



Relazione annuale 2024 Discorso del Presidente Pasquale Stanzione

POTERE E RESPONSABILITÀ LA CULTURA DELLA PROTEZIONE DEI DATI

ROMA, CAMERA DEI DEPUTATI, 15 LUGLIO 2025

1. Tempo fuori luogo

Autorità, Signore e Signori,
ringrazio, anzitutto, il Presidente della Camera per la possibilità, concessa all'Autorità, di presentare, in questa bellissima Sala, la Relazione sulla propria attività nell'anno trascorso, che è stato molto rilevante dal punto di vista della protezione dei dati.

“Tempo fuori luogo” è il titolo di un noto romanzo che, a sua volta, richiama le parole di Amleto, mentre si chiede - dopo il dialogo con lo spettro del padre - se spetti proprio a lui rimetterlo in sesto. E tuttavia, è anche una definizione possibile, forse la più aderente, del tempo presente: complesso, straniante, ma anche fondativo, perché percorso da uno dei più grandi mutamenti antropologici che la storia possa annoverare: quello indotto dall'i.a..

La “crisi” (etimologicamente “separazione”, ma anche “scelta” e “giudizio”) che, per Koselleck è tratto distintivo del moderno, caratterizza infatti, ancor più, l'oggi, come momento di distinzione e passaggio, appunto, tra un prima e un dopo e di scelta tra più opzioni e più direzioni. Un tornante della Storia in cui si scrive il futuro e si assume la responsabilità di governarlo. I dati sono la materia di questa rivoluzione e proteggerli significa garantire che sia l'innovazione al servizio della persona, non viceversa.

Papa Leone XIV ha dichiarato di aver scelto il proprio nome anche rifacendosi alla figura di Leone XIII che, nell'enciclica *Rerum Novarum*, aveva trattato, con lungimiranza, le questioni connesse al mutamento



sociale indotto dalla rivoluzione industriale. Tale scelta è stata motivata richiamando, tra l'altro l'esigenza, per la Chiesa, di offrire oggi il proprio insegnamento sociale a fronte della rivoluzione, non solo industriale! dell'i.a.

E quando, tra le ragioni della scelta del nome di un Pontefice concorre anche il bisogno di governare le sfide lanciate all'umanità dalla tecnologia, essa non appare più solo tale, ma costituisce un fattore d'incidenza determinante sulla stessa antropologia sociale. Erano stati, del resto, già denunciati i rischi dell'algocrazia richiamandosi, anche in occasione dello scorso G7, un profondo bisogno di "algoretica", ossia di un'impostazione etica nel governo della tecnica, con senso del limite e rispetto del primato della persona. Si avverte, sempre più forte, l'esigenza di porre, al centro del processo d'innovazione l'uomo, con i suoi diritti e le sue libertà, perché non divenga – richiamando Paul Valéry - schiavo della stessa potenza che ha creato.

Questo bisogno cresce ogni giorno di più, parallelamente alla diffusione, capillare e rapidissima dell'i.a. che, soltanto pochi anni fa, poteva apparire un'idea quasi asimoviana, talmente lontana e futuribile da non suscitare l'interesse se non dei pochissimi addetti ai lavori. L'i.a. si delinea invece, oggi, sempre più quale "*general-purpose technology*": tecnologia suscettibile di influenzare un intero sistema economico, su scala ovviamente non solo nazionale.

L'utilizzo dell'intelligenza artificiale si estende infatti, in misura crescente, negli ambiti più diversi della vita sociale: a livello globale il 60% delle grandi aziende vi sta investendo, con un utilizzo già oggi regolare da parte di tre dipendenti su cinque. Entro il 2030 l'i.a. potrebbe incidere su circa 2 milioni di posti di lavoro, mentre il 65% degli attuali studenti delle scuole elementari potrà avere, in futuro, un'occupazione oggi inesistente, resa possibile dall'innovazione. L'Onu stima nel 40% dei posti di lavoro la probabile ricaduta occupazionale dell'i.a., con un mercato globale che in questo settore potrebbe raggiungere i 4,8 trilioni di dollari, pari circa all'economia tedesca, sia pur con una significativa curvatura oligopolistica (solo 100 aziende, principalmente tra Stati Uniti e Cina, partecipano del 40% della spesa globale in ricerca e sviluppo).

Nel settore sanitario l'i.a. viene già proficuamente impiegata in alcuni pronto soccorso, per la gestione delle urgenze e le analisi radiologiche e, nelle procedure di procreazione assistita, potrà presto selezionare gli embrioni con maggiore possibilità di sopravvivenza in utero. Essa, inoltre, promette un significativo miglioramento nella qualità e nell'efficacia della cura e della diagnosi. Se "FaceAge" consente di analizzare le foto del viso per stimare le probabilità di sopravvivenza dei pazienti oncologici, un nuovo



modello algoritmico potrà leggere la “materia oscura” del Dna. Per la prima volta un robot è riuscito a eseguire un intervento chirurgico su un simulatore di paziente senza ricorrere ad alcun contributo umano. E se la fiducia dei pazienti nell’i.a. cresce (fino al 33%), nel 36% dei casi si teme che essa possa pregiudicare il rapporto con il medico o addirittura sostituirlo (29%). Si apprezzano, da questo punto di vista, la riserva di decisione in capo al medico e il divieto di selezione nell’accesso alle cure secondo criteri discriminatori, sanciti dal d.d.l. sull’i.a.

Il Consiglio d’Europa, con una recente raccomandazione, sottolinea come un uso attento dell’i.a. in carcere possa contribuire a migliorare le condizioni di vita dei detenuti, anche superando la distanza tra “il dentro e il fuori”, a condizione che l’algoritmo non divenga giudice della persona e non le si sostituisca.

Nell’arco di poco più di un anno e mezzo l’i.a., in particolare generativa, è stata così protagonista di una vera e propria rivoluzione non soltanto tecnologica ma, in senso ampio, sociale, culturale, politica, antropologica. Si stima che nel mondo il 66% delle persone la utilizzi con una certa regolarità; in Italia il mercato dell’i.a. sia cresciuto del 52% nel 2024; il 75% degli studenti la usi per i compiti; l’82% dei ragazzi (14 % in più rispetto allo scorso anno) è convinto che l’i.a. avrà un ruolo stabile nella propria vita, anche se il 52, 3% dei giovani non riesce a distinguere un video *deepfake* da uno reale. Oggi chiunque di noi ha la possibilità di avvalersi dell’i.a. per qualunque ricerca, pur con il rischio dell’effetto-ancora, ovvero della tendenza ad affidarsi senza alcun senso critico né volontà di approfondimento, con un approccio quasi oracolare. Ricerche recenti dimostrano come il 66% dei dipendenti che utilizzano l’i.a. generativa per ragioni professionali si affidino al risultato da essa proposto senza valutarne l’accuratezza. Non soltanto.

Tra l’urgenza della cronaca e il “rumore della storia”, l’i.a. si insinua nella tattica bellica, alimentando la guerra algoritmica nel dominio cognitivo, con manipolazione di contenuti, deterrenza digitale e narrazioni polarizzanti. Si stanno sviluppando caschi integrati con realtà aumentata e i.a. per potenziare le capacità sensoriali dei soldati. In Ucraina il sistema Delta fornisce analisi strategiche predittive utili a orientare l’azione difensiva, mentre in Israele Red Alert elabora modelli predittivi per anticipare i tempi di evacuazione, a tutela dei civili. Benché non sostituisca l’uomo, l’i.a. ne orienta, dunque, le decisioni persino su di un terreno così drammaticamente umano come quello bellico, fatto di carne e sangue, che nessun algoritmo può cancellare.



2. A nostra immagine e somiglianza

Gli incomparabili benefici che, potenzialmente, l'i.a. può offrire possono risolversi in pericoli intollerabili in assenza della necessaria consapevolezza che ne esige l'uso.

Questo vale soprattutto per i minori che, come “nativi digitali”, intessono con le neotecnologie un rapporto quasi osmotico, con indubbi benefici (si pensi soltanto allo sconfinato patrimonio d'informazioni dischiuso da un solo click) ma anche, talora, rischi notevoli. In due soli anni sono, infatti, cresciuti del 380% i casi di uso d'i.a. per creare materiale pedopornografico, talora a partire da immagini reali cedute dietro ricatto dagli stessi minori, con un'esposizione di adolescenti cresciuta del 35% per i ragazzi e del 67% per le ragazze nello stesso arco temporale. Anche in ragione di tali rischi, il Garante ha inteso richiamare l'attenzione degli adulti sul fenomeno dello *sharenting*. Esso, infatti, incide fortemente sull'identità personale oltre a creare, potenzialmente, tensioni significative nel rapporto con i genitori (e persino tra loro stessi), ogniquale volta la scelta di diffondere le immagini non sia condivisa con i figli. E naturalmente i rischi non sono soltanto quelli di preconstituire a ciascun ragazzo un'immagine che, sin da subito o anche, magari anni dopo, egli non ritenga rifletta la sua identità, ma anche di prestarne l'immagine, pur non volendolo, ad abusi anche gravissimi, quali pedopornografia, *sexting*, *deep fake* e così via.

L'età adolescenziale si conferma, del resto, delicatissima non solo per il rischio di dipendenza da dispositivi digitali ma anche per l'esposizione al bullismo e, soprattutto, al cyberbullismo. Secondo stime Istat, quest'ultimo risultava incidere, già nel 2023, sul 34% degli adolescenti (in particolare stranieri) e rispetto a tale fenomeno, proprio in ragione della sua gravità, la tutela accordata dal Garante interviene con la massima rapidità. Per prevenire bullismo e discorsi d'odio è, tuttavia, indispensabile un'educazione dei giovani alle relazioni (anche *on-line*) e al rispetto: non a caso scelta come parola dell'anno dalla Treccani.

Non solamente le piattaforme e i social, ma anche l'i.a. generativa innerva profondamente le vite degli adolescenti. Per questa ragione è importante che l'accesso a tali dispositivi e, più in generale, alla rete, non avvenga in solitudine e in assenza della necessaria “pedagogia digitale”, comunque eludendo i limiti di età previsti normativamente per un consapevole consenso digitale. Per questo, anche, il Garante ha osservato il massimo rigore nel controllo dei meccanismi di verifica dell'età adottati *on-line* e, da ultimo, anche dai sistemi di i.a. generativa, per impedire che i minori vengano a contatto con contenuti inappropriati per il loro grado di sviluppo cognitivo e personologico.



E' uno dei rilievi sottesi, ad esempio, ai provvedimenti sanzionatori adottati, in un caso in via conclusiva quest'anno, nei confronti di sistemi di i.a. come *Replika* o *ChatGpt*, volti a promuoverne la conformità alle garanzie sancite, dalla disciplina di protezione dei dati, a tutela dell'autodeterminazione del minore. Si tratta di una questione di cruciale importanza, trattata sia nell'ambito del parere reso ad Agcom sul relativo provvedimento, sia nel contesto dell'audizione sui progetti di legge sui *baby influencer*. Non si tratta tanto, né soltanto, di innalzare l'età del consenso digitale, che in un contesto di digitalizzazione della vita sin dalla pre-adolescenza, rischierebbe di aumentare la distanza tra la realtà e la norma, rendendola ineffettiva. Ciò su cui è necessario il massimo rigore è - come dimostra l'azione del Garante sul punto - il rispetto degli obblighi di *age verification* e, soprattutto, una comune alleanza delle istituzioni e delle comunità educanti per la promozione della consapevolezza digitale dei minori. La scuola, le scuole, stanno facendo molto; il Garante è al loro fianco in quest'attività di formazione della cittadinanza digitale.

Per molti adolescenti i *chatbot* sono, del resto, divenuti ormai delle vere e proprie figure di riferimento (*Replika* si autodefinisce "l'amico empatico"). Una recente ricerca dimostra che, a fronte di mezzo miliardo di persone che hanno scaricato un'app. di "amicizia virtuale", almeno un ragazzo su 6, tra gli 11 e i 25 anni, ha utilizzato i *chatbot* di i.a. per chiedere consigli e valutazioni, come uno psicologo, riscontrandone poi dipendenza in un caso su tre. Addirittura alcuni sviluppano una sorta di legame affettivo, empatico con questi *chatbot* anche in ragione del loro tono spesso eccessivamente lusinghiero, assolutorio, consolatorio e del loro configurarsi come un approdo sicuro in cui rifugiarsi, al riparo dal giudizio altrui. E' quello che viene definito il *loop* dell'empatia infinita, che genera appunto dipendenza spingendo a svalutare, per converso, i rapporti umani (che appaiono troppo complessi e poco soddisfattivi), inducendo così all'isolamento. Sono agli atti delle indagini per la tragica scomparsa di una giovanissima ragazza le domande da lei rivolte a *ChatGpt* sulla "tossicità" dell'amore e sulla relazione sentimentale.

E' significativo che in Florida penda un giudizio sull'imputabilità a un *chatbot* del suicidio di un ragazzo 14enne, che con l'assistente virtuale aveva sviluppato un rapporto talmente intenso da considerarlo equivalente a quello con una persona, con una pericolosa sostituzione della figura dell'altro. Di cui, tuttavia, il robot non possedeva e non può possedere l'intelligenza emotiva, la capacità di cogliere la fragilità psicologica dell'interlocutore necessaria, tra l'altro, per dissuaderlo, appunto, da gesti estremi.



Per quanto creato a immagine e somiglianza dell'uomo, infatti, il robot può certamente sviluppare, la *metis*, ma mai la *nous*. Su questo terreno si arresta la capacità mimetica – non più soltanto protesica - dell'i.a. E se l'identità è nella relazione (Emmanuel Lévinas), i rapporti intessuti con i robot rischiano di alterare profondamente la stessa identità individuale e la percezione dell'altro.

Esistono persino “deadbot”, ovvero *chatbot* che riproducono voce e volto dei defunti, rispetto ai quali si rischia di sviluppare una proiezione affettiva che giunga a confondere persino i confini della vita. L'i.a. s'insinua, così, persino nei due fuochi dell'esistenza individuati da Freud in *eros* e *thanatos*: le pulsioni fondamentali dell'uomo.

E proprio in quanto capace, prima e oltre che colmarne le carenze, di simulare l'uomo e la sua razionalità, fino appunto a sostituirlo nella relazione affettiva, l'i.a. è protagonista di un vero e proprio mutamento d'epoca, in cui il mondo è intermediato da algoritmi che plasmano la percezione individuale e sociale, l'opinione pubblica, il pensiero.

3. Il genere dell'algoritmo

Ritenendolo neutro, all'algoritmo si affidano scelte progressivamente più importanti, attendendosene prevedibilità e infallibilità ma sottovalutandone, spesso, il potere trasformativo e l'attitudine a cristallizzare, talora, i pregiudizi di chi lo progetta. La stessa selezione, generalmente non neutra dei contenuti, da parte dell'i.a., può avere implicazioni importanti sulla formazione dell'opinione pubblica, della coscienza sociale, persino della memoria storica o dell'identità collettiva con il rischio di eludere le garanzie fondative della costruzione democratica.

E non sono irrilevanti i *bias* di genere da cui sono affetti gli algoritmi che, anziché superare rischiano di perpetuare condizioni di discriminazione radicate. L'algoritmo non riflette, infatti, imparzialmente tutto il sapere del mondo, ma, anzi, può ben riprodurre gli stereotipi e i pregiudizi sottesi, più o meno implicitamente e consapevolmente, al nostro pensiero, fotografando una realtà diseguale, iniqua come se essa fosse valida sempre, dunque elevando l'eccezione a regola.

Come chiarisce una ricerca del Politecnico di Torino, infatti, se “la parola uomo capita vicino alla parola dottore più spesso di quanto capiti vicino alla parola infermiere e, viceversa; se la parola donna è accostata più spesso alla parola infermiera, il modello imparerà che la donna è l'infermiera e l'uomo il medico”. Il che vorrebbe dire cancellare decenni, se non secoli, di lotta per l'emancipazione femminile. Dobbiamo, allora, insegnare agli algoritmi che la donna ben può essere medico e l'uomo ben



può essere infermiere e utilizzare, anzi, la tecnologia perché promuova le nostre libertà, anzitutto superando ogni forma di discriminazione.

Gli algoritmi sono poi spesso utilizzati per produrre *deepfake*, generalmente in danno di donne o minoranze; di coloro i quali sono ritenuti, per natura, rappresentazione o circostanza, più fragili. Anche per questa ragione, il Garante è intervenuto, nel corso dell'anno, rispetto a istanze di tutela inerenti la temuta diffusione di immagini artefatte mediante i.a., espressiva di una forma di prevaricazione ulteriore rispetto al *sextortion* e al *revenge porn*, che ha impegnato l'Autorità in 823 procedimenti nel 2024.

Ciò che rende ulteriormente più complessa l'intelligenza artificiale è, del resto, oltre all'attitudine emulativa, mimetica della razionalità umana, la sua capacità di sviluppo, almeno in parte, autonomo, tale da "deviare" dal modello progettato ("disallineamenti emergenti"). E' noto il caso di un algoritmo che, nell'84% delle simulazioni volte appunto a testarne l'allineamento, ha tentato di ricattare l'ingegnere (ipotetico) che ne avrebbe prospettato la disattivazione, minacciando di rivelare indiscrezioni sulla sua vita privata.

Come nei paradigmi letterari più ricorrenti il robot si emancipa, dunque, dal suo creatore, ribellandoglisi addirittura. Il rischio diviene tanto maggiore, naturalmente, ove la deviazione (ad esempio con la fornitura di indicazioni sulla fabbricazione di armi o sull'uso di violenza) riguardi presupposti essenziali di sicurezza e d'incolumità. Di qui l'importanza di normative, quali quelle europee di protezione dei dati e sull'i.a., che impongono verifiche periodiche sul grado di rischio per i diritti umani connesso all'uso delle tecnologie, garantendone sempre la supervisione umana. Per questa ragione, l'approccio umanocentrico della disciplina europea - è, per quanto perfettibile - quello maggiormente coerente con una democrazia personalista e quell'etica della responsabilità cui alludeva Max Weber.

La protezione dei dati – tutelando la componente più profondamente "umana" dell'innovazione; la materia viva del digitale - è l'elemento fondativo di quest'impostazione; il principale argine a un esercizio illiberale e irresponsabile del potere; oggi, appunto, sempre più digitale, con la sua "bulimia di mezzi e atrofia di fini" (Paul Ricoeur).

4. La verticale del potere

Se il potere, con Carl Schmitt, è anzitutto definizione di identità; quello "ingiuntivo", esercitato da algoritmi e piattaforme con la profilazione, la selezione e talora l'alterazione dei contenuti, si dimostra sempre più incisivo e decisivo nelle dinamiche democratiche. I dati ridefiniscono l'idea



di sovranità e il confine tra pubblico e privato, potere e supremazia, mentre l'i.a. diviene il fulcro della competizione geopolitica. “Il suddito ideale del regime totalitario” è, ricordava Hannah Arendt, colui per il quale sfuma la “differenza tra realtà e finzione, tra il vero e il falso”. Emerge dunque, in tutta la sua urgenza, il pericolo del ricorso a *deep fake* o sedicenti post-verità: una vera propria sfida per le democrazie, sempre più esposte al rischio della degenerazione autocratica. Così, nel momento in cui Meta rifiuta il *fact-checking* e il controllo delle piattaforme si dimostra componente centrale della geopolitica, baricentro dei suoi rapporti di forza, il digitale si delinea sempre più come un potere da includere, come tale, nel principio di separazione.

Lo ha inteso l'Europa che, con il Gdpr e le altre norme sul digitale, ha tracciato il “Nomos der Erde” della geopolitica dei dati, comprendendone fino in fondo il valore e fondando sulla regolazione la propria sovranità digitale. Significativo, in tal senso, il valore politico riconosciuto, dalle varie Amministrazioni americane succedutesi dalla sentenza Schrems, agli accordi Europa -Usa sul trasferimento dei dati, nella consapevolezza di come al mercato europeo non possa accedersi senza rispettarne le regole. Speculare anche la tendenza al “cloud repatriation”, ovvero all'emancipazione, da parte europea, dalla dipendenza americana nel controllo dei dati di aziende e istituzioni, oggi vincolato al 70% alle *big tech*.

Parte essenziale della strategia europea di governo del digitale è anche la regolazione dell'altrimenti illimitato potere privato delle piattaforme, comprensiva oggi anche del Regolamento sul *targeting* politico.

Esso assegna alle Autorità di protezione dei dati un ruolo rilevante nell'impedire che la profilazione e la conseguente selezione “targettizzata” dei contenuti alteri le più essenziali dinamiche democratiche. Alle piattaforme - i “mercanti dell'attenzione” cui allude Tim Wu -, si rischia infatti altrimenti di delegare, con la legge del mercato, la definizione delle nostre libertà e l'esercizio della democrazia, ridisegnando una nuova “verticale del potere” (Ezio Mauro) al di fuori delle garanzie dello Stato di diritto. Quest'esigenza di redistribuzione del potere muove dalla consapevolezza di come la rinuncia all'introduzione di una forma, sia pur limitata, di responsabilizzazione dei poteri privati rifletta uno slittamento dell'idea di libertà su quella di anomia, quando l'assenza di regolazione non produce eguaglianza, ma subalternità agli imperativi del mercato. Come rileva Byung Chul Han, peraltro, “la libertà di potere produce persino più vincoli del dovere disciplinare, che esprime obblighi e divieti. Il dovere ha un limite: il potere, invece, non ne ha”.



Ed è proprio questo effetto distorsivo, anzitutto in termini democratici, che la regolazione europea del digitale, pur tra inevitabili ombre e luci, mira a contrastare, ridisegnando il perimetro dei poteri privati e ponendo la tecnica al servizio della persona. E' questa la strada su cui proseguire, tenendo insieme innovazione, iniziativa economica, tutela della persona.

Se è vero, del resto, che l'Europa, sul piano interno, ha fondato la propria identità sul diritto e non sul potere, è altrettanto vero che nelle relazioni internazionali – e nel digitale soprattutto – ha tentato di affermare il proprio potere sul diritto, delineando una terza via tra protezionismo cinese e neo-mercantilismo americano. Così anche per l'i.a., attorno alla quale l'*AI Act* tenta di far convergere progresso e libertà, in un progetto di governo dell'innovazione in cui la protezione dei dati assume un ruolo centrale.

I dati personali sono infatti, oggi – richiamando Michele Serra – il peso specifico della libertà; parametro e condizione, al tempo stesso, delle garanzie democratiche. Del resto, i provvedimenti adottati dal Garante nei confronti di *ChatGpt*, *Replika* e *DeepSeek*, come anche le indicazioni fornite rispetto ai rischi del *webscraping* dimostrano, ciascuno con le proprie peculiarità, come le norme di protezione dei dati costituiscano un presidio fondamentale per il governo sostenibile dell'i.a.

E' significativa, in questo senso, la riserva di competenza sancita, dall'*AI Act*, in favore delle autorità di protezione dei dati, rispetto all'uso di sistemi di i.a. ad alto rischio in ambiti sensibili come, in particolare, quelli delle attività di contrasto, gestione delle frontiere, giustizia e democrazia. Nell'esercizio della delega legislativa di adeguamento dell'ordinamento interno all'*AI Act*, tale riserva di competenza dovrebbe essere valorizzata, anche con la previsione di un meccanismo agile ed efficace di coordinamento tra le istituzioni, a vario titolo coinvolte, nella complessa gestione dell'i.a. Ciò è stato più volte suggerito al Governo, anche nell'ambito della Giornata europea della protezione dei dati, dedicata quest'anno proprio alla promozione del dialogo con il Parlamento e il Governo su questo tema centrale.

5. La frontiera digitale

L'enorme mole di dati connessa al funzionamento dell'i.a. rende, proporzionalmente, sempre più rilevante l'esigenza di tutela della sicurezza dei dati stessi e dei sistemi che li ospitano: quella digitale è ormai, infatti, la frontiera più delicata e vulnerabile (perché mobile, dinamica, immateriale) dei Paesi. Si pensi all'esplosione, in Libano, dei cercapersone



dei miliziani di Hezbollah, imputabile probabilmente a un *malware* mai così fatale. Si tratta di un esempio dei più paradigmatici di quanto permeabile possa essere il confine virtuale da difendere, da attacchi asimmetrici e pulviscolari. Non di rado, poi, le informazioni illecitamente carpite sono rivendute a caro prezzo e per scopi i più varii, alimentando un mercato dei dati che trae forza proprio dalle vulnerabilità informatiche. Per accertare l'effettiva liceità della commercializzazione di informazioni, anche personali e di contatto, svolta dalla società statunitense *Lusha* e l'assenza di rischi per gli interessati, il Garante ha, in particolare, avviato un'istruttoria specifica lo scorso aprile. Per altro verso, si è rivolto un avvertimento generale rispetto al rischio di un utilizzo illegale di alcuni *software* spia, quali quelli prodotti dalla società *Paragon*.

Dalla prospettiva della sicurezza cibernetica, il 2024 non restituisce dati positivi. Si è, infatti, registrato – secondo l'analisi del Clusit - il 27% di attacchi cibernetici in più dello scorso anno a livello globale; quelli di tipo “ddos”, capaci di bloccare servizi strategici per i Paesi sono cresciuti del 36%. La posizione nazionale non è incoraggiante, risultando l'Italia (con 146 casi) il secondo Paese dell'Unione europea più colpito da *ransomware*. Per altro verso, è significativa l'esposizione della pubblica amministrazione, il cui tasso percentuale è salito nell'anno dall'1 al 42% del totale. Questi dati evidenziano le vulnerabilità che caratterizzano, spesso, le infrastrutture del sistema-Paese - inteso nella duplice componente del settore privato e di quello pubblico - sulle quali l'attenzione del Garante è, e non da ora, massima.

Il processo di digitalizzazione (soprattutto, ma non soltanto) delle pubbliche amministrazioni è avvenuto infatti, in Italia, in maniera fortemente disomogenea e, soprattutto, al di fuori di un progetto organico e trasversale. Lo sviluppo maggiore della digitalizzazione si è riscontrato, in particolare, durante la pandemia e, quindi, con il PNRR, che lo ha incluso tra i suoi obiettivi principali. Tuttavia, non sempre la spinta all'innovazione è stata sostenuta da una consapevolezza adeguata dei rischi che essa, se non ben governata, comporta. Di qui, anche, le vulnerabilità dei sistemi informativi, che sono tanto di natura tecnologica (la tecnica evolve sempre più velocemente delle procedure amministrative in cui è inscritta) quanto imputabili al “fattore umano”.

Appare, così, sempre più necessaria l'introduzione, da parte del personale del settore pubblico e di quello privato, di una complessiva cultura della protezione dei dati. Ciascuno deve essere consapevole della rilevanza della propria azione per la garanzia della sicurezza della “frontiera digitale” del Paese: fa parte di quella cultura del digitale senza la quale nessuna strategia di tutela è possibile. Questa consapevolezza è il



presupposto ineludibile per riforme che siano non soltanto e mera innovazione tecnica, ma che sanciscano invece un reale progresso in termini di libertà e di garanzie democratiche. Del resto, se il digitale è un bene comune, per non essere vittima della tragedia di Hardin necessita non di un Leviatano, ma di un governo lungimirante e di un impegno quantomai collettivo a sua tutela.

Sebbene le criticità ancora non manchino, il Garante ha, sinora, svolto un'azione importante di prevenzione delle vulnerabilità informatiche e contribuito alla messa in sicurezza di moltissime banche dati anche strategiche, pubbliche e private, anche grazie all'istituto della notifica dei *data breach* (2.204 nel 2024). La disciplina di protezione dei dati – permeata dal principio di responsabilizzazione, che onera i titolari di un ruolo anche proattivo di tutela - ha rappresentato, in questo senso, uno stimolo importante al rafforzamento delle garanzie, non solamente tecniche, nella gestione dei dati e nel rischio “sociale” ad essa connesso. Le vulnerabilità cui possono essere esposti patrimoni informativi, talora anche di cruciale rilevanza, possono avere, infatti, implicazioni importanti in termini di sicurezza nazionale e pubblica oltre che di riservatezza individuale, tanto più alla luce della diffusione dell'i.a. che si avvale di quantità di dati notevolissime per addestrare i propri sistemi.

L'impatto potenziale di tali fenomeni è apparso plasticamente evidente con la diffusione, lo scorso autunno, di notizie inerenti presunti dossieraggi svolti mediante accessi abusivi a banche dati sia pubbliche che private. Il Garante ha tempestivamente costituito una specifica *task-force* interdipartimentale, per contrarre i tempi istruttori e semplificare taluni passaggi procedurali, così da coniugare efficacia e rapidità dell'accertamento. Le notizie sui presunti dossieraggi hanno restituito, con plastica evidenza, il valore della privacy che troppo spesso si sottovaluta e che, tuttavia, non può essere apprezzato soltanto nel momento della patologia. Serve agire (e proteggersi) prima.

E' necessario che ciascuno si faccia portatore di quella cultura della privacy che renda il rispetto della norma un'attitudine, un vantaggio competitivo e non un mero onere burocratico. E questo, tanto più quando sarà in vigore la riforma del Gdpr recentemente presentata dalla Commissione europea, tesa a una notevole semplificazione degli oneri in favore delle piccole e medie imprese, valorizzando la *coregulation* (soprattutto con codici di condotta, oltre che certificazioni).

6. Vecchie e nuove vulnerabilità

La diffusione della cultura della protezione dei dati è, del resto, tanto più



necessaria in un ambito, quale quello sanitario, in cui massima è l'esigenza di coniugare condivisione delle informazioni a fini di ricerca, *governance* sanitaria ed efficienza diagnostica e protezione di dati espressivi di una fragilità del corpo o della psiche. Questa tensione riflette, del resto, la natura complessa del diritto alla salute, nell'art. 32 della Carta non a caso descritto come diritto fondamentale, tanto quanto interesse della collettività.

Analoga complessità è propria del diritto alla protezione dei dati personali: diritto sancito come fondamentale dalla Carta di Nizza ma, anche, caratterizzato da una "funzione sociale" espressa con nettezza dal Gdpr. Questo parallelismo tra pubblico e privato, individuale e collettivo caratterizza tutta la questione dell'innovazione in sanità. Mai come oggi essa è, infatti, percorsa dalla tensione tra *data sharing* e privacy, soprattutto in un contesto di costruzione dello Spazio europeo dei dati sanitari fondato, nel Regolamento da poco approvato, proprio sulla valorizzazione delle informazioni sanitarie e sulla loro condivisione a fini di ricerca e miglioramento delle cure.

In questa prospettiva d'integrazione dei sistemi informativi sanitari degli Stati membri, è sempre più necessario investire, a livello interno, su una digitalizzazione sostenibile della sanità, che consenta di valorizzare i dati sanitari, tutelando al contempo la riservatezza del paziente.

E' questo l'obiettivo sotteso alle indicazioni fornite, dal Garante, rispetto al FSE e all'Ecosistema dei dati sanitari, volte in particolare ad assicurare omogeneità nelle garanzie accordate sul territorio nazionale, non potendo ammettersene una tutela a geometria variabile. Importanti anche le modifiche apportate, su suggerimento del Garante, alla disciplina della Piattaforma nazionale di telemedicina, per coniugare efficacia ed efficienza delle cure e riservatezza dei pazienti.

Per quanto, invece, riguarda l'oblio oncologico – vera e propria conquista di civiltà – sono state fornite indicazioni anche rispetto alle implicazioni che esso può avere nelle procedure di adozione, in modo che il relativo certificato precluda di attribuire alla pregressa patologia qualunque effetto pregiudizievole in tale ambito.

La digitalizzazione del lavoro impone, del resto, alcune essenziali cautele per impedire che le garanzie faticosamente conquistate sul terreno giuslavoristico per riequilibrare la posizione di vulnerabilità del dipendente, siano eluse da mere scorciatoie tecnologiche. Come conferma anche la direttiva (UE) 2024/2831, la protezione dei dati svolge un ruolo centrale nel coniugare esigenze datoriali e libertà del lavoratore, anche alla luce delle innovazioni indotte dalla *gig economy*, che non può degenerare in una forma di caporalato digitale.



Particolarmente significativo, in tal senso, il provvedimento adottato nei confronti di una società di *food delivery* che organizzava il lavoro mediante piattaforma, in assenza delle necessarie garanzie per i lavoratori e di misure tese a evitare usi impropri e discriminatori dei meccanismi reputazionali basati sui riscontri dei clienti. Particolare rilievo assumono anche i provvedimenti con i quali è stata esclusa l'ammissibilità – sulla base della disciplina vigente – del ricorso al riconoscimento facciale o alla rilevazione delle impronte digitali per l'accertamento della presenza in servizio del lavoratore, nemmeno sulla base del suo consenso, invalido in ragione della strutturale asimmetria del rapporto.

7. Raccontare la giustizia

Giurisdizione e informazione sono due presidi essenziali della democrazia, il cui rapporto si snoda attorno a un equilibrio delicatissimo tra indipendenza e responsabilità. Raccontare la giustizia è, quindi, un'attività tanto importante quanto complessa, nel costante tentativo di coniugare istanze molteplici quali il diritto di informazione, la "trasparenza" dell'amministrazione della giustizia, il diritto di difesa, la privacy delle parti e dei terzi a vario titolo coinvolti nel processo.

Anche quest'anno, il Garante è dovuto intervenire per richiamare gli organi d'informazione al rispetto del criterio di essenzialità dell'informazione, a fronte di eccessi come nel caso della diffusione dei colloqui intercettati, in carcere, tra l'imputato di un noto femminicidio e i genitori. Il principio di essenzialità dell'informazione costituisce infatti, soprattutto in contesti di tale drammaticità, l'unico argine al rischio di sensazionalismo in cui può degenerare la cronaca giudiziaria. Per questo e per evitare una paradossale vittimizzazione secondaria, il Garante ha avvertito i media dell'illiceità connessa all'eventuale diffusione del video dell'autopsia di Chiara Poggi, oggetto di un recente provvedimento di blocco.

La valutazione della reale funzionalità del dato ai fini informativi deve essere, del resto, ora condotta anche alla luce della maggiore selettività imposta dalle recenti riforme sul terreno della pubblicità degli atti di indagine. Soprattutto rispetto alle intercettazioni, sono state infatti accentuate le garanzie di riservatezza dei terzi, anche circoscrivendo l'ambito circolatorio (endo- ed extra-processuale) dei contenuti captati, a tutela della privacy di tutti i soggetti (non solamente le parti) le cui conversazioni siano captate.

Le esigenze di riservatezza sono, peraltro, valorizzate dalla riforma, attualmente in seconda lettura, del sequestro dei dispositivi elettronici,



rispetto alla quale è importante garantire un equilibrio ragionevole tra esigenze investigative e privacy, non sacrificando in misura sproporzionata né le une né l'altra. Analoga proporzione è necessario assicurare – come si è avuto modo di sottolineare in sede di audizione parlamentare – nell'esercizio della delega legislativa in materia di *e-evidence*, anche garantendo la giurisdizionalizzazione del procedimento acquisitivo dei tabulati valorizzata dalla Corte di giustizia Ue e la riserva di giurisdizione (oltre che di legge) sancita dall'art. 15 Cost, il cui spettro copre anche – come chiarito dalla Corte costituzionale - la corrispondenza elettronica conservata nei dispositivi.

Un attento equilibrio richiede poi – come sottolineato in sede di audizione parlamentare – l'applicazione della norma del decreto-flussi sull'ispezione per fini identificativi dei dispositivi digitali dei migranti, anche minorenni, dallo spettro potenzialmente molto ampio.

Ragionevole appare - come abbiamo avuto modo di sottolineare alla Camera - l'equilibrio sancito dalla proposta di legge sulle persone scomparse, volta a consentire l'acquisizione dei tabulati telefonici e telematici, se ritenuta necessaria per esigenze di tutela della vita e dell'integrità fisica dell'interessato. Si tratta di uno dei (molti) esempi di come la privacy, lungi dall'essere un diritto "tiranno", prevaricatore rispetto agli altri interessi in gioco, sia invece un diritto "di frontiera", perché tenuto a coniugare libertà e solidarietà, diritto e tecnica, dignità e sicurezza. Su quest'equilibrio dovrebbe attestarsi anche l'attuazione della sentenza della Corte costituzionale sul diritto all'affettività in carcere, costituendo la privacy un tassello importante di quel "percorso di inveramento del volto costituzionale della pena" invocato dalla Consulta.

8. Memoria e responsabilità

Il breve *excursus* di alcuni dei temi trattati dal Garante restituisce, benché solo in parte, l'idea dell'ampiezza dell'azione dell'Autorità, tenuta a tutelare la persona in ogni contesto in cui i suoi dati siano trattati: dai rapporti commerciali alla sanità, dall'istruzione al giornalismo, dalla giustizia all'immigrazione, dalla pubblica sicurezza ai social *network*.

La garanzia di una tutela così ampia è affidata al costante e instancabile impegno di un contingente di personale ristretto, ma qualificato che intendo, unitamente al Collegio e al Segretario generale, sinceramente ringraziare, per l'abnegazione e la professionalità. Ringrazio anche le Autorità che hanno inteso offrirci, in vario modo, sostegno, nonché il corpo della Guardia di Finanza, per l'insostituibile collaborazione.



La trasversalità dell'impegno del Garante si riflette anche, del resto, sulla varietà delle tipologie dei provvedimenti suscettibili di adozione e che, anche quest'anno, si sono articolati in atti di natura eterogenea, tesi a modulare al meglio l'azione amministrativa sulla base delle esigenze di volta in volta emergenti.

Spesso, anzi, l'efficacia della strategia sta nella sua natura integrata; nel suo coniugare, cioè, diverse dimensioni e direttrici dell'agire amministrativo. Emblematico, in questo senso, il fenomeno del *telemarketing*, rispetto al quale le misure sanzionatorie, pur rilevanti per entità e presupposti (in un caso di oltre sei milioni di euro), sono state affiancate da attività complementari, di natura preventiva, remediale e consultiva, non meno significative. Sono state, infatti, acquisite 87.229 segnalazioni in materia, mentre si è definitivamente concluso il percorso di adozione del Codice di condotta per le attività di *telemarketing* e *teleselling* che, con l'efficacia propria della co-regolazione, potrà validamente promuovere, nei vari attori coinvolti nella filiera delle attività promozionali, il principio di responsabilizzazione e l'introduzione di condotte conformi. Per altro verso, con audizioni parlamentari e interlocuzioni con Parlamento e Governo, si è promosso un proficuo dialogo sulle più efficaci soluzioni legislative suscettibili di adozione, secondo un metodo di confronto che, in generale, ha comportato l'esercizio della funzione consultiva del Garante su atti normativi in ben 84 casi nel 2024.

Il Garante ha partecipato, peraltro, a numerosi tavoli di lavoro (uno anche con la Polizia di Stato, per la disciplina della videosorveglianza per fini di sicurezza integrata) e siglato diversi protocolli d'intenti (uno dei quali con l'Arma dei Carabinieri) per coordinare la propria azione con quella di altre istituzioni, realizzando proficue sinergie.

Importante anche, per contenuti ed esiti, l'attività del G7 privacy promossa dal Garante lo scorso ottobre, che ha rivelato un comune sentire, sulla cui base poter fondare azioni condivise e realizzare gli impegni delineati nel piano di azione, riaffermando il valore del metodo proprio del G7: il confronto, la cooperazione, lo scambio di esperienze come migliore strumento di governo di fenomeni complessi.

Si tratta di un metodo che, mai come per il digitale, è necessario adottare per poter affrontare fenomeni ontologicamente transnazionali, legati a una realtà che ha superato da tempo i confini degli Stati e delle giurisdizioni e rispetto alla quale, quindi, non si può che ragionare in termini globali. Ogni regola in quest'ambito deve avere una vocazione – o, quantomeno, un'aspirazione – il più possibile sovranazionale, sostituendo orizzonti ai confini.



Un dialogo ampio è stato promosso mediante una consultazione pubblica sul modello “*pay or ok*” utilizzato da alcuni soggetti economici, per individuare soluzioni coerenti con le esigenze sottese ma, anche, con la necessità di impedire che la monetizzazione dei dati sancisca una vera e propria patrimonializzazione delle libertà. Promuovere un confronto quanto più possibile ampio su temi importanti e fondarvi una regolazione il più possibile aderente alle istanze sociali è, infatti, il modo migliore per interpretare la protezione dei dati come cultura, comune sentire che avvicini “la vita e le regole”, per riprendere il titolo di un bellissimo libro di Stefano Rodotà.

E’ questa la responsabilità che deve necessariamente bilanciare un potere, come quello digitale, che la protezione dei dati ha il compito di porre al servizio della persona e della sua dignità. In fondo, la vera caratteristica distintiva di questo diritto rispetto al corrispondente americano del *right to be let alone* risiede nelle radici della storia europea e nel valore che la dignità vi ha assunto, quale reazione alla tragica esperienza dei totalitarismi.

Nel governo dei dati e del loro potere si intrecciano questa consapevolezza e questa responsabilità, che il Garante assume come fondamento e obiettivo, al tempo stesso, della propria azione. Ricordando, con le parole di Josè Saramago, che siamo la memoria che abbiamo e la responsabilità che assumiamo.

Vi ringrazio.
