GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Il potere dell'innovazione e la solitudine digitale

La protezione dei dati a tutela della persona

Relazione del Presidente Pasquale Stanzione
2022

Roma, 6 luglio 2023

Signor Presidente della Camera,

Autorità,

Signore e Signori,

Tecnica e geopolitica

la relazione che oggi presento espone alcune delle sfide cui l'Autorità è stata chiamata nel corso di quest'anno, di particolare rilevanza sotto il profilo sociale, etico, giuridico, persino democratico; mentre altre, non meno importanti, iniziano a delinearsi con la forza delle grandi questioni epocali.

Si svolge oggi un'altra, non meno cruciale fase, di quella rivoluzione pacifica che Stefano Rodotà attribuiva all'introduzione delle prime norme sulla privacy in Italia.

Da allora, infatti, questa disciplina, adeguandosi progressivamente a una realtà in costante evoluzione, si è affermata come potente strumento di redistribuzione del potere informativo, di fronte al quale la persona rischia di divenire sempre più vulnerabile. E se ieri si trattava di "democratizzare" la privacy, emancipandola dalla dimensione tradizionalmente borghese del right to be let alone, oggi la sfida è rendere questo straordinario diritto di libertà - con l'evoluzione che l'ha caratterizzato - protagonista di uno sviluppo inclusivo e umano-centrico del digitale.

Con l'urgenza delle più forti istanze democratiche emerge infatti, progressivamente più chiara, la necessità di uno statuto, giuridico ma anche etico, delle neotecnologie, che ne promuova

massimamente lo sviluppo, ma al servizio della persona, della solidarietà, dei diritti fondamentali.

Ad oltre un anno dal ritorno, alle porte dell'Europa, dello spettro, drammatico e dimenticato, della guerra, il primato sul digitale e l'indipendenza tecnologica assumono un crescente valore strategico, anche dal punto di vista geopolitico. E' significativa l'ipotesi di divieto, al vaglio della Commissione Ue, di utilizzo delle tecnologie offerte da Huawei per lo sviluppo delle reti 5G. Le limitazioni, imposte da alcuni Governi, all'uso di piattaforme di origine cinese o il divieto statunitense di esportazione di materiale hi-tech sensibile verso Pechino esprimono anche la preoccupazione per la capacità di condizionamento, persino sotto il profilo militare, della tecnica. La guerra dei chip è, in fondo, solamente un'altra faccia della stessa, silente ma nettissima, contrapposizione tra Usa e Cina. Sembra delinearsi una nuova, ma non meno temibile, guerra fredda, sempre più "privatizzata" e ibrida, come si è detto, per l'incidenza delle big tech nelle dinamiche belliche.

E mentre sugli schermi scorrono le immagini, quasi antistoriche, di carri armati schierati tra trincee e confini contesi, cresce il non infondato timore di una delega all'algoritmo persino di quelle "tragic choices" che sono le scelte in materia militare, con sullo sfondo jet a guida autonoma e droni kamikaze. Il segretario generale delle Nazioni Unite ha espresso preoccupazione per la potenziale applicazione dell'intelligenza artificiale nel settore delle armi, auspicando la definizione di "alcune linee rosse".

L'autonomia decisionale che taluni sistemi d'intelligenza artificiale sono pronti a sviluppare preoccupa dunque, anche in campo militare, soprattutto in uno scenario internazionale ancora dominato dalla guerra. Si temono, infatti, rischi non fronteggiabili neppure con quel, pur innovativo, "codice etico" per un'intelligenza artificiale, "responsabile" in campo bellico, adottato dagli Usa già due anni fa, all'insegna della trasparenza e della supervisione umana.

Matura così, anche sulla base di questi timori l'intenzione americana, come quella degli Stati riuniti al G7 di fine maggio, di voler regolare l'aspetto forse più dirompente delle neotecnologie: l'intelligenza artificiale appunto, già oggetto, in Europa, di una proposta di regolamento in fase avanzata di discussione. Ancora una volta l'"effetto Bruxelles", la vis attractiva di molte norme europee promuove, come già per il Gdpr in questi cinque anni di applicazione, una spinta globale alla regolazione delle neotecnologie. E non certo per una pretesa egemonia culturale del vecchio continente né, probabilmente, per la deterrenza delle sanzioni previste in caso di violazione delle norme europee che, con efficacia parzialmente extraterritoriale, si applicano (tanto per la protezione dei dati quanto per l'intelligenza artificiale) a chiunque si rivolga al mercato europeo.

La forza attrattiva delle norme europee deriva, piuttosto, dalla lungimiranza delle sue scelte, con quello sguardo anticipatore proprio, anche etimologicamente, della figura emblematica del dominio della tecnica: Prometeo. Il governo del digitale e la regolazione dei dati assumono, così, una valenza geopolitica strategica, capace di riorientare assetti di potere

consolidati. Lo dimostrano gli effetti della sanzione irrogata dal Garante irlandese a Meta e la complessità della definizione dell'accordo per il trasferimento dei dati negli Usa, su cui si gioca una partita importante anche in termini di politica internazionale.

Il diritto alla protezione dei dati ma, più in generale, la tutela della persona rispetto al potere della tecnica necessita di una garanzia universale, che superi asimmetrie normative del tutto inadeguate a una realtà, come quella digitale, che prescinde dal limite territoriale.

Verso il futuro

In tale contesto l'Europa, prima nel mondo, si avvia a disciplinare l'intelligenza artificiale per renderla "trustworthy", affidabile. E' una scelta importante in sé, soprattutto in un contesto in cui la frequente tendenza alla deregulation finisce con il delegare alla legge del mercato e al potere dell'innovazione, insofferente ai limiti, la definizione del perimetro di diritti e libertà.

Quest'opzione caratterizza tutta la politica europea del digitale, dal Gdpr sino ai più recenti Data Governance, Digital Services e Digital Markets Act, accomunati dall'esigenza di riequilibrare il rapporto tra Stato e mercato, persona e tecnica, libertà e innovazione.

Anche nel metodo, la regolazione europea delinea un modello notevolmente distante, tanto da quello liberista americano, quanto da quello statalista cinese, regolando non la

tecnica, ma i suoi vari usi, in una prospettiva il più possibile "future-proof".

La convergenza tra innovazione e libertà si realizza nella tassonomia dei livelli di rischio dei vari usi dell'intelligenza artificiale, sino a quelli vietati perché potenzialmente idonei a violare la dignità umana o amplificare le discriminazioni dalle quali, invece, proprio le macchine avrebbero dovuto liberarci. Di qui, ad esempio, il divieto di ricorso alle tecniche subliminali o intenzionalmente manipolative, tali da sfruttare le vulnerabilità soggettive o a sistemi di social scoring.

Anche se pensate per favorire l'inclusione offrendo prestazioni sociali ai soggetti più svantaggiati, per eterogenesi dei fini queste applicazioni rischiano invece **-** come dimostra il sistema antifrode olandese Syri - di determinare ulteriore divario sociale, anche per effetto di discriminazioni algoritmiche sempre più opache e, dunque, difficili da individuare. La classificazione delle persone in base al comportamento sociale, alla condizione socio-economica, alle caratteristiche soggettive, già di per sé problematica, lo diviene ancor più se affidata a un algoritmo, con bias che possono caratterizzarlo (per scarsa inclusività e sub-rappresentatività del set di dati su cui si è formato), distorcendone l'esito. Se ne è occupato anche il Garante, rispetto ad iniziative locali volte all'erogazione di benefici sulla base di meccanismi di scoring associati a comportamenti "virtuosi" del cittadino in vari settori. Peraltro, come dimostrano il Social credit system cinese e il, pur diverso, Gosuslugi russo, il monitoraggio centralizzato dell'accesso alle prestazioni sociali necessita di cautele, tali da evitarne la degenerazione in una forma di controllo

sociale panottico, se non, addirittura, di totalitarismo digitale. Per altro verso, l'utilizzo dell'i.a. nel campo della ricerca è agevolato e tanto più potrà essere valorizzato grazie alla possibilità di condivisione dei dati a fini solidaristici e, appunto, di promozione della ricerca consentita dal Data Governance Act, con l'innovativo istituto dell'altruismo dei dati.

Il Regolamento sull'intelligenza artificiale ha introdotto limiti rigorosi rispetto alla congiunzione tra potere investigativo e potenza della tecnica, che impone condizioni tanto più stringenti quanto più avanzato sia il grado d'autonomia decisionale della macchina. Così, oltre ai sistemi di polizia predittiva e rilevazione delle emozioni, il divieto si è esteso al riconoscimento facciale, in luoghi pubblici.

L'utilizzo dell'intelligenza artificiale nel settore investigativo necessita, infatti - come chiarito anche dal Garante - di cautele tali da scongiurare il rischio della delega all'algoritmo - tutt'altro che immune da errori - di attività potenzialmente incidenti sulla libertà personale e della sorveglianza massiva. Ciò che si teme non è tanto e non è solo il "pendio scivoloso", quanto la tendenza all'acritica accettazione sociale di una progressiva limitazione della libertà.

L'uomo di vetro

Tra le garanzie necessarie per impedire effetti socialmente regressivi dell'intelligenza artificiale, quelle già sancite dalla disciplina di protezione dei dati – dal divieto di uso discriminatorio al diritto alla spiegazione oltre, appunto, al principio di

proporzionalità - rappresentano un presidio essenziale. E concorrono alla definizione del limite che l'uomo deve saper (op)porre alla tecnica, il diritto al potere, la democrazia all'ideologia del controllo.

Il caso Chat Gpt è, in questo senso, significativo. L'intervento del Garante ha, infatti, consentito di indirizzare lo sviluppo di questa forma d'intelligenza artificiale generativa in una direzione compatibile con la tutela della persona, contrastando lo sfruttamento di quei frammenti dell'io che sono i dati personali.

La loro protezione è protezione della libertà e della dignità della persona, tanto più quando sono coinvolti i minori, con la comprensibile voglia, propria di quella fase della vita, di fare esperienza di tutto, anche di ciò che è troppo più grande di loro. Importante anche, in questo senso, il provvedimento adottato nei confronti del chatbot Replika, presentato addirittura come una sorta di amico virtuale, capace di migliorare il benessere emotivo dell'utente, con un'incidenza psicologica potenzialmente significativa su soggetti, come i minori, dalla personalità ancora in formazione.

In entrambi i casi su descritti, l'uso dell'intelligenza artificiale, non presidiato da alcune necessarie garanzie, avrebbe esposto gli utenti, soprattutto se minori, a rischi non irrilevanti.

Nell'esigere il rispetto degli obblighi di trasparenza, di verifica dell'età e di liceità del trattamento, il Garante ha infatti potuto sollecitare l'attenzione (non solo europea) sulla necessità che il progresso non si affermi in danno della persona,

limitandone la libertà e sacrificando i diritti sul terreno del mercato, ma promuova invece un ragionevole equilibrio tra iniziativa economica, innovazione, tutela della persona.

Questo vale anche per le ulteriori frontiere dell'intelligenza artificiale nel campo, ad esempio, delle neuroscienze, dove si è realizzato un decoder "semantico" dell'attività neurale a partire dai dati forniti da una risonanza magnetica funzionale, combinando scansione cerebrale e database di modelli linguistici, come quelli usati da Chat Gpt. E' recente, peraltro, l'autorizzazione resa a una nota società dal competente ente regolatorio statunitense, all'avvio dei test per impiantare un chip nel cervello umano, per aiutare alcuni pazienti neurologici a comunicare direttamente con un device esterno, attraverso il pensiero. 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 con l'adozione di ogni misura necessaria a impedire derive post-umaniste.

L'applicazione dell'intelligenza artificiale in campo neuroscientifico e, soprattutto i sistemi di brain reading, idonei almeno potenzialmente a decodificare il pensiero, devono infatti sempre garantire, come primo dei "neurodiritti", la privacy mentale, condizione ineludibile di autodeterminazione, presupposto intangibile di libertà. Varcata la soglia della lettura del pensiero, la deriva da impedire è rendere la persona un archivio liberamente accessibile, le cui idee siano messe a nudo senza più alcuno spazio per la libertà, anzitutto di determinazione.

Mai come in questo caso, alla infinita volontà di potenza della tecnica, a ciò che si è definito il “playing God”, deve porsi un indirizzo e un limite, etico e giuridico, a tutela della dignità della persona. Il rischio, altrimenti, è che le tecniche divengano sempre più opache, mentre le persone sempre più trasparenti, secondo l’idea dell’uomo di vetro cara a sistemi tutt’altro che democratici.

Rischi non meno trascurabili pone il metaverso, destinato ad avere implicazioni dirimenti sulla società e sulla stessa antropologia contemporanea. L’esperienza immersiva e totalizzante che esso consente, rendendo l’utente protagonista e non solo fruitore del suo mondo, avrà un impatto non trascurabile sul rapporto tra uomo e tecnica. Alcuni ricercatori prefigurano, addirittura, un’ibridazione così profonda tra reale e virtuale nella percezione degli utenti, da potersi ipotizzare persino delle “cyberemozioni”, in grado di trasformare l’esperienza soggettiva.

Molto delle sue potenzialità e dei suoi rischi dipenderà da come verrà strutturato, se cioè sarà terreno di conquista dei soli big tech, riproducendo l’oligopolio del capitalismo digitale, se sarà open source o se invece vedrà una presenza, da definire nei modi e nelle forme, del pubblico. Certo è che la concentrazione di dati che comporterà questa vera e propria società della simulazione, dovrà essere bilanciata da responsabilità rilevanti delle piattaforme. L’impostazione tecnologicamente neutra del Gdpr potrà fornire una regolazione tendenzialmente completa sui principali aspetti di questo mondo nuovo. Ma emergeranno certamente nuove istanze di tutela, a fronte di vulnerabilità e persino soggettività nuove, come quella del gemello digitale in cui

si proietterà il nostro io o nuovi tipi di dati, quali quelli inferiti dalle interazioni on-line, suscettibili di esprimere stati emotivi, cui dovrà accordarsi una particolare "privacy relazionale".

Ma, rispetto al metaverso, andranno adottate tutte le misure necessarie ad impedire un'eccessiva dipendenza, soprattutto dei giovani, da questa dimensione quasi onirica, capace di alienarli dalla realtà e di svincolarli dal rapporto con essa, proiettandoli nello spazio dell'infinitamente possibile.

La solitudine digitale

Quello dello straniamento è, del resto, un rischio tutt'altro che remoto se si considera il fenomeno, sempre crescente, della violenza non solo assistita in maniera del tutto inerte, ma addirittura filmata e poi esibita sul web. Poche settimane fa, a Napoli, un bambino di dodici anni è stato massacrato di calci e pugni, mentre il branco riprendeva il pestaggio, per poi "esibirlo", come macabro trofeo, in rete. Mesi prima, a Civitanova Marche, un uomo è stato ucciso a bastonate mentre i passanti si limitavano a riprendere quel dramma con il telefono. Ebbene, questo inerte osservare la violenza, con il telefono in mano, non può non interrogarci, come singoli e come istituzioni. Ed esige una riflessione la ricerca spasmodica, da parte dei giovani, di una "visibilità" sui social spinta sino al punto di mettere a rischio la vita degli altri.

Si rischia così troppo spesso di divenire spettatori inerti del male o, come nel recente caso di cronaca, di sacrificare la vita di un bambino per un like in più. Se tutto ciò è frutto dell'alienazione

dal reale cui può condurre la sempre più marcata traslazione on line della vita, è prioritario ricostruire una coscienza comune che tenga conto degli effetti, sulle relazioni, della digitalizzazione di tutto.

Se confondiamo la persona con la sua immagine, se non interveniamo sul male che si compie, ma lo filmiamo, rinunciamo a cogliere, della tecnica, le sue straordinarie potenzialità inclusive e ci condanniamo a un'inconsapevole solitudine digitale, celata da una malintesa idea di connessione totale. Perché, nel rapporto impari con la tecnica e la sua potenza geometrica, la più grande vulnerabilità della persona (soprattutto, ma non solo minorenne) è la sua solitudine, il suo confrontarsi, quasi inerme, con un potere che rischia di divenire insindacabile e totalizzante, più dei vecchi arcana imperii.

La disciplina di protezione dei dati mira a colmare questo vuoto, riequilibrando il rapporto tra uomo e tecnica nel segno della tutela dei diritti e delle libertà. Proprio il caso Chat Gpt (rispetto al quale l'intervento dell'Autorità ha fornito l'impulso per la costituzione di una task force a livello europeo) dimostra come il dialogo con il Garante, lungi dal "bloccare" l'innovazione, possa orientarla verso una direzione compatibile con la tutela della persona e dei suoi diritti.

E questo anche rispetto a un'altra accezione della solitudine digitale: l'autismo informativo e relazionale cui, paradossalmente, ci costringe la rete, relegandoci in "filter bubbles" alimentate dei soli contenuti ritenuti affini al profilo di utente stilato, con il pedinamento digitale, dall'algoritmo. Questa

presentazione selettiva della realtà (il fenomeno del “Daily me”, la personalizzazione algoritmica della rete), può produrre intolleranza a tutto ciò che è diverso da noi, distorsioni significative sul processo di formazione dell’opinione pubblica, sempre più polarizzata su opposti estremismi. La crisi della democrazia scomparsa è, non a caso, correlata da Byung Chul Han proprio alla scomparsa dell’”Altro” e, quindi, alla “crisi dell’ascolto” indotta dalla dinamica autoreferenziale della rete: “il like esclude qualsiasi rivoluzione”.

Ed è significativo che nell’Artificial Intelligence Act i sistemi di raccomandazione con valenza condizionante le scelte elettorali siano compresi tra quelli ad alto rischio, per gli effetti potenzialmente distorsivi sulle garanzie democratiche che possono avere, come insegna il caso Cambridge Analytica, già oggetto, anni fa, di un provvedimento sanzionatorio del Garante. Un ulteriore intervento dell’Autorità ha invece riguardato la funzione Election day information offerta da Meta in occasione delle scorse elezione politiche. Il trattamento di dati ad essa correlato è stato oggetto di un provvedimento di limitazione (successivo a un avvertimento), per l’assenza di garanzie e della necessaria trasparenza rispetto all’utilizzo di dati potenzialmente anche espressivi dell’orientamento politico del cittadino, peraltro in un momento, quale quello dell’esercizio del diritto di voto, centrale nelle dinamiche democratiche.

Un’ulteriore criticità del capitalismo delle piattaforme riguarda la tendenza alla remunerazione del consenso al trattamento dei dati personali, assunto come parte di uno scambio tra dati e servizi. Il Garante se ne sta occupando, in

particolare, nell'ambito dell'istruttoria, avviata lo scorso autunno, sull'uso dei cookie wall da parte di molte testate giornalistiche on-line, che subordinano l'accesso ai contenuti alla prestazione del consenso ad attività di profilazione o, alternativamente, al pagamento di un prezzo. Per non derubricare i dati personali, oggetto di un fondamentale diritto di libertà a mera risorsa economicamente sfruttabile, va delineato un confine tra data-economy e monetizzazione della privacy, con tutti i rischi, in termini di libertà ed eguaglianza, suscettibili di derivarne, come abbiamo avuto modo di sottolineare anche al Senato, in audizione sul recepimento della direttiva "omnibus". Benché il modello capitalistico attuale (non meno "estrattivo" del suo archetipo) si fondi sempre più sulla deduzione dei dati nel sinallagma negoziale, bisogna evitare ogni deriva che renda la privacy un lusso per pochi, contraddicendo quel percorso che l'ha resa, da tradizionale prerogativa borghese, uno straordinario presidio di tutela di tutte e tutti, soprattutto dei più vulnerabili.

Per altro verso si diffondono, con incredibile viralità, notizie false e immagini artefatte, che si finisce con il credere vere per quel meccanismo autoconfermativo che fa dipendere l'attendibilità non dalla verificabilità del contenuto, ma dalla quantità di condivisioni ottenute: dalla sua diffusività e non dalla sua intrinseca veridicità. Il DSA – parallelamente al DMA - introduce una responsabilizzazione complessiva delle piattaforme, anche sotto il profilo della trasparenza, rilanciando la scommessa europea di regolare la rete senza limitarne la libertà, proprio quando la Corte suprema americana conferma l'immunità (pur condizionata) delle piattaforme rispetto alla

responsabilità per i contenuti diffusi dagli utenti. Le norme europee da poco approvate disciplinano, con un ragionevole equilibrio tra libertà di espressione, di iniziativa economica e tutela degli utenti gli obblighi di trasparenza delle piattaforme e le garanzie da accordare nell'attività di moderazione e raccomandazione. Significativi sono, in particolare, le limitazioni poste alle possibilità di combinazione di dati da fonti diverse, gli obblighi informativi sulla pubblicità e sui sistemi di raccomandazione, i divieti di pratiche di autopreferenza e di inserzioni pubblicitarie basate sulla profilazione di utenti minori, le misure di prevenzione della pubblicità occulta, capace di condizionare fortemente scelte e comportamenti individuali.

Queste distorsioni dell'informazione e delle relazioni in rete, l'eclissi del reale, sono tanto più pregiudizievoli per chi, come i giovani, non dispone ancora delle risorse cognitive e del senso critico per discernere le notizie vere dalle fake news, la critica dall'hate speech, la nuova amicizia dal grooming. I giovani fanno esperienza del mondo soprattutto tramite il web, senza tuttavia disporre degli strumenti per comprenderlo e spesso imbattendosi, da soli, in contenuti inadatti alla loro età, con attitudine manipolativa.

Così, ad esempio, relazioni intrattenute sui social possono determinare il coinvolgimento del minore in sfide potenzialmente anche letali, nella cessione di scatti intimi poi utilizzati a fini estorsivi, in incontri pericolosi, non più solo virtuali. Solo quest'anno, sono stati ben 4618 i casi trattati dal Centro Nazionale per il Contrasto della Pedofilia Online relativi ad adescamento, pedopornografia e altri reati correlati all'abuso

sessuale, tecnomediato, di minori. 430 sono risultati, invece, i casi di adescamento online, di cui ben 264 in danno di infratredicenni. Tra il 2021 e il 2022, la circolazione di materiale pedopornografico autoprodotto è cresciuta, a livello internazionale, del 374% rispetto ai livelli pre-pandemici, in virtù anche del maggior uso della rete da parte dei minori.

Le infinite possibilità d'interazione, non sempre positive, consentite dai social network eludono così, spesso, le cautele preposte dai genitori nel mondo off-line, con la selezione della cerchia di amici di riferimento, dei contesti e delle attività consentite al minore, delle sue possibilità di scelta autonoma.

Le straordinarie opportunità di crescita, di informazione, di conoscenza offerte dalla rete si affiancano così a pericoli che si amplificano, in misura esponenziale, quanto più piccoli e, dunque, tendenzialmente immaturi siano gli utenti delle piattaforme. Stabilire la soglia di accesso autonomo dei minori alla rete diviene, dunque, tema cruciale per impedire i rischi della "solitudine digitale" e, quindi, dell'esposizione del minore a contenuti potenzialmente lesivi per lo sviluppo della sua personalità, senza neppure la mediazione degli adulti di riferimento. Ora, non si tratta di proibire l'uso dei social (le cui potenzialità emancipatrici sono simboleggiate ad esempio dall'ausilio che hanno, in vario modo, fornito al movimento femminista iraniano) ma, certamente, di renderlo più sicuro; per i minori innanzitutto.

La disciplina di protezione dei dati offre, sotto questo profilo, un presidio importante, di cui va garantita effettività

soprattutto grazie a sistemi di age verification che, pur non comportando una schedatura dei minori, assicurino adeguata verifica dell'età, anche incaricando di ciò terze parti affidabili. In questa direzione si muove, ad esempio, il tavolo istituito con il recente protocollo d'intesa tra Garante ed Agcom, per la promozione di un codice di condotta relativo ai sistemi per la verifica dell'età delle piattaforme.

La tutela preventiva assicurata dall'age verification è, del resto, il necessario complemento della tutela remediale accordata dal Garante, in particolare rispetto al cyberbullismo e al revenge porn**,** che si conferma essere un presidio essenziale per ragazze e ragazzi vittime di un uso violento della rete, purtroppo anche da parte dei loro coetanei. Proprio in ragione della sua efficacia questa misura, caratterizzata peraltro da una procedura rapida come richiedono i tempi contratti del web, potrebbe essere estesa – come si era proposto nella scorsa legislatura e come si è suggerito alla Camera - ai contenuti istigativi all'autolesionismo. In tal modo, infatti, si potrebbe limitare il rischio di coinvolgimento dei minori in sfide pericolose, che troppo spesso hanno indotto adolescenti e, persino, bambini, a scelte fatali.

Strategie integrate

In quest'anno, il Garante si è misurato con la sfida di rendere la protezione dei dati un obiettivo da raggiungere anche con attività di indirizzo e impulso, nella consapevolezza dell'importanza di promuovere questo diritto come fondamento di una civiltà digitale matura.

Così, a fronte del tradizionale strumento sanzionatorio e correttivo, applicato in 317 casi, l'Autorità ha valorizzato anche la funzione consultiva e, lato sensu, d'indirizzo, volta alla promozione della protezione dei dati anzitutto come "cultura", insieme di diritti ed obblighi costitutivi, oggi, della cittadinanza.

Particolarmente rilevante, in tal senso, è il settore lavoristico, nel quale l'attività consultiva ha affiancato, su temi importanti, quella di tipo correttivo. Per un verso, infatti, si è sanzionato l'accesso datoriale alla mail dell'ex dipendente, non giustificabile né con l'interesse a mantenere i rapporti con i clienti né con l'esigenza di tutela giurisdizionale dei diritti in sede contenziosa. Analogamente, è stata sanzionata la rilevazione biometrica della presenza dei propri dipendenti da parte di una società sportiva, in assenza di ragioni idonee a giustificare la raccolta sistematica di dati, quali appunto quelli biometrici, cui l'ordinamento accorda una tutela rafforzata.

Per altro verso, però, il Garante ha fornito indicazioni particolarmente importanti sulle garanzie lavoristiche alla luce delle innovazioni introdotte dal c.d. "decreto trasparenza", n. 104 del 2022. Si è, in particolare, chiarito come il dipendente abbia diritto di conoscere i principali parametri utilizzati per programmare i sistemi automatizzati, anche di valutazione delle prestazioni e come il ricorso a sistemi particolarmente invasivi, quali il machine learning, il rating e ranking, presenti notevoli criticità per la libertà e dignità del lavoratore. Il ricorso intensivo alle neo-tecnologie nel contesto lavorativo (già cresciuto esponenzialmente con la pandemia) non può, infatti, rappresentare l'occasione per eludere le essenziali garanzie di

autodeterminazione, frutto delle più antiche conquiste raggiunte per il lavoro tradizionale, quasi come in un nuovo neotaylorismo digitale.

Una significativa convergenza di misure correttive e d'indirizzo è stata realizzata anche sul terreno - quantomai cruciale per la democrazia - del giornalismo e, in particolare, della cronaca giudiziaria, che deve poter sempre coniugare diritto di (e all') informazione e dignità. Anche lo scorso anno il Garante ha dovuto richiamare i media, al rispetto di un ragionevole equilibrio tra queste due istanze, non indulgendo alla spettacolarizzazione soprattutto rispetto alla cronaca giudiziaria. Così, è stato necessario sanzionare la divulgazione, da parte di una testata giornalistica, di immagini fotosegnaletiche o di analogo tenore, di soggetti fermati. Per altro verso, rispetto ad alcuni eccessi riscontrati nella cronaca della cattura di un noto latitante, si è richiamata l'esigenza del rispetto del principio di dignità della persona e di essenzialità dell'informazione, che impongono di astenersi dalla rivelazione, certamente lesiva, di dettagli non rilevanti ai fini informativi, tanto più quando attengano a patologie di cui soffra il soggetto.

Una strategia integrata peculiare ha richiesto, anche, il telemarketing illegale, endemico per diffusione e radicamento nelle strutture economico-sociali; spesso la "spia" di un più complesso sistema d'illegalità e concorrenza sleale. L'estensione alle utenze mobili del registro delle opposizioni, a partire da luglio scorso, ha solo in minima parte arginato il problema senza, tuttavia, risolverlo, anche per l'incidenza dello "spoofing", capace di eludere il sistema di garanzie previsto. In tale contesto sono

state irrogate sanzioni anche elevate (una di 4.900.000 euro, a un'importante società del settore energetico), in presenza di violazioni connesse a una più generale condizione di inosservanza sistemica degli obblighi propri del titolare. E' stata anche disposta, per la prima volta, la confisca di banche dati illecitamente costituite, da parte di società aduse allo sfruttamento sistematico dei dati dei cittadini.

Ma, quale misura destinata ad avere un'efficacia maggiore nel lungo periodo, il Garante ha promosso un codice di condotta per gli operatori del settore, che in ragione della sua maggiore efficacia conformativa potrebbe risultare persino più risolutivo della deterrenza sanzionatoria. E questo soprattutto se, parallelamente, si prestasse, da parte dei consumatori, maggiore attenzione alla prestazione del consenso al trattamento dei dati a fini promozionali.

Inoltre, al fine di agevolare l'accesso alla tutela accordata dal Garante, si è predisposto uno specifico servizio telematico per la segnalazione di telefonate indesiderate, risultato particolarmente utile se si considera che, in un solo mese, ha ricevuto quasi 11.000 segnalazioni.

Il Garante ha peraltro offerto, anche quest'anno, un contributo significativo rispetto alle misure attuative del PNRR e, in particolare, al processo di delineazione dell'architettura digitale del Paese, nella consapevolezza dell'esigenza, oggi più forte ancora di ieri, di rendere meno permeabile e, quindi, meno vulnerabile la frontiera digitale. E' significativo che, come osserva il Clusit, proprio nell'anno dell'avvio della guerra in Ucraina sia

stato registrato il valore più alto di attacchi cyber a livello globale, con impatto critico nell'80% dei casi. L'Italia e' risultata, secondo l'Agenzia per la Cybersicurezza nazionale, tra i Paesi maggiormente interessati dalla diffusione generalizzata di malware e da attacchi cibernetici mirati. Il settore sanitario (il terzo per numero di cyber attacks) ha registrato, secondo le stime di Ibm, il costo medio più alto per violazione, destinato probabilmente anche a crescere per effetto dell'affinamento delle tecniche intrusive. Proprio per la sua centralità nella strategia di difesa cibernetica del Paese, quello sanitario è stato uno dei settori oggetto di particolare attenzione da parte del Garante, anche nell'ambito dell'attività conseguente alla comunicazione di data breach. Essa è, infatti, spesso il fattore propulsivo di un'azione di controllo e di riorganizzazione nel segno della resilienza informatica, come dimostrano anche i recenti attacchi subiti da alcune aziende sanitarie locali e le attività successivamente intraprese.

Anche per questo, il dialogo con il Governo sull' Ecosistema Dati Sanitari (e parallelamente sul FSE) è stato particolarmente articolato e ha richiesto modifiche progressive.

Rispetto al FSE, è stato peraltro necessario chiarire che l'inserimento, al suo interno, del referto sulla sieropositività è subordinato alla comunicazione dell'esito dell'esame al paziente, di persona. Il processo di digitalizzazione non può, infatti, determinare l'elusione di garanzie fondamentali nel rapporto terapeutico.

Specifiche indicazioni sono state fornite anche rispetto alla piattaforma per l'erogazione dei benefici economici ai cittadini che, in quanto destinata a raccogliere informazioni su aspetti, anche i più delicati, della vita quotidiana dell'intera popolazione, va protetta dal rischio di usi impropri e accessi abusivi.

Le campagne di comunicazione istituzionale (in particolare quella rivolta alle scuole e quella, più generale, sulle garanzie di sicurezza) hanno svolto, peraltro, un ruolo centrale nell'attività di quest'anno, nella convinzione di quanto più efficace della sanzione possa essere la promozione della consapevolezza dell'importanza di proteggere i nostri dati, per rendere la tecnica alleata della libertà e della democrazia.

Il processo, le parti, i terzi

Particolarmente rilevante è stata, nell'anno trascorso, l'attività consultiva svolta dal Garante in relazione alle riforme in materia di giustizia.

Sul versante processuale, civile e penale, le modifiche introdotte hanno, in primo luogo, promosso una rilevante digitalizzazione di attività e flussi informativi, che tanto più garantirà efficienza quanto più potrà assicurare l'effettiva protezione dei dati personali delle parti e dei terzi coinvolti. La riforma del processo penale, poi, ha introdotto alcune importanti innovazioni che il Garante ha contribuito a migliorare. In primo luogo rileva l'oblio per i destinatari di provvedimenti di archiviazione e proscioglimento, realizzato nella forma della deindicizzazione preventiva o successiva, alla pubblicazione, di

questi atti. Si tratta di misure volte a circoscrivere gli effetti della pubblicità del provvedimento giurisdizionale, mediante la limitazione della sua reperibilità attraverso i motori di ricerca. Esse – anche grazie alle indicazioni fornite dal Garante - coniugano tutela della dignità, presunzione d'innocenza ed esigenze informative, secondo una direttrice analoga a quella sottesa al d.lgs. 188 del 2021.

Ma la protezione dati è anche presupposto d'efficacia di un altro degli istituti innovativi della riforma, alla cui definizione il Garante ha fornito un contributo importante: la giustizia riparativa. La riservatezza dei colloqui in cui si articola il percorso riparativo- e dunque, garanzie elevate di protezione dei dati - è, infatti, il presupposto necessario per il buon esito di questa giustizia dell'ago e del filo capace, si è detto, di abbandonare i tre simboli tradizionali della spada, della benda e della bilancia. Il Garante, nel parere sullo schema di decreto legislativo e, poi, di regolamento attuativo, ha infatti fornito indicazioni per assicurare che i programmi rappresentino uno spazio franco, in cui favorire il più ampio confronto tra imputato e vittima, in virtù delle garanzie di riservatezza e confidenzialità accordate.

Per altro verso, il Garante ha anche fornito il proprio contributo nell'ambito dell'indagine conoscitiva condotta, dalla Commissione giustizia del Senato, sulla disciplina delle intercettazioni. In quella sede si è, in particolare, sottolineato come le vere innovazioni delle riforme recenti siano state la previsione di criteri di essenzialità nella redazione dei brogliacci o nella citazione delle conversazioni nei provvedimenti cautelari e la devoluzione delle conversazioni irrilevanti o inutilizzabili all'

archivio riservato, con l'applicazione del regime del segreto d'ufficio e sanzioni rilevanti in caso di diffusione. L'effettiva impenetrabilità dell'archivio rappresenta, pertanto, il punto di forza della disciplina vigente, che va però concretizzato con misure realmente idonee a impedire la circolazione extraprocessuale delle intercettazioni irrilevanti. Per questo, l'archivio in cui esse sono custodite dev'essere protetto adeguatamente, con misure indicate da tempo dal Garante e che devono rappresentare lo standard uniforme di garanzia per ciascun ufficio giudiziario.

Bisogna investire su queste soluzioni per coniugare esigenze di giustizia, diritto di difesa, privacy e informazione, senza che nessun interesse sia tiranno rispetto all'altro. Importante è anche la possibilità di ottenere la rettifica o la cancellazione di propri dati illegittimamente trattati in sede processuale, che può offrire una tutela significativa ai terzi le cui conversazioni siano state intercettate e riportate in atti processuali, in maniera scorretta o eccedente. Anch'essa, tuttavia, andrebbe valorizzata con la previsione – già proposta nelle scorse legislature - di un onere comunicativo, a carico del Pubblico ministero, che informi il terzo dell'esistenza, negli atti processuali, di proprie conversazioni, per consentirgli di attivare la specifica tutela prevista.

Più complesso è il tema della pubblicazione, in violazione del segreto (meramente) esterno ex art. 114, c. 2 cpp, di stralci spesso ampi di conversazioni captate. Benché questo divieto sia posto a tutela non tanto della privacy quanto della neutralità conoscitiva del giudice, la sua violazione (che ben può ledere la riservatezza) integra comunque un trattamento illegittimo di dati

personali. Ad esso si applicano rilevanti sanzioni amministrative previste dalla disciplina di protezione dei dati, che possono svolgere una rilevante funzione deterrente rispetto alla divulgazione acritica e indiscriminata delle conversazioni captate, ben oltre le reali esigenze di cronaca (il giornalismo "di trascrizione" di cui parla taluno).

Per quanto invece concerne le intercettazioni mediante captatori, le potenzialità intrusive di tali strumenti impongono uno scrutinio rigoroso di proporzionalità nel rapporto tra esigenze investigative e privacy. Esso deve orientare non solo la definizione del perimetro, oggettivo e soggettivo di ammissibilità di tali captazioni, ma anche l'adozione di alcune garanzie essenziali, modulate sulla capacità d'incidenza, sul nucleo intangibile della vita privata, di un mezzo potenzialmente ubiquitario e dalle operazioni non agevolmente predeterminabili.

Tali garanzie devono, in particolare, salvaguardare la funzione investigativa delle intercettazioni impedendone, però, la degenerazione in mezzi di sorveglianza eccessivamente ampia o, per converso, in fattori di moltiplicazione esponenziale delle vulnerabilità del compendio probatorio, reso inevitabilmente permeabile se allocato in server non sicuri o, comunque, posti al di fuori dei confini nazionali.

Si potrebbe dunque ipotizzare un divieto di utilizzo almeno delle meno garantite modalità di uso dei captatori, mediante software che non siano inoculati direttamente sul dispositivo-ospite, ma scaricati da piattaforme liberamente accessibili a tutti o, per altro verso, con archiviazione cloud in server posti fuori dal

territorio nazionale. Si dovrebbe, inoltre, vietare il ricorso a captatori idonei a modificare il contenuto del dispositivo ospite e a cancellare le tracce delle operazioni svolte. Ai fini della corretta ricostruzione probatoria, del diritto di difesa e della stessa privacy è, infatti, indispensabile disporre di software idonei a ricostruire, nel dettaglio, ogni attività svolta sul sistema ospite e sui dati ivi presenti, senza alterarne il contenuto, con una verbalizzazione analitica delle operazioni compiute.

Quest'esigenza è tanto più indispensabile rispetto ad operazioni investigative, come quelle in esame, ad alto tasso di esternalizzazione e che come tali presentano maggiori vulnerabilità, essendo in larga parte affidate a privati che devono, quindi, essere adeguatamente responsabilizzati rispetto agli obblighi di sicurezza da garantire.

Come sottolineato anche dal Procuratore della Repubblica di Milano, andrebbe peraltro specificamente disciplinato (con l'estrazione dei soli contenuti essenziali e la tempestiva restituzione) il sequestro dei dispositivi elettronici, ormai porta d'ingresso per la parte più intima della nostra vita privata. Non a caso la Corte suprema americana, nel 2014, vi ha esteso le garanzie tradizionalmente previste per le misure limitative della libertà personale, con un significativo parallelismo tra habeas corpus e habeas data.

Infine, l'orientamento della CGUE ormai consolidato (nell'ultimo anno con tre nette sentenze) sull'inammissibilità della data retention generalizzata - legittima solo se e in quanto "mirata" (ovvero delimitata, soggettivamente, oggettivamente e

cronologicamente) o rapida - imporrebbe una revisione della disciplina interna. La pur recente e condivisibile riforma operata con il d.l. 132 del 2021 si è, infatti, limitata a recepire, dei principi europei, l'esigenza di terzietà dell'organo titolare del potere autorizzatorio continuando, tuttavia, a prevedere - pur a fronte di una differenziazione per titolo di reato in fase acquisitiva - la conservazione preventiva e generalizzata dei dati di traffico relativi alla generalità indistinta dei cittadini.

Corpo e identità

La protezione dei dati incrocia anche altre e nuove istanze di tutela, legate al corpo, alle sue fragilità, alla soggettività e alle relazioni che esprime. Il corpo è del resto, con le parole di Nietzsche, una grande "regione, una pluralità con un solo senso (...) un possente sovrano, un saggio ignoto".

Tra le molteplici istanze legate al corpo l'oblio oncologico assume una rilevanza particolare. Pazienti ormai da tempo guariti si vedono negare la concessione di mutui a lungo termine, mutare radicalmente le condizioni di assicurazione, affievolirsi la possibilità di stipulare un contratto di lavoro o persino di adottare un bambino. Sembra insomma, come si è scritto, che sia possibile guarire dalla malattia, ma impossibile liberarsi del suo stigma, come se proiettasse la sua ombra sulla vita futura del paziente.

Proprio per questo; per impedire che la persona sia risolta nella sua malattia, il Parlamento europeo ha raccomandato agli Stati membri l'adozione di norme (già presenti in alcuni Paesi) che vietino la richiesta di informazioni sulle patologie pregresse,

dopo un tempo ragionevole in assenza di recidive. L'introduzione, nel nostro ordinamento, di norme analoghe – proposte in vari progetti di legge, già dalla scorsa legislatura – contribuirebbe a garantire il diritto della persona di prescindere dal male che ha sofferto.

Per altro verso, la vicenda del piccolo Enea richiama l'esigenza di dare seguito al monito rivolto, da tempo, dalla Corte costituzionale al Parlamento, sul bilanciamento tra diritto del nato alla ricerca delle proprie origini e anonimato materno. Di tale istituto, indispensabile per la garanzia del diritto della donna a una maternità effettivamente libera, va infatti superata quell'irreversibilità che finisce, paradossalmente, per privare la madre della possibilità di rivedere, se del caso, la propria scelta e il figlio dell'opportunità di cogliere tale disponibilità. Per questo la Corte ha sollecitato il legislatore a introdurre una procedura che consenta l'eventuale incontro della volontà del figlio di ricercare la madre e quella di costei di rivedere, in piena autonomia, la propria scelta passata, garantendo la riservatezza di ciascuno.

Sarebbe opportuno, dunque, riprendere l'esame dei progetti di legge in materia (alcuni dei quali, peraltro, attribuivano al Garante la gestione di tale procedura), soprattutto garantendo un'estrema riservatezza nella comunicazione di dati così importanti. La loro rivelazione può rompere, anche traumaticamente, equilibri delicatissimi su cui si fondano vite e relazioni, potendo anche precludere quel rapporto – umano, benché non giuridico – tra madre e figlio, che la revoca dell'anonimato dovrebbe poter consentire. La protezione dati tutela, del resto, scelte femminili non meno complesse, come

quelle sull'interruzione della gravidanza, la cui riservatezza è condizione prima della loro effettiva libertà. Anche per questo, il Garante è intervenuto rispetto all'indebita rivelazione di queste scelte, determinata dall'indicazione, sulla sepoltura dei feti nel comune di Roma, del nome della madre.

Quelli su cui ci siamo soffermati oggi sono soltanto alcuni degli ambiti nei quali si esprime la protezione dei dati. Diritto definito, non a caso, di frontiera, richiamando un concetto che, nella narrativa occidentale, è il luogo simbolico tanto della sfida quanto dell'incontro con l'altro-da-sé, perché la protezione dei dati vive del confronto, sempre dinamico, con una realtà mai eguale a sé stessa.

Dalla bioetica all'intelligenza artificiale, dai poteri privati delle piattaforme al cyberbullismo; dai discorsi d'odio all'oblio; dagli invisibili digitali della gig economy alla telemedicina: in tutti questi ed altri contesti il Garante fornisce il proprio contributo, a tutela di chi viva la solitudine digitale (per assenza di protezione, per asimmetrie cognitive, per necessità) come soggezione all'altrui potere. La solitudine - scriveva, del resto, Michel Foucault - è la condizione prima della totale sottomissione.

Contrastarla, a tutela della libertà e della dignità della persona, è l'obiettivo che il Garante persegue ogni giorno, anche e soprattutto grazie al lavoro prezioso del personale tutto, 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.

Essere all'altezza delle sfide epocali che ci attendono, come singoli e come società, è l'obiettivo che il Garante continuerà a perseguire, con profondo rispetto per la così grande responsabilità affidatagli dal Parlamento.

Vi ringrazio.