Umanesimo digitale e protezione dei dati

1. Il “rumore della storia”

Signora Presidente del Senato,
Autorità,
Signore e Signori,

questa Relazione si inserisce in una congiuntura del tutto particolare, che con le parole del Papa potremmo definire più un cambiamento d’epoca che un’epoca di cambiamenti. Tanto profonde, sono, infatti, le innovazioni che caratterizzano l’ora presente, da aver determinato un vero e proprio mutamento di paradigma generale nel rapporto tra l’uomo e il mondo.

In questo più ampio contesto si inscrive la riflessione di oggi, al crocevia tra due momenti importanti: la congiuntura socio-politica attuale, segnata dal passaggio dall’emergenza sanitaria a quella internazionale e le spinte riformatrici sul terreno del digitale di cui l’Europa si è resa protagonista indiscussa, sviluppando l’itinerario intrapreso già sei anni fa con il quadro giuridico europeo in materia di protezione dei dati.

Ma il dramma che si agita sullo sfondo è una priorità logica e assiologica da cui non è possibile prescindere; il “rumore della Storia” e l’ “immane concretezza” del reale impongono una considerazione preliminare.

La guerra irrompe, contro ogni tentativo di rimozione, alle porte dell’Europa da più di quattro mesi, lascia consumare vite e le armi tornano a sostituire, con una pericolosa regressione storica e simbolica, la competizione non solo tra Stati ma tra modelli politici, tra autoritarismi e democrazie. Poco più in là dai confini del vecchio continente, il *nomos* della Terra si riprende, prepotentemente, lo spazio sinora occupato dalla paziente tessitura del diritto e dalla costante mediazione della politica. E gli effetti drammatici di

questa anacronistica “patologia del confine” dimostrano, ancora una volta, le irrinunciabili virtù della democrazia e dello Stato di diritto, per perfettibili che siano.

Lo aveva, del resto, reso evidente la pandemia, nel raffronto tra le politiche di contenimento sanitario adottate in Europa e le ben diverse misure di biosorveglianza di alcuni sistemi asiatici. Proprio la protezione dei dati è stata uno dei pilastri del modello europeo di governo dell’emergenza, che in snodi importanti come le scelte sul *contact tracing* o sul *green pass* ha suggerito la direzione più conforme al personalismo sotteso alla costruzione europea.

Sul terreno dell’emergenza sanitaria si è infatti misurata, fino in fondo, la capacità tutta europea di coniugare libertà e solidarietà senza consentire prevaricazioni dell’una sull’altra. E in questo gioco di equilibri in continua ridefinizione, la privacy ha dimostrato di essere un diritto mai tiranno, duttile nelle soluzioni di volta in volta richieste ma rigoroso nei principi e nel significato ultimo: promuovere la sinergia tra innovazione e libertà, collocando sempre – come ci ha ricordato il Presidente della Repubblica e analogamente al preambolo della Carta di Nizza - la “persona al centro”.

Questo straordinario diritto di libertà si è rivelato determinante nel guidare la transizione digitale promossa, con accelerazione esponenziale, dalla pandemia, per impedire che il doveroso distanziamento sociale annientasse le relazioni e la vita collettiva, spostando il nostro quotidiano nella realtà virtuale senza, tuttavia, il rischio di divenire schiavi del sempre più invasivo occhio elettronico.

Ma lo sviluppo dirompente della digitalizzazione, favorito con progressione geometrica dalla pandemia, mostra oggi, nel contesto della prima guerra (anche) cibernetica, tutte le sue più profonde implicazioni per quella che lucidamente è stata definita “super-società”, fatta di interdipendenze inestricabili, paradossalmente proprio nell’era della disintermediazione (M. Magatti). Nel passaggio dal reale al virtuale, in quello che è stato un vero e proprio

*uploadin*g della vita individuale e collettiva, la simmetria della trasposizione *online* non ha riguardato anche - o non come avrebbe dovuto e non solamente in Italia - i presidi a tutela della persona e degli Stati. Secondo le stime del World Economic Forum, nell'anno trascorso si sarebbe registrato un aumento del 151% degli attacchi ramsomware: cifra tutt'altro che marginale se si considera che ciascun incidente può determinare una perdita aziendale quantificabile addirittura, secondo il Ponemon Institute, in 4 **,**24 milioni di dollari**.** Ecco, anche, perché la protezione dati rappresenta per le aziende non già un costo ma un fattore di competitività, oltre che una risorsa reputazionale importante.

La più accentuata esposizione on line delle nostre vite ha mutato, parallelamente, la stessa generale percezione della vulnerabilità informatica: secondo uno studio del Censis, il 56, 6% degli italiani teme, oggi, di subire violazioni della propria sicurezza informatica più del libero accesso alla rete da parte dei minori (34,7%), della dipendenza dal web (23,7%) e di essere vittima di hater (22%). E la vicenda milanese (operazione "Rear Window") delle organizzazioni criminali aduse a violare gli impianti di sorveglianza persino domestici, consentendo così di spingere un'insana curiosità sin nelle pieghe più intime delle "vite degli altri", è soltanto un esempio di quanto la porosità del confine digitale possa pregiudicare i singoli e la collettività.

Talmente veloce e improvvisa è stata la traslazione o*nline* delle nostre attività che quella digitale è apparsa, progressivamente, come la frontiera più permeabile e agevolmente valicabile da parte della criminalità informatica e di chiunque intenda sfruttare dati e informazioni, anche personali, a fini illeciti. Proprio durante il *lock down* si è registrato un incremento significativo degli attacchi informatici ai danni (anche) di enti pubblici, di catene di approvvigionamento e di reti sanitarie, secondo una tendenza che si sarebbe, inevitabilmente, amplificata con il conflitto russo-ucraino.

Ma se la guerra convenzionale soggiace, quantomeno, alla logica territoriale del confine, la sua componente ibrida, cibernetica, ne

prescinde mettendo in gioco, sia pur solo per *spillover*, anche i Paesi che non partecipano direttamente alle ostilità. L'Enisa ha calcolato che oltre un terzo dei trecento attacchi *cyber* verificatisi tra Russia, Ucraina e Bielorussia, dall'inizio delle ostilità, ha avuto implicazioni nell'Unione europea: anche sotto questo profilo la guerra, dunque, ci riguarda e impone una strategia comune di difesa. La protezione della frontiera digitale – la cui componente centrale è proprio la protezione dei dati personali – assume, quindi, una funzione prioritaria nella tutela dei singoli e degli Stati.

Particolarmente lungimirante, in questo senso, è stata la scelta dell'UE di aggiornare, proprio a fine 2020, la propria strategia di *cybersecurity* proponendo anche una nuova direttiva (la NIS2) maggiormente calibrata sulle sfide attuali. Altrettanto opportuna è apparsa, in ambito nazionale, l'istituzione dell'Agenzia per la cybersicurezza nazionale, con cui il Garante ha sin dall'inizio instaurato – come previsto dalla stessa disciplina istitutiva – una proficua collaborazione, recentemente declinata in uno specifico protocollo d'intenti.

Ma la guerra alle porte dell'Europa non è "soltanto", anche, una *cyber-war*, ma è persino una *social-war*, combattuta con strategie di condizionamento del consenso realizzate soprattutto attraverso i social network, sulle quali potrà peraltro incidere il recente Codice di condotta sulla disinformazione della Commissione europea. Anche in questo caso, la pandemia aveva anticipato la tendenza futura all'infodemia che, con la guerra, ha mostrato di poter divenire persino autarchia informativa, realizzata mediante censura di contenuti ostili e promozione della narrazione dei fatti più utile alla propria parte.

Si tratta di implicazioni tutt'altro che trascurabili del processo di datificazione della vita individuale e collettiva, che ridisegna assetti di potere e strategie di gestione del consenso e che l'Unione europea mira a governare, concentrando proprio sul digitale la sua spinta riformatrice, per temperare la *rule of technology* con la *rule of law*.

2. La via europea al digitale

Particolarmente significativo, da questo punto di vista, è il *draft* di *Artificial Intelligence Act*, che introduce alcune misure indispensabili a prevenire le implicazioni pregiudizievoli, per i singoli e la collettività, dell'intelligenza artificiale.

La proposta sottende una scelta importante, in termini non soltanto regolatori, ma anche e soprattutto politici e assiologici. Essa esprime l'esigenza di rimodulare il perimetro del tecnicamente possibile sulla base di ciò che si ritiene giuridicamente ed eticamente accettabile.

L'*Artificial Intelligence Act* è uno (forse persino il più rilevante) dei vari tasselli che compongono il mosaico, in costante evoluzione, della regolazione europea del digitale, nel cui ambito il Gdpr svolge un ruolo centrale, sotto il profilo del metodo e del merito. Esso, infatti, ha da un lato rappresentato un vero e proprio paradigma di tutela cui la legislazione europea successiva si sta conformando, valorizzandone ora la sinergia tra *principles* e *rules*, ora la neutralità tecnologica, ora il principio di responsabilizzazione e, in linea generale, la fonte regolamentare quale forma regolatoria elettiva per garantire livelli di garanzie uniformi (*one continent, one law*).

Per altro verso, il Gdpr ha espresso il primo, importante tentativo di introdurre, con obblighi di responsabilizzazione e trasparenza nel trattamento, un argine significativo al capitalismo delle piattaforme, la cui egemonia anche culturale (nell'accezione gramsciana) si fonda sullo sfruttamento di quei frammenti dell'io che sono i dati personali. Quest'istanza regolatoria è stata espressa tentando di coniugare le esigenze di circolazione dei dati- funzionali non solo a fini economici ma anche solidaristici - e diritto dei singoli al "governo" della propria sfera informazionale. E l'altro elemento del binomio su cui si fonda, sin dal titolo, il Gdpr ("la libera circolazione" dei dati) è l'oggetto delle due ulteriori proposte legislative *(Data Act* e *Data Governance Act)* che, pur con un testo

certamente perfettibile (come chiarito anche dal Comitato europeo per la protezione dei dati e dal Garante europeo) concorrono al quadro delle riforme del settore. Nella stessa linea, la proposta normativa sullo Spazio europeo dei dati sanitari dovrà realizzare un congruo bilanciamento tra condivisione, anche a fini di ricerca, di questo particolare tipo d'informazioni e la tutela rafforzata che esse meritano.

Particolarmente importanti sono, del resto, il *Digital Services Act* e il *Digital Markets Act*, presentati dalla Commissione con l'intento di introdurre una regolazione essenziale del potere privato delle piattaforme. A tal fine se ne rafforzano gli obblighi (di informazione, lealtà, correttezza ma più in generale responsabilizzazione) e, per converso, si riconosce all'utente una gamma di strumenti di intervento volti a promuoverne, anche in forma proattiva, la tutela ad ampio spettro.

Ma non meno significative sono anche le proposte normative sul *targeting* politico e sul lavoro su piattaforma, entrambe le quali affrontano, sia pure da punti di vista diversi, i rischi di involuzione sociale e democratica connessi a un abuso delle nuove tecnologie. La *gig economy*, con il rischio di un nuovo caporalato digitale, ma anche il targeting politico funzionale al condizionamento del consenso, sono, infatti, due emblemi significativi dell'esigenza di una *governanc*e del digitale che tenga conto delle implicazioni, potenzialmente distorsive, delle nuove tecnologie sulle coordinate essenziali della democrazia.

Si tratta, dunque, di disciplinare le condizioni per un utilizzo sostenibile della potenza di calcolo che, con la sua capacità di "colonizzare il pensiero" (L. Violante), rischia di incidere su quella libertà cognitiva necessaria per la garanzia di ogni altro diritto fondamentale. Il capitalismo delle piattaforme non è, infatti, più soltanto cognitivo (fondato dunque sulla raccolta delle informazioni) ma addirittura, come suggerisce Eric Sadin, delle "affezioni", in quanto tale da condizionare comportamenti partendo dall'analisi delle reazioni ai contenuti diffusi. Anche per questo la

privacy comportamentale è un presupposto essenziale di libertà a fronte del rischio di un costante pedinamento digitale: lo abbiamo ricordato, in particolare, con le Linee guida sui cookies, che contengono indicazioni importanti per un uso consapevole della rete.

Le implicazioni complessive delle riforme in discussione sono rilevanti. Esse contribuiscono infatti, ciascuna nel suo ambito, a una rimodulazione generale dell'assetto dei poteri così scardinato dal digitale, in una direzione funzionale alla tutela della persona (e della stessa libertà di espressione), contrastando gli effetti distorsivi di una tecnica altrimenti anomica. E il dibattito statunitense di questi giorni, sulla rimozione dai *social* dei contenuti relativi a farmaci abortivi, dimostra quanto cruciale sia una regolazione delle piattaforme realmente conforme ai valori di una democrazia.

La protezione dei dati rappresenta un elemento costitutivo di questo disegno regolatorio europeo, anche in funzione di contenimento dei poteri privati. Esso, infatti, presuppone anzitutto, in capo alle piattaforme, obblighi di trasparenza e responsabilizzazione mutuati dalla disciplina privacy e con essa interrelati. Di qui anche l'estensione delle competenze delle Autorità di protezione dati (si pensi alla direttiva sul lavoro mediante piattaforme o al regolamento sul targeting politico), pur al di là di una loro attribuzione formale di specifici ruoli (come pure si è auspicato per l'*Artificial Intelligence* Act e il *Digital Services Act*).

Le Autorità di protezione dei dati s'inseriscono dunque, pienamente, nel disegno riformatore europeo, di cui sono anzi interpreti d'avanguardia. Esse sono state infatti chiamate ad applicare la prima effettiva, organica regolazione del digitale, che non a caso viene assunta a modello in molti altri Paesi (effetto Bruxelles), tra i quali, da ultimo, la Cina o comunque esige un'uniformazione delle garanzie a livello globale, come dimostra la vicenda delle sentenze Schrems e dei successivi accordi con gli Usa. Un'eccessiva asimmetria nel livello di garanzie accordate

dagli ordinamenti dei Paesi terzi nel trattamento dei dati personali determina, infatti, l'impossibilità di avvalersi di canali più agevoli per il trasferimento dei dati, con l'esigenza di bloccare i flussi informativi che non siano assistiti da misure di protezione adeguate. E' quanto si è dovuto ricordare, anche recentemente, con il provvedimento su Google Analytics, che affronta le implicazioni (anche in termini di sovranità digitale e indipendenza tecnologica) dell'asimmetria, e livello internazionale, nella regolazione dell'uso dei dati: infrastruttura strategica per lo sviluppo dei Paesi, come ha sottolineato il Ministro del lavoro e delle politiche sociali.

Ecco anche perché la protezione dei dati assurge sempre più a fattore determinante della geopolitica, in un contesto in cui, se la Cina tende a far coincidere spazio fisico e virtuale, confini territoriali e risorse informative, per parte opposta anche negli Stati Uniti si discute di rideclinare in forme nuove l'idea di sovranità digitale.

3. Il dialogo istituzionale

La centralità della protezione dei dati nel contesto sociale attuale si riflette sul ruolo del Garante e sul suo coinvolgimento, sempre più rilevante, nella dinamica istituzionale. Nell'ultimo anno si è registrato, in particolare, un incremento rilevante (nell'ordine di circa il 50%*)* nel numero di pareri su (schemi di) atti legislativi o regolamentari, nonché di audizioni parlamentari, sia in sede di istruttoria legislativa sia nell'ambito di specifiche indagini conoscitive promosse anche da commissioni d'inchiesta (come ad esempio è stato per quelle sul femminicidio o sulla tutela dei consumatori**),** anche di là, dunque, dalla sola consultazione obbligatoria.

Proprio la varietà dei contesti istituzionali in cui il contributo del Garante viene richiesto dimostra come si stia, progressivamente, diffondendo la consapevolezza dell'esigenza di progettare le riforme, in qualsiasi campo, secondo una prospettiva *privacy-*

oriented, per promuovere innovazioni che siano realmente inclusive e non determinino, sia pur per mera preterintenzione, discriminazioni.

Il coinvolgimento del Garante, in varie forme e nelle diverse fasi del procedimento normativo (inclusa dunque quella attuativa*)* ha consentito, ad esempio, alla disciplina del *green pass* di delineare progressivamente, per approssimazioni successive, un equilibrio ragionevole tra esigenze di sanità pubblica, riservatezza individuale e autodeterminazione in ordine alle scelte sanitarie.

Attraverso l'audizione del Garante sui principali snodi dell'evoluzione normativa che ha caratterizzato la materia e la sua consultazione sui provvedimenti attuativi, si sono infatti approntate le garanzie necessarie, tra le altro, per consentire la verifica della certificazione senza, però, renderne ostensibile il presupposto di rilascio. Si è potuto così impedire l'indebita conoscenza, da parte di terzi, della condizione sanitaria o, comunque, delle scelte vaccinali del soggetto, tranne per il solo aspetto, su cui il monito del Garante è rimasto inascoltato, della facoltà di consegna della certificazione al datore di lavoro nel periodo di vigenza del relativo obbligo di verifica. Si è, inoltre, conferita maggiore determinatezza tanto all' "architettura" quanto alle finalità del trattamento, di cui si è correttamente prescritta la previsione con legge statale, in ragione delle riserve legislative su cui incide la disciplina.

Costruttivo e determinante è stato il confronto tra Camere, Governo e Garante sul *telemarketing* illecito**,** che resta un fenomeno endemico, al punto di essere assurto a simbolo dell'invadenza del mercato nella vita privata. Nell'ultimo anno, in particolare, con un emendamento al d.l. 'capienze' che ha esteso la riferibilità del registro delle opposizioni alle chiamate automatizzate, si è superato, nel senso auspicato dall'Autorità, uno stallo che ha impedito, per oltre due anni, la piena attuazione della l. n. 5 del 2018. Il che ha consentito anche l'approvazione del nuovo regolamento sul registro pubblico delle opposizioni, che ha recepito i rilievi espressi dal Garante con ben tre pareri e che determinerà, tra pochi giorni, il suo

effettivo funzionamento con estensione alle utenze mobili (e riservate), nonché alle chiamate automatizzate.

Il radicamento, nelle dinamiche economiche, del fenomeno del *telemarketing* illegale esige tuttavia una strategia di contrasto multilivello, che alla forza della disciplina normativa affianchi l'efficacia delle regole di settore. Così, il Garante ha incoraggiato e sostiene attivamente - come già ho rappresentato in Parlamento - il progetto di redazione di un codice di condotta in materia che, promuovendo la responsabilizzazione dei titolari favorisca comportamenti virtuosi, persino forse più di quanto possa riuscirvi la deterrenza esercitata dal quadro sanzionatorio, pur elevato e che anche quest'anno ha determinato l'irrogazione di sanzioni tra le più rilevanti per un Paese, quale il nostro, risultato al secondo posto per numero di sanzioni irrogate e quarto per ammontare complessivo (nell'ultimo anno pari a oltre 38 milioni di euro per il solo *telemarketing*).

Un altro contesto sul quale la consultazione del Garante è stata intensa è quello fiscale, interessato ora peraltro da una delega legislativa che, nel suo sviluppo, dovrà delineare quel congruo equilibrio tra esigenze di contrasto degli illeciti e riservatezza dei contribuenti, cui alludevamo in audizione sulle politiche fiscali. Le indicazioni del Garante volte a migliorare gli standard di esattezza e qualità dei dati trattati contribuiranno, peraltro, ad assicurare una più corretta rappresentazione della capacità contributiva degli interessati, migliorando complessivamente l'efficacia dell'analisi del rischio fiscale su cui si fonda buona parte delle politiche di contrasto in materia.

Nello sviluppo della delega si dovrà anche considerare che, (anche) in quest'ambito, sono necessari non tanto e non solo, genericamente, dati in maggiore quantità, ma di migliore qualità, non eterogenei per struttura e dimensione né soggetti al rischio di disallineamento, perché aggiornati. Solo in tal modo l'interoperabilità potrà offrire un contributo effettivo alla semplificazione e all'efficienza dell'azione amministrativa, come si

è del resto avuto modo di chiarire in relazione alla Piattaforma digitale nazionale dati ma anche alla complessiva materia della sanità digitale.

In quest'ultimo caso, poi, l'esigenza di qualità ed esattezza dei dati è ancor più rilevante, dal momento che un errore nel dato sanitario o un suo mancato aggiornamento può determinare, nel contesto clinico, rischi addirittura per la salute del paziente: tema ineludibile soprattutto per il fascicolo sanitario elettronico.

Proficua è stata l'interlocuzione anche rispetto a un tassello centrale, ancora mancante, della disciplina di protezione dati: il regolamento sui dati giudiziari *ex* art. 2-*octies* del Codice, necessario ai fini dell'individuazione dell'ambito legittimo di trattamento di questa particolare tipologia di dati, in particolare nel settore privato**.** Proprio in ragione della funzionalità di questa disciplina allo svolgimento di molte, rilevanti attività (anche) economiche in condizioni di sicurezza e affidabilità, lo stallo nell'adozione del testo definitivo dev'essere necessariamente superato.

4. Per un'innovazione non regressiva

Ancor più rilevante è e continuerà ad essere il confronto tra Camere, Governo e Garante sui provvedimenti attuativi del PNRR, su alcuni dei quali (in particolare sull'innovazione della p.a. e la sanità digitale*)* l'Autorità si è già pronunciata. E' importante mantenere questo dialogo costante anche e soprattutto dopo la denormativizzazione operata dal decreto-capienze rispetto ai presupposti del trattamento dei dati personali (non giudiziari, come chiarito in un recente provvedimento) in ambito pubblico.

La perdita di centralità della fonte normativa a favore di atti amministrativi generali rischia infatti, in assenza di una visione sinottica, di rendere disomogenei gli standard di tutela, laddove invece l'innovazione delle pubbliche amministrazioni dovrebbe

promuovere non soltanto l'efficienza dell'azione amministrativa ma anche l'inclusione, la partecipazione e, in ultima analisi, il superamento delle diseguaglianze.

Il Garante è pronto a supportare le amministrazioni in questo passaggio così determinante, nella consapevolezza di come la protezione dati abbia rappresentato sinora un fattore unificante (perché impone uniformità di garanzie), a fronte della frammentazione che, spesso, ha caratterizzato il processo di digitalizzazione nel nostro Paese, replicando se non addirittura accentuando la disomogeneità, su base territoriale, nel livello di prestazioni erogate.

Anche l'indagine conoscitiva avviata, dalle Autorità di protezione dati europee (tra cui il Garante), sul ricorso a sistemi *cloud* in ambito pubblico mira a indirizzare l'allocazione di asset informativi strategici in un percorso di piena sicurezza, che garantisca effettivamente indipendenza tecnologica.

Per questo l'innovazione - quale obiettivo trasversale di riforma - va declinata in termini più complessi della mera delega al digitale di più o meno significative funzioni pubbliche e private. Essa va intesa come un progetto di sviluppo organico e lungimirante, in cui la tecnica sia posta al servizio dell'uomo e non viceversa e in cui il progresso sia, anzitutto, progresso nei diritti. Il richiamo alla "resilienza" all'interno dell'acronimo PNRR è, in questo senso, molto più che uno slogan. Indica, infatti, la capacità dell'Europa prima (e, per essa, dei singoli Stati) di adattamento a congiunture avverse, come quelle emergenziali, senza tuttavia mai indebolire la garanzia dei diritti.

E' quanto, del resto, traiamo dall'esperienza della pandemia, che l'Italia e l'Europa tutta hanno affrontato senza mai porre un *aut aut* tra sanità e diritti individuali, tra solidarietà e libertà, ma coniugando queste istanze in modo da realizzarne il miglior equilibrio. L'attuazione delle riforme deve anzitutto far tesoro del lascito dell'esperienza di questi mesi difficili: la "lotta per il diritto" è anche e, soprattutto, lotta per l'affermazione del diritto nelle varie

emergenze che si ripropongono, soprattutto in un ordinamento, come il nostro, che non prevede stati di eccezione.

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. E per far questo è indispensabile che la digitalizzazione proceda parallelamente alle garanzie di protezione dei dati, tra le quali soprattutto i principi di minimizzazione, di sicurezza, di trasparenza del trattamento, come abbiamo avuto modo di sottolineare rispetto ad alcuni provvedimenti espressivi di politiche, anche sociali, innovative (Carta europea della disabilità, Registro nazionale tumori, Carta dello studente, Anagrafe nazionale degli assistiti, App Io, raccolta on line di firme per referendum e iniziativa legislativa popolare, Spid minori, Anagrafi dell'istruzione). Va, infatti, assicurato che il percorso di transizione digitale dell'azione amministrativa, in ogni campo, non avvenga rivelando dati, in particolare se soggetti a tutela rafforzata come quelli "sensibili", giudiziari o sui minori non strettamente indispensabili, non li esponga a rischi d'esfiltrazione e corrisponda sempre a quanto normativamente previsto e reso noto al cittadino. Il rischio, altrimenti, è quello di replicare, se non addirittura approfondire, le diseguaglianze esistenti, con un effetto paradossalmente regressivo in termini sociali. Le notevoli potenzialità in termini di efficienza ed efficacia delle politiche sociali, offerte dagli algoritmi devono dunque essere valorizzate minimizzando i rischi connessi a un uso poco attento delle neotecnologie, assicurandone un controllo costante sui possibili effetti distorsivi, non certo rinunciando ai benefici suscettibili di derivarne.

I rischi, in termini di discriminazione, potenzialmente connessi al *social scoring* (non a caso vietato, se basato sul monitoraggio individuale, dall'Artificial Intelligence Act) hanno indotto così, ad esempio, la nostra Autorità a disporre accertamenti sulle iniziative di alcuni enti territoriali volte a offrire incentivi a fronte di

comportamenti virtuosi dei cittadini, oggetto di monitoraggio o di una vera e propria profilazione.

Ecco, dunque, che il richiamo - frequente nel PNRR - all'innovazione, alla digitalizzazione, alla crescita non può mai essere disgiunto da una visione, di lungo periodo, più complessiva, che coniughi sviluppo e diritti.

La protezione dei dati assume dunque un ruolo baricentrico nel comporre queste istanze, tracciando la direzione intorno alla quale imprimere al Paese un'innovazione sostenibile anche in termini di diritti e libertà.

5. Libertà, giustizia, dignità

Particolarmente significativo è stato, in particolare in quest'anno, il confronto con il Governo sul tema dell'uso giudiziario dei tabulati, al centro di due importanti sentenze della Corte di giustizia europea.

Con la prima, del 2 marzo 2021, *H.K. c. Prokuratuur (C 746-18*) la Corte di giustizia ha sottolineato l'esigenza di terzietà, rispetto al soggetto pubblico richiedente, dell'autorità titolare del potere di acquisizione dei tabulati. A seguito di tale pronuncia il Garante aveva rivolto, nel luglio scorso, una segnalazione al Parlamento e al Governo, volta a suggerire una riforma della disciplina modulata sulla piena giurisdizionalizzazione del procedimento acquisitivo e sulla revisione, in senso maggiormente conforme al canone di proporzionalità, di condizioni, limiti e termini di conservazione dei tabulati.

Sviluppando le indicazioni della Corte (e della stessa segnalazione), il Governo ha sottoposto al parere del Garante uno schema di decreto-legge di revisione della disciplina della *data retention* che, oltre ad attribuire al giudice la competenza autorizzatoria in materia, ha limitato la possibilità di acquisizione dei tabulati ai soli procedimenti per reati connotati da una determinata gravità, in presenza di sufficienti indizi e della

rilevanza dell'acquisizione ai fini dell'accertamento dei fatti. Il testo definitivo del decreto-legge (n. 132 del 2021), già in linea con la segnalazione, ha anche recepito le indicazioni del Garante sull'esercizio, da parte degli interessati, dei propri diritti in relazione ai dati contenuti nei tabulati.

Si è così realizzato un rilevante (ancorché non del tutto risolutivo) avanzamento nelle garanzie correlate all'acquisizione dei tabulati, in virtù della convergenza tra terzietà nella fase autorizzatoria e limitazione oggettiva dei casi di ammissibilità. Ma anche quest'assetto sembra destinato ad essere superato dai rilievi più dirimenti espressi con la sentenza C-140/20 del 5 aprile scorso, con la quale la Corte di giustizia Ue ha chiarito come la *co*nservazione dei tabulati a fini di giustizia non possa essere generalizzata e indifferenziata, ma soltanto "mirata" sulla base di criteri soggettivi, geografici o di altra natura (purché oggettivi e non discriminatori) ovvero "rapida" (*quick freeze*). La Corte suggerisce, dunque, una vera e propria mutazione della natura di questo strumento investigativo, che esigerà un'ampia riforma della disciplina interna. Essa, infatti, - pur a fronte di una differenziazione per titolo di reato in fase acquisitiva - presuppone, comunque, la conservazione preventiva e generalizzata dei dati di traffico relativi alla generalità indistinta dei cittadini. Dovranno, dunque, essere disciplinati, non solamente la conservazione rapida e il relativo accesso, ma soprattutto i parametri (oggettivi e non discriminatorii) sulla base dei quali procedere alla conservazione mirata dei dati di traffico e relativi all'ubicazione, da utilizzare a fini di contrasto di reati gravi.

Il ricorso alle neotecnologie nell'ambito delle attività di contrasto può amplificarne, in assenza di un quadro organico di garanzie, i rischi tanto sul piano individuale quanto su quello collettivo. La congiunzione tra potere d'indagine e potenza della tecnica impone, infatti, la previsione di limiti tanto più stringenti quanto più avanzato sia il grado d'autonomia decisionale della macchina. In questo senso, l'utilizzo dell'intelligenza artificiale nel settore investigativo dev'essere circondato delle garanzie

necessarie ad evitare la delega all'algoritmo di attività della massima delicatezza perché, tra l'altro, potenzialmente incidenti sulla libertà personale. Per questo, ad esempio, il Garante ha escluso che il ricorso alle *body cam*, da parte delle autorità di pubblica sicurezza, potesse di per sé legittimare anche il riconoscimento facciale in ragione dei rischi, per la dignità e libertà individuali, ad esso connessi, su cui ci ammoniscono anche le recenti Linee guida del Comitato europeo per la protezione dei dati. Ed è significativo che, con un emendamento al d.l. 'capienze', si sia introdotta una generale moratoria nel ricorso al riconoscimento facciale, ammesso solo in ambito di polizia - previo parere favorevole del Garante - o giudiziario. I rischi di un monitoraggio su base biometrica dei cittadini, realizzato peraltro da soggetti privati "rastrellando" dati dalla rete (*web scraping*) è, del resto, alla base del provvedimento inibitorio e sanzionatorio (dell'entità di venti milioni di euro) adottato nei confronti di Clearview.

Il rapporto tra esercizio della funzione giurisdizionale, informazione e privacy - tra i più complessi del nostro sistema giuridico- è stato, peraltro, oggetto di recenti modifiche normative di rilievo. Da un lato, infatti, la riforma del processo penale ha previsto (quale criterio direttivo per l'esercizio della delega legislativa) che le pronunce giurisdizionali favorevoli costituiscano titolo per un provvedimento di deindicizzazione che, nel rispetto della normativa in materia di protezione dei dati personali, garantisca il diritto all'oblio dell'interessato. La pronuncia favorevole assurge, dunque, a presupposto normativo per una specifica tutela della privacy (già, peraltro, accordata in questi termini da una consolidata prassi del Garante), che coniuga esigenze informative e riservatezza individuale.

Particolarmente rilevante è anche il d.lgs. 188 del 2021, che ha introdotto un articolato sistema di tutele del diritto dell'indagato o dell'imputato a non essere indicato "pubblicamente come colpevole" finché non ne sia definitivamente accertata la

responsabilità penale, unitamente a nuove modalità di gestione del rapporto tra giustizia e informazione. Parallelamente a queste garanzie extraprocessuali della presunzione d'innocenza, si introducono poi ulteriori garanzie specificamente intraprocessuali, rilevanti (anche) quali parametri di redazione degli atti. Si rimodula, dunque, il rapporto tra comunicazione sulla giustizia e dignità personale, nella condivisibile direzione di una loro effettiva sinergia.

6. Vecchie e nuove vulnerabilità

Tra le direttrici dell'attività del Garante che più si stanno accentuando vi è quella incentrata sulla tutela della persona che versi, per qualità soggettiva o per contesto oggettivo, in condizioni di particolare vulnerabilità. Se, infatti, protezione dei dati personali è, sempre, diritto al libero sviluppo della propria personalità, in condizioni di autodeterminazione informativa, nel caso dei soggetti più vulnerabili essa è anche di più. E' tutela della persona (della sua identità, dignità, finanche libertà) da discriminazioni vecchie e nuove, spesso amplificate dalla potenza della rete o accentuate dalla (solo pretesa) neutralità dell'algoritmo.

Quest'obiettivo di tutela - indicato già un anno fa come prioritario per il nostro mandato - è sotteso a pressoché tutta l'attività del Garante; ne qualifica anzi l'identità come Autorità per la tutela delle (di tutte le) persone (neppure soltanto dei cittadini). Ma, nell'anno trascorso, alcune specifiche esigenze di tutela sono emerse, in modo particolare, nel contesto dell'informazione e nel rapporto di lavoro. Per quanto riguarda il giornalismo, si è avuto modo, in particolare, di sottolineare come l'esigenza informativa vada soddisfatta nel rispetto del criterio di essenzialità (come ad esempio si è ribadito per il caso del liceo Montale di Roma), ma soprattutto senza indulgere a forme di spettacolarizzazione del dolore o sensazionalismo, suscettibili di pregiudicare ulteriormente la condizione delle vittime e dei loro familiari.

Il giornalismo vive del costante equilibrio tra diritto di (e all') informazione e dignità della persona, che mai va strumentalizzata a fini di cronaca; soprattutto se versi in condizioni di particolare vulnerabilità: minori, malati detenuti, arrestati. Ecco la ragione per cui, anche a proposito della guerra, abbiamo ribadito l'esigenza di evitare, pur nel prezioso esercizio della libertà di stampa, la spettacolarizzazione del dolore, espresso dalla forza drammatica dei corpi straziati, soprattutto dei bambini. La narrazione della guerra - cui non dobbiamo mai assuefarci come a uno spettacolo da osservare, quasi anestetizzati, da comoda distanza - non ha bisogno di sacrificare la dignità della persona per soddisfare le pur legittime esigenze informative.

Nel corso dell'anno sono stati diversi i casi nei quali il Garante ha rappresentato l'esigenza di non indulgere sulla "personalizzazione del dramma", sull'imprimere alle tragedie (che pur vanno raccontate) necessariamente il volto straziato, martoriato, offeso delle vittime e i dettagli della loro vita privata non essenziali alla descrizione dei fatti. Lo si è sottolineato, ad esempio, rispetto al bambino ucciso a Vetralla e alla bimba morta a Cisliano, a fronte di un eccesso informativo incompatibile con la tutela rafforzata della riservatezza accordata ai minori (non solo in vita) dall'ordinamento.

Analogamente, meritano una tutela specifica i soggetti sottoposti a misure limitative della libertà personale che- come è stato necessario ricordare anche quest'anno – non devono essere ripresi, in chiaro, in tali condizioni e vanno protetti – come afferma, per le traduzioni, la legge sull'ordinamento penitenziario– dalla mera "curiosità del pubblico".

L'esigenza di tutela rafforzata delle persone (non soltanto minori) che versino in condizioni di fragilità va, peraltro, osservata anche al di fuori del contesto giornalistico in senso stretto ed anche laddove la pubblicazione sia sostenuta da fini di "denuncia" anche politica, come si è avuto modo di sottolineare rispetto alla diffusione, via *social,* di video e foto di ragazzi disabili o in situazioni di disagio socio-economico.

Analogamente, è stata sanzionata la diffusione sul web, da parte di una pubblica amministrazione, dei dati personali degli studenti percettori di sussidi economici riservati a nuclei familiari con reddito inferiore a una determinata soglia, così rivelandone la condizione di disagio socio-economico che la disciplina sulla trasparenza amministrativa vuole, correttamente, sottratta a pubblicità. Anche in tal caso, il fine sotteso al divieto di diffusione è quello di evitare discriminazioni e stigmatizzazioni riferite alle condizioni di vulnerabilità del soggetto, che per questo merita invece una tutela rafforzata e specifica, tale da rappresentare anche un limite interno agli obblighi di pubblicità.

Analoga tutela specifica s'impone per quella peculiare condizione di debolezza propria del lavoratore, dovuta alla sua posizione all'interno di un rapporto strutturalmente asimmetrico, quale quello di lavoro, non a caso destinatario, con la l. 300 del 1970, delle prime norme dell'ordinamento a tutela dell'autodeterminazione informativa. Tra queste, in particolare, il divieto di controllo a distanza dell'attività lavorativa, funzionale a evitare ingerenze datoriali indebite nella sfera di riservatezza dei lavoratori.

Così, si è precisato che anche i sistemi di *customer care* dai quali derivi, sia pur indirettamente, un controllo sull'attività lavorativa necessitano delle garanzie (concertazione sindacale o autorizzazione amministrativa) previste dallo Statuto dei lavoratori, pena un'indebita elusione di tale forma di tutela. Analoga elusione è stata stigmatizzata rispetto al monitoraggio indiscriminato e preventivo della navigazione in internet dei lavoratori, inammissibile in quanto tale, appunto, da annullare quelle garanzie essenziali di autodeterminazione riconosciute come indispensabili sin dal 1970.

Per altro verso, in sede consultiva, si sono suggerite alcune integrazioni volte a ulteriormente perfezionare un già condivisibile disegno di legge governativo per l'introduzione di alcune garanzie essenziali nel contesto del lavoro mediante piattaforma. Si è, in particolare, condivisa la scelta – già sottesa alla corrispondente

direttiva europea – di disciplinare condizioni e tutele specifiche, anche in termini di equità e trasparenza, per il ricorso a processi decisionali automatizzati con effetti sul rapporto di lavoro.

7. Una tutela inclusiva

Se la tutela della persona in condizioni di particolari vulnerabilità è una componente (sempre più) rilevante della protezione dei dati personali, lo è non certo per mera contingenza ma per un'intima, originaria, vocazione di questo diritto al riequilibrio dei rapporti sociali e alla ridefinizione degli assetti di potere.

Questa vocazione viene oggi valorizzata dal legislatore, che proprio in quest'anno ha attribuito all'Autorità funzioni rilevanti sul terreno della tutela dei soggetti più vulnerabili, secondo il paradigma, risultato particolarmente efficace, del cyberbullismo. Il "decreto-capienze" ha, infatti, esteso tale modello di tutela al *revenge porn*, legittimando (anche gli ultraquattordicenni) a presentare istanza, al Garante, di blocco del caricamento di contenuti intimi riguardanti il richiedente, in presenza di specifici presupposti. I primi provvedimenti, approvati sulla base di tale disciplina, si sono dimostrati particolarmente efficaci nel prevenire la diffusione di contenuti suscettibili di arrecare pregiudizi, anche gravissimi – come insegna la tragedia di Tiziana Cantone – alla dignità della persona.

Questi nuovi strumenti risulteranno particolarmente utili a tutelare soprattutto i minori, che sembrano purtroppo assurgere a vittime elettive dell'accelerazione del processo di digitalizzazione innescato dalla pandemia, come si evince dall'incremento del 295% dei casi di abusi su minori trattati dalla Polizia postale e delle comunicazioni, rispetto ai dati prepandemici del 2019, con un significativo aumento delle vittime di età compresa tra i dieci e i tredici anni, per quanto concerne la pedopornografia. Anche tenendo conto di questi elementi, nell'ambito del Tavolo per la

tutela dei minori *on line* istituito presso il Ministero della giustizia si è condivisa, in particolare, l'opportunità di rafforzare le garanzie di *age verification* promuovendo il ricorso alla certificazione dell'identità da parte di terzi; introdurre norme a tutela dei *baby influencer*, verificandone i profitti generati online; estendere al fenomeno dello *sharenting* (diffusione d'immagini di minori da parte di adulti di riferimento) la tutela remediale, accordata al minore, sul terreno del cyberbullismo.

Anche per quanto riguarda un uso consapevole della rete da parte dei minori**,** risulterà rilevante il ruolo attribuito, sul terreno della pedagogia digitale, al Garante, che può ora prescrivere (o, comunque, valutare ai fini della commisurazione sanzionatoria) l'effettuazione, da parte del titolare del trattamento, di campagne di comunicazione istituzionale volte alla promozione della consapevolezza del diritto alla protezione dei dati personali.

Promuovere la "cultura" della protezione dei dati è certamente una delle soluzioni più importanti per favorire comportamenti virtuosi sia da parte dei titolari del trattamento che degli stessi interessati, spesso ignari dell'importanza di proteggere, con i propri dati, la propria libertà, con il rischio di divenire schiavi della "dittatura della presenza" (M. Serra).

Profetiche le parole di Umberto Eco, secondo cui il compito più significativo delle autorità di garanzia della privacy sarebbe stato non tanto e non solo "di assicurarla a coloro che la sollecitano (…) bensì di farla considerare un bene prezioso a coloro che vi hanno entusiasticamente rinunciato", pur di liberarsi, con la micro-celebrità che assicurano le neotecnologie, di uno "spaventoso e insopportabile anonimato".

E' stato peraltro approvato, in prima lettura, un progetto di legge che condivisibilmente attribuisce al Garante la competenza a decidere le istanze - presentate anche da minori, se ultra quattordicenni - di rimozione di contenuti istigativi al suicidio. Anche in tal caso, si intende contenere gli effetti pregiudizievoli della diffusione virale di comunicazioni suscettibili di

condizionare, talora anche fatalmente, il comportamento degli utenti, soprattutto se minorenni.

Ecco perché il Garante sta divenendo progressivamente, sempre più, Autorità a tutela non già della persona digitale ma della persona, complessivamente intesa, (anche e soprattutto) nel digitale. Alcuni emendamenti e progetti di legge hanno colto, correttamente, lo spirito di quest'evoluzione, proponendo di designare il Garante quale Autorità per i diritti fondamentali.

Di là dalla soluzione legislativa, queste proposte sottendono una consapevolezza nuova e significativa, che è emersa con sempre maggiore nettezza nel corso dei venticinque anni dall'istituzione del Garante, in un processo di progressiva "democratizzazione" di un diritto, la cui vocazione liberale e garantista affonda le sue radici proprio in quel "*penumbral right*" della sentenza Roe v. Wade.

Oggi quel diritto - arricchitosi di implicazioni e contenuti nuovi - riafferma e valorizza, ulteriormente, la sua caratterizzazione democratica. In un contesto in cui i dati, anche e soprattutto personali, rappresentano le principali e più rilevanti risorse per l'economia, per la ricerca, per la crescita sociale, per l'attività politico-istituzionale, l'autodeterminazione informativa assurge, infatti, a presupposto ineludibile di altri diritti e libertà fondamentali, per la promozione dell'umanesimo digitale.

Ed ecco perché la protezione dei dati personali costituisce, sempre più, una componente centrale delle democrazie liberali, allorché garantisce che l'innovazione, l'iniziativa economica, l'attività pubblica in ogni campo non violino - con un indebito sfruttamento dei dati e contraddicendo la stessa natura dello Stato di diritto - la dignità della persona. Soprattutto la dignità di soggetti quali minori, migranti, malati, detenuti, vittime o appartenenti a minoranze comunque individuate; di tutti coloro, cioè, la cui fragilità - per natura o per circostanza - rischia di renderli davvero "nudi" di fronte al potere: dello Stato, del mercato, della tecnica.

E proprio il potere della tecnica determina non solto nuove vulnerabilità ma addirittura nuove soggettività che esigono tutela:

tra tutti, il “gemello digitale” di ciascuno di noi in quella dimensione sempre più “iperreale”- nell’accezione di Baudrillard - che appare il Metaverso. Anche per queste nuove istanze sociali la protezione dei dati può rappresentare uno strumento importante di tutela inclusiva, perché una tecnica sempre più ingiuntiva (demiurgica, predittiva e quindi performativa) non degeneri in egemonia distopica dell’algoritmo, in “gabbia di durissimo acciaio” di weberiana memoria. L’obiettivo da perseguire è promuovere una vera e propria civiltà digitale, in cui la direzione dell’innovazione sia ancora agita e non subita dall’uomo, a partire dalla definizione delle coordinate assiologiche in cui inscrivere uno sviluppo tecnologico inclusivo, concependo il confine (anche con l’altro-da-sé) non solo come “*limes*, frontiera rigida, ma sempre anche come *limen*, cioè soglia, contatto” (M. Magatti).

Il Garante accoglie questa sfida con senso di responsabilità e di consapevolezza dell’importanza dell’obiettivo, da perseguire grazie al lavoro costante e attento 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.

Con l’auspicio di sapere sempre, come da venticinque anni, “guardare negli occhi il destino del proprio tempo” (Max Weber).