche favorendo standard uniformi di conformità delle condotte dei vari attori coinvolti nella filiera delle attività promozionali, non realizzabili forse neppure con la deterrenza esercitata dal quadro sanzionatorio, pur elevato.

Tra le attività di promozione della consapevolezza delle esigenze di protezione dei dati, vanno segnalate anche le Linee guida per la conservazione delle *password,* adottate d'intesa con l'Agenzia per la cybersicurezza nazionale, volte a fornire raccomandazioni sulle funzioni crittografiche ritenute attualmente più sicure per la conservazione delle *password,* per evitarne la violazione e il conseguente utilizzo per furti di identità, richieste di riscatto o altri tipi di attacchi (la cui criticità raggiunge oggi la soglia dell'81% del totale, contro il 47% del 2019).

Questi pochi esempi testimoniano, almeno in parte, la complessa articolazione dei compiti del Garante che, combinando funzioni consultive, regolatorie, decisorie, di controllo e di *advocacy*, può offrire una tutela davvero integrata alla persona, nel suo rapporto altrimenti impari con la tecnologia. E può farlo contando sul costante impegno di un contingente di

personale ristretto (e meritevole di ampliamento, proporzionalmente alle crescenti competenze dell'Autorità) ma qualificato, che voglio qui, unitamente al Collegio e al Segretario generale, sinceramente ringraziare. E ringrazio anche le Autorità che hanno inteso offrirci, in vario modo, sostegno, nonché il corpo della Guardia di Finanza, per la ormai consueta collaborazione.

La collaborazione istituzionale, la relazione costante con i cittadini, la sinergia delle varie forme di tutela offerte, la cooperazione internazionale, l'alto senso di responsabilità nello svolgimento dei compiti affidati al Garante consentono di renderne la prospettiva lungimirante quanto necessaria a comprendere, prima ancora che regolare, una realtà in costante evoluzione (quasi l'eterna velocità marinettiana), come quella digitale. Soltanto guardando oltre lo stretto orizzonte del contingente si può, infatti, tutelare un diritto – come quello alla protezione dei dati – "inquieto", perché in costante dialettica con l'evoluzione tecnologica - e necessariamente mite, perché mai tiranno. E', in fondo, lo sguardo presbite che deve avere il diritto per poter regolare un futuro.

Solo con uno sguardo presbite si può regolare un futuro che, per riprendere le parole di Rainer Maria Rilke, "*entra in noi, per trasformarsi in noi, molto prima che accada*".

Vi ringrazio.