GPDP

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Tecnica, protezione dei dati e nuove vulnerabilità

Relazione del Presidente Pasquale Stanzione 2020

Roma, 2 luglio 2021

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Piazza Venezia, 11
00187 Roma
Tel. 06 696771
email: protocollo@gpdp.it
www.gpdp.it

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Tecnica, protezione dei dati e nuove vulnerabilità

Relazione del Presidente Pasquale Stanzione
2020

Signor Presidente della Camera, Autorità, Signore e Signori,

la presentazione di questa relazione ha un significato particolare, perché nel delineare l'orizzonte del nostro mandato esprime la consapevolezza dei temi, delle urgenze, dei problemi che questo primo anno di lavoro molto intenso ci ha offerto.

Il Collegio che mi pregio di presiedere ha sentito di dover onorare l'alto incarico ricevuto dal Parlamento con spirito di servizio nei confronti dei cittadini, assicurando loro in ogni contesto, senza distinzioni, l'effettività del diritto alla protezione dei dati personali.

Era questo, in particolare, il retaggio espressamente affidatoci un anno fa dal precedente Collegio, nella sua ultima Relazione.

Lo abbiamo raccolto con senso di responsabilità nei confronti del Paese tutto, in cui si sta affermando, con forza progressivamente maggiore, la consapevolezza del valore di questo straordinario diritto.

Esso si manifesta, in maniera sempre più netta, come requisito ad un tempo di libertà e di democrazia, assicurando al singolo le condizioni per la libera costruzione di sé e alla società il giusto equilibrio tra privato e pubblico, tra diritti e solidarietà.

La più grande forza di questo diritto, mai dispotico, è infatti la sua "mitezza", la sua capacità cioè di realizzare inattese sinergie con i vari interessi in gioco, fornendo all'innovazione un governo antropocentrico, iscritto in un orizzonte di senso, perché sia la tecnica al servizio dell'uomo e non viceversa.

1. Emergenza, non eccezione

La funzione sociale della privacy è resa ancor più evidente in una congiuntura, come l'attuale, contraddistinta da rilevanti trasformazioni nel rapporto tra singolo e collettività, tra libertà e poteri, che rendono questa una stagione quasi costituente sotto il profilo della garanzia dei diritti.

La permanenza della condizione pandemica ci ha insegnato a convivere con le limitazioni dei diritti,

tracciando tuttavia il confine che separa la deroga dall'anomia, dimostrando come la democrazia debba saper lottare, sempre, con una mano dietro la schiena.

Ma quella della democrazia liberale contro le derive autoritarie è una vittoria da rinnovare giorno per giorno mai dandola per acquisita, come ha fatto l'Europa che ha dimostrato, anche in quest'occasione, di saper coniugare, senza contrapporle, libertà e solidarietà, sfuggendo alla tentazione delle scorciatoie tecnocratiche della biosorveglianza.

E se la traslazione on line della vita e la funzionalizzazione, a fini sanitari, della tecnica è stata possibile senza cedere allo stato di eccezione, ciò non ha comunque potuto impedire una profonda trasformazione sociale, culturale e perfino antropologica di cui la pandemia è stata un catalizzatore, rivelando quanto sia profonda l'interrelazione tra la nostra vita e il digitale.

A partire dai primi mesi di lockdown e con effetti, tuttavia, verosimilmente destinati a perdurare, alle piattaforme è stata affidata la stragrande maggioranza delle nostre attività quotidiane; la parte più significativa degli scambi commerciali è avvenuta on-line, persino

le prestazioni sociali più rilevanti (dalla scuola all'università, dai servizi amministrativi alla giustizia) sono state erogate da remoto.

In fondo, se il distanziamento fisico imposto per esigenze sanitarie non è divenuto anche sociale, lo si deve alle nuove tecnologie, capaci di ricreare nello spazio virtuale quei legami impediti nel reale, pur costringendoci a ripensare il sistema delle garanzie nel passaggio dall'off-line all'on-line.

2. Il capitalismo delle piattaforme

Il digitale ha, così, dimostrato di poter essere al servizio dell'uomo, ma non senza un prezzo di cui bisogna avere consapevolezza: l'accentramento progressivo, in capo alle piattaforme, di un potere che non è più soltanto economico, ma anche - e sempre più - performativo, sociale, persino decisionale.

Un potere che si innerva nelle strutture economico-sociali, fino a permeare quel "caporalato digitale" rispetto ai lavoratori della gig economy, protagonisti (anche in Italia) del primo sciopero contro l'algoritmo:

gli “invisibili digitali”, come da taluno sono stati definiti.

I “gatekeepers”, appunto, stanno assumendo un ruolo sempre più determinante nelle dinamiche collettive, economiche, persino politiche, assurgendo a veri e propri poteri privati scevri, tuttavia, di un adeguato statuto di responsabilità.

La pandemia ha dimostrato l’indispensabilità dei servizi da loro forniti ma, al contempo, anche l’esigenza di una strategia difensiva rispetto al loro pervasivo ‘pedinamento digitale’, alla supremazia contrattuale, alla stessa egemonia “sovrastrutturale”, dunque culturale e informativa, realizzata con pubblicità mirata e microtargeting.

Di più. La sospensione degli account Facebook e Twitter di Donald Trump ha rappresentato plasticamente come le scelte di un soggetto privato, quale il gestore di un social network, possano decidere le sorti del dibattito pubblico, limitando a propria discrezione il perimetro delle esternazioni persino di un Capo di Stato.

Il private enforcement dei social sembra, dunque,

aver superato finanche quei limiti posti del Communication Decency Act, ritenuti incostituzionali dalla Corte Suprema.

E nel nostro ordinamento, a fronte dell'oscuramento del profilo social di un movimento politico per diffusione di contenuti contrari alla policy del gestore, il Tribunale di Roma ha rilevato come il pur ordinario contratto privatistico di fornitura del servizio di social network soggiaccia a una peculiare forma di eteroregolazione dovuta alla sua incidenza su diritti fondamentali.

E' questo il nodo di fondo del capitalismo delle piattaforme: l'esigenza di una loro cooperazione nell'impedire che la rete divenga uno spazio anomico dove impunemente si possano violare diritti, senza tuttavia ascrivere loro un ruolo arbitrale rispetto alle libertà fondamentali e al loro bilanciamento, da riservare pur sempre all'autorità pubblica.

Su questo crinale stretto si muove il Digital Services Act (DSA), così da introdurre forme di responsabilizzazione delle piattaforme, il cui potere di moderazione dei contenuti viene assoggettato ad

obblighi di trasparenza e a rimedi impugnatori che ne consentano un sia pur minimo sindacato esterno.

L'approvazione di questo testo, oltre che del Digital Markets Act (DMA), auspicabilmente con le modifiche richieste dal Garante europeo, segnerà per ciò un passaggio importante, superando almeno in parte lo schermo immunitario che, sinora, ha reso i big tech attori egemoni - tanto quanto irresponsabili - nel contesto economico, informativo, sociale.

Come abbiamo osservato in audizione al Senato, la responsabilizzazione delle piattaforme sarà determinante tra l'altro per contrastare la manipolazione delle notizie che, nello scorso anno, ha assunto i tratti di una vera e propria infodemia.

Intervenendo in maniera complementare su aspetti diversi, tanto il DSA quanto il DMA rafforzeranno inoltre la garanzia della libertà cognitiva dell'utente-consumatore, quale diritto di non subire il potere pervasivo di condizionamento del microtargeting e del marketing fondato su tecniche psicometriche, volto a potenziarne la capacità persuasiva adattando il messaggio alle preferenze e alle inclinazioni desunte dalla profilazione algoritmica.

Non è un caso che, negli Usa, l'accesso alla "scatola nera" degli algoritmi, per verificarne l'impatto sulla circolazione delle notizie, sulla loro amplificazione e dunque sulla formazione dell'opinione pubblica, sia divenuto oggetto di richieste sempre più frequenti da parte di esponenti politici di opposti schieramenti.

Questa potentissima forma di "nudging", tesa ad orientare le scelte degli utenti secondo la stima predittiva dell'algoritmo, rivela quanto i singoli siano disarmati di fronte al potere performativo del digitale.

In un contesto definito di "capitalismo estrattivo"- per l'attitudine predatoria delle piattaforme nei confronti dei dati, liberamente attinti come fossero res nullius - è indispensabile rafforzare - come ha fatto ad esempio la Corte di giustizia europea con la sentenza di novembre sul consenso on line e come fa lo schema di regolamento e-privacy - l'autodeterminazione informativa.

In questa direzione il Garante ha, ad esempio, sottoposto al Comitato europeo per la protezione dei dati l'esigenza di accertare l'effettiva idoneità dell'informativa fornita da Whatsapp apparsa poco chiara,

a consentire agli utenti la manifestazione di una volontà libera e consapevole. Essa presuppone del resto, come ha chiarito una recente sentenza di legittimità, la piena conoscenza della logica algoritmica applicata al trattamento, che deve essere inclusa dunque nell'oggetto del consenso.

L'autodeterminazione informativa è, infatti, il necessario presupposto di scelte libere e, appunto, consapevoli, in un contesto in cui servizi apparentemente gratuiti sono invece pagati al caro prezzo dei nostri dati e, quindi, della nostra libertà. Perché "quando è gratis, il prodotto sei tu".

3. La "geopolitica" della privacy

L'attenzione riservata, tanto dalla Corte di giustizia quanto dal legislatore europeo ai requisiti di effettiva libertà e consapevolezza del consenso dimostra quanto l'autodeterminazione informativa sia determinante per un governo sostenibile della società (e dell'economia) delle piattaforme.

Una più netta presa di coscienza del valore dei

propri dati è, infatti, l'unico, effettivo baluardo contro il rischio della monetizzazione della privacy, che rappresenta oggi la vera questione democratica nel governo della rete.

Da un lato, infatti, la zero price economy ha reso prassi ordinaria lo schema negoziale 'servizi contro dati'; dall'altro, riconoscere la possibilità della remunerazione del consenso rischia di determinare una rifeudalizzazione dei rapporti sociali, ammettendo che si possa pagare con i propri dati e, quindi, con la propria libertà.

Su questo "pendio scivoloso" è in gioco, forse più che in ogni altro campo, l'identità europea come "Comunità di diritto", fondata sulla sinergia tra libertà, dignità, eguaglianza, quali presidi essenziali che nessuna ragion di Stato o, tantomeno, di mercato può violare.

E' significativo che l'Unione Europea abbia negli ultimi cinque anni (a partire, in particolare, dal nuovo quadro giuridico sulla privacy, sino al recente schema di regolamento sull'intelligenza artificiale) messo al centro della propria agenda politica la regolazione del digitale, consapevole che l'anomia cui altrimenti

sarebbe consegnata la rete non esprime libertà, ma soggezione alla lex mercatoria, tanto quanto alla lex informatica.

Se "code is law" è perché il digitale esprime un nuovo paradigma di senso, un nuovo ordine antropologico e simbolico che va coniugato con il sistema, anzitutto di valori, proprio del rule of law cui s'ispira la costruzione europea.

E proprio sul governo antropocentrico del digitale l'Unione europea sta promuovendo - adesso anche con lo schema di regolamento citato - uno sviluppo sostenibile dell'innovazione, che la renda funzionale al progresso sociale.

Questa vocazione personalista contraddistingue, certamente, le politiche dell'innovazione europee dall'"imperialismo digitale" cinese, con la sua pericolosa alleanza tra potenza di calcolo e potere coercitivo, di cui il social credit system e il riconoscimento facciale (persino "emotivo") sono un esempio emblematico.

Ma la "differenza" europea connota, ancora una volta sul terreno della privacy, anche il rapporto con gli Stati

Uniti, sia per l'approccio liberistico all'innovazione, sia per il rapporto tra garanzie individuali e sicurezza nazionale.

Con la sentenza Schrems II del luglio 2020, infatti, la Corte di giustizia europea ha invalidato anche il Privacy Shield e la conseguente decisione di adeguatezza dell'ordinamento americano in ragione della carenza, per i dati lì trasferiti, di garanzie sostanzialmente equivalenti a quelle sancite dalla disciplina dell'Unione.

Importante anche che la Corte abbia subordinato la validità, ai fini del trasferimento dei dati all'estero, di strumenti privatistici (pur eteroregolati), quali le clausole contrattuali standard, a un sistema di rimedi effettivi nell'ordinamento di destinazione.

Ciò dimostra come la privacy necessiti di una tutela "oggettiva", che non si esaurisce nella fase negoziale rimessa alla sola disponibilità delle parti, ma esige tutele pubblicistiche effettive.

La privacy, come è stato detto, appare paradossalmente sempre meno una mera questione "privata" e, sempre più, un tema di rilievo pubblico centrale, su cui si misura, anche in termini geopolitici, la tenuta dello Stato di diritto.

4. Libertà e sicurezza: la sinergia necessaria

Nella valutazione di (in)adeguatezza del sistema di tutele accordate dall'ordinamento americano ha avuto un peso determinante il regime di accesso ai dati per fini investigativi, modulato in forme assai diverse da quelle invalse in Europa e ritenute determinanti ai fini della "identità costituzionale" europea.

La Corte di giustizia, sotto questo profilo, ha valorizzato la funzione democratica della privacy, capace di realizzare l'equilibrio tra libertà e sicurezza prescritto dall'art. 6 della Carta di Nizza e valorizzato ulteriormente da una recente pronuncia CEDU sull'illegittimità della sorveglianza massiva.

Il terreno elettivo di questa lettura garantista è stato, sin dalla sentenza Digital Rights, quello della data retention, rispetto alla quale proprio nei mesi scorsi la Corte ha sancito alcune affermazioni importanti.

Per un verso, infatti, con la sentenza Privacy International di ottobre, la Corte ha riconosciuto l'applicabilità della disciplina privacy alla conservazione dei tabulati, da parte dei gestori, per precostituire

materiale investigativo rilevante a fini di sicurezza nazionale.

In tal modo la Corte ha impedito che la finalizzazione secondaria a tali esigenze (escluse dall'ambito applicativo della disciplina privacy) potesse divenire il grimaldello per eluderne le garanzie in un ambito in cui, invece, proprio l'equilibrio realizzato da tale disciplina può rappresentare un importante presidio di libertà.

Per altro verso, con la sentenza del 2 marzo la Corte ha chiarito come l'acquisizione dei tabulati esiga il vaglio di un'autorità (giudiziaria o amministrativa indipendente) effettivamente terza rispetto all'organo inquirente e vada limitata ad esigenze di contrasto di gravi reati o minacce per la sicurezza pubblica.

Per questo, è stata recentemente sollevata questione pregiudiziale interpretativa relativamente alla compatibilità della disciplina italiana con quella europea; mentre, in un altro caso, alla sentenza della Corte è stata data attuazione riservando al gip l'autorizzazione all'acquisizione dei tabulati, limitatamente a procedimenti per reati che legittimino le intercettazioni in senso proprio.

Si tratta di una lettura fortemente garantista della disciplina privacy, che valorizza l'esigenza di terzietà e residualità rispetto all'uso di uno strumento investigativo assai più invasivo di quanto possa apparire.

Tali esigenze di garanzia dovrebbero essere valorizzate anche dal legislatore nazionale, chiamato in questo ambito a una riforma che il Garante ha più volte sollecitato e che, dopo l'accoglimento del relativo ordine del giorno al disegno di legge europea, appare finalmente ben avviata.

Come pure condivisibile e in linea con quanto da noi più volte richiesto è l'indirizzo impresso dal Parlamento al Governo rispetto alla limitazione dell'utilizzo di uno strumento polifunzionale e potenzialmente onnivoro, come il captatore informatico, alle sole attività di intercettazione ambientale previste dalla legge e autorizzate di volta in volta dal gip, subordinandone usi ulteriori alle condizioni specificamente previste per gli altri mezzi di ricerca della prova.

Opportuni appaiono anche gli atti d'indirizzo emanati da alcune Procure in queste settimane, volti a contenere i rischi dell'esternalizzazione delle operazioni

captative di cui la cronaca sta fornendo esempi significativi. In linea con le indicazioni fornite dal Garante appare, in particolare, la previsione, nella circolare della Procura di Milano, della possibilità di accettazione dei soli captatori di proprietà dei fornitori, di cui essi conoscano appieno il funzionamento, ricorrendo a server di transito stabiliti in Italia e con limitazione della visibilità dei software-spia ai soli utenti "bersaglio", per evitare che le captazioni possano interessare, come già accaduto in passato, soggetti del tutto estranei alle indagini.

5. La pandemia e le sue sfide

In un contesto così complesso come l'attuale, caratterizzato dalla convergenza tra potenza di calcolo ed emergenza, suscettibile di alterare il sistema delle garanzie democratiche, la disciplina della privacy, nell'applicazione quotidiana dell'Autorità, si è rivelata uno strumento prezioso.

Rispetto alla "rivoluzione" indotta, sotto vari profili, dalla pandemia, i numerosi interventi del Garante

sono stati nel complesso finalizzati a realizzare un bilanciamento equo tra sanità pubblica e privacy, cui la tecnica sia funzionale e non antagonista.

In ordine al contact tracing digitale, il Garante ha consolidato le proprie funzioni consultive e di controllo volte ad assicurare, in fase di progettazione tanto quanto di attuazione del sistema, la sua esclusività sulla base della previsione legislativa statale, sottolineando l'inammissibilità di forme di tracciamento realizzate a livello territoriale o, addirittura, aziendale o comunque privato; la funzionalizzazione del sistema di allerta a soli fini di sanità pubblica e l'effettiva volontarietà dell'adesione allo stesso.

In sede di audizione sul decreto-legge che ha prorogato la funzionalità del sistema di allerta nazionale e disposto l'interoperabilità delle piattaforme europee di tracciamento, il Garante ha sottolineato l'esigenza di verificarne l'uniformità in termini di garanzie (analizzate poi nella successiva valutazione d'impatto sottopostaci) e di limitare il flusso informativo ai soli dati necessari, comunque pseudonimizzati.

In ordine alle politiche vaccinali l'Autorità ha

fornito il suo contributo - non sempre, tuttavia, richiesto nella fase in cui sarebbe stato doveroso - per garantirne l'efficace attuazione nel rispetto della riservatezza, indicando le condizioni per la legittima circolazione dei dati tra i soggetti coinvolti.

Quanto alla disciplina dell'obbligo vaccinale per gli operatori sanitari, si è in particolare suggerita maggiore precisione nella definizione delle categorie soggettive interessate dalla misura: l'incerto ambito di applicazione ha generato diverse difficoltà in sede di attuazione.

Riguardo, invece, alle certificazioni verdi, si è richiesta in particolare la previsione di garanzie specifiche - carenti nella versione originaria del decreto-legge - per il trattamento di dati, contenuti nei pass, dai quali possono tra l'altro evincersi informazioni sullo stato di salute del soggetto.

L'incidenza del green pass su materie coperte da riserva di legge statale ha poi reso necessario evidenziare la dubbia legittimità di autonome iniziative regionali sul tema, come del resto di app gestite da società private volte ad accertare la negatività dei partecipanti

a determinati eventi, al di fuori delle ipotesi normativamente previste.

Per il contesto lavoristico, si è chiarito che spetta al medico competente trattare i dati sanitari dei lavoratori, verificandone l'idoneità alla "mansione specifica" anche, se del caso, sulla base della sottoposizione a vaccino, secondo le indicazioni fornite dalle autorità sanitarie.

Per altro verso, spetterà al datore di lavoro attuare le misure indicate dal medico competente nei casi di parziale o temporanea inidoneità alla mansione assegnata.

La traslazione on line, indotta o anche soltanto accelerata dalla pandemia, di molta parte delle attività quotidiane, ha poi rappresentato l'oggetto di una rilevante attività consultiva e d'indirizzo dell'Autorità, volta ad assicurare le garanzie necessarie alla riservatezza.

Particolarmente rilevante, in questo senso, è l'attività, consultiva e di controllo svolta rispetto alla didattica a distanza (su cui ci si è confrontati anche con le Camere, in audizione) al fine di orientarne lo svolgimento verso modalità il più possibile rispettose della privacy di studenti e docenti, rendendo così il

dramma della pandemia un'occasione per realizzare la "scuola-Telemaco", di cui discorre uno studioso.

Tra le varie indicazioni fornite rilevano, segnatamente, quelle relative al proctoring, ovvero all'uso di sistemi di rilevazione, prevalentemente biometrica, del comportamento degli studenti durante le prove on-line, al fine di garantirne la correttezza dello svolgimento.

Il Garante ha rilevato in particolare, anche in sede di audizione, l'esigenza di una previsione normativa che introduca misure adeguate per rendere i controlli non eccedenti le necessità effettive di verifica della corretta esecuzione delle prove, in modo da impedire un monitoraggio eccessivamente invasivo del comportamento dello studente.

Merita, peraltro, apprezzamento, l'introduzione - richiesta dal Garante, benché con un perimetro più ampio di quello previsto - del diritto alla disconnessione, da esercitare senza pregiudizi per il lavoratore, per impedire l'eccessiva osmosi tra tempo di vita e tempo di lavoro che rischia altrimenti, con lo smart working, di vanificare alcune tra le più basilari conquiste del diritto del lavoro.

Sono state, inoltre, fornite indicazioni importanti nell'ambito di un parere su un'istanza di riesame in materia di accesso civico generalizzato, volto a conoscere la distribuzione dei casi di Covid-19 registrati in un determinato ambito territoriale.

In quella sede si è avuto modo di ribadire come la pur condivisibile esigenza conoscitiva sottesa a queste istanze debba tenere conto delle possibilità di reidentificazione suscettibili di verificarsi, soprattutto in presenza di esiguità demografica, combinando le informazioni acquisibili. Il rischio, in questi casi, è quello di disvelare, sia pur indirettamente, dati sulla salute che sono invece doverosamente sottratti a questo pur prezioso strumento di controllo diffuso sull'operato delle amministrazioni.

6. Servitù volontarie e nuove vulnerabilità

Nell'affrontare le sfide poste, alla società tutta, dalla pandemia il Garante ha assunto, quale obiettivo prioritario, la tutela della persona rispetto alle nuove vulnerabilità ingenerate dall'attuale contesto, segnato per un

verso dalla prevalenza di esigenze pubblicistiche e, per altro verso, dall'accelerazione esponenziale del processo di transizione digitale.

Quest'obiettivo ha del resto caratterizzato, in questi primi mesi di mandato, l'azione dell'Autorità in ogni ambito e ne costituirà il principio ispiratore in futuro, perché la privacy contribuisca a correggere le asimmetrie determinate dal nuovo assetto di poteri ingenerato dal digitale.

Ciò è emerso univocamente sul terreno della tutela della persona on-line, rispetto ai rischi di coinvolgimento dei minori in situazioni per loro inadeguate e, quindi, pericolose o riguardo all'uso, a fini ritorsivi o altrimenti pregiudizievoli, dell'immagine altrui.

Con il provvedimento adottato d'urgenza nei confronti di Tik Tok il Garante ha inteso esigere il rispetto degli obblighi imposti dal Regolamento europeo a tutela del minore on line: prima fra tutte, la verifica dell'età dell'utente, che, al di sotto della soglia minima di età prevista, non può fruire dei social.

Allorché il Garante ha ritenuto, in un primo momento, insufficiente l'adempimento del provvedi-

mento, ha accolto l'impegno di TikTok all'assunzione di misure considerate dall'Autorità significative, pur riservandosene il costante monitoraggio, nelle more del più complessivo esame, anche in sede europea, delle ulteriori criticità contestate al social network.

Naturalmente, l'age verification è una condizione necessaria, ma non sufficiente per rendere il web un ambiente se non sicuro, almeno non inospitale per i minori.

Per raggiungere quest'obiettivo si deve promuovere una reale pedagogia digitale e rendere effettiva la responsabilità per i contenuti illeciti diffusi.

Del resto, ogni dato "abbandonato" in rete è un dato perso, affidato alle scelte, non sempre responsabili e leali, che altri faranno (si pensi al licenziamento, per un post, dell'operaio tarantino) e che, una volta immesso nel web, è quasi impossibile recuperare e "oscurare" ove lo si volesse.

I rischi non sono soltanto quelli della condivisione virale di frasi o immagini che poi, a distanza di tempo, potremmo voler cancellare e non vedere più associate alla nostra persona.

L'intelligenza artificiale consente anche - come abbiamo rappresentato al Senato - di innestare immagini di nudo su visi tratti da foto.

Più tracce di noi lasciamo in rete, più ci condanniamo a servitù (solo apparentemente volontarie), esponendoci all'azione di chi voglia colpirci, ad esempio, con il deep nude (tema su cui il Garante ha aperto un'istruttoria nei confronti di Telegram) o con altre forme di contenuti "fake".

Questi rischi sono, per i minori, amplificati dalla loro scarsa consapevolezza delle implicazioni di ogni loro "click", ma anche dall'effetto che ogni lesione dell'immagine o della dignità ha su una personalità più fragile, ancora in formazione.

La via della consapevolezza è necessaria per non privare i minori, almeno ultra14enni, di una socialità che oggi si esprime anche in questi modi, conferendo loro, tuttavia, anche gli strumenti indispensabili per orientarsi in un contesto che altrimenti è davvero troppo "più grande" di loro.

E' indispensabile seguire i ragazzi, in quest'esperienza, con discrezione ma anche con attenzione; educan-

doli al senso critico e all'autonomia di giudizio rispetto al comportamento da tenere.

Anche per effetto della telematizzazione della vita, indotta dalla pandemia, nel 2020 si è registrato un incremento di circa il 132%, rispetto al 2019 dei casi trattati dal Centro nazionale per il contrasto della pedopornografia e un aumento del 77% dei casi di vittimizzazione dei minori per grooming, cyber bullismo, furto d'identità digitale, sextorsion. Il 68% degli adolescenti risulta essere stato, nel 2020, testimone di casi di cyberbullismo (Terres des Hommes).

Sono dati allarmanti, che non possono non esigere un'assunzione di responsabilità collettiva rispetto a soggetti, quali i minori, le cui vulnerabilità possono renderli le vittime elettive delle distorsioni del web.

Analoga preoccupazione è espressa dal Comitato dei Ministri del Consiglio d'Europa nella dichiarazione del 28 aprile 2021.

Il Garante attribuisce, per questo, una rilevanza centrale alla tutela dei minori, in chiave sia preventiva - appunto quella accordata esigendo sistemi di age verification affidabili - sia remediale (in particolare

quella offerta in materia di cyberbullismo), rispetto al quale, anche grazie alla cooperazione con la Polizia postale, si stanno ottenendo risultati importanti.

Lo stesso paradigma di tutela remediale del Garante delineato per il cyberbullismo potrebbe, peraltro, estendersi in via più generale - come peraltro prevede qualche proposta di legge - all'hate speech e ad ogni altro contenuto discriminatorio diffuso on line.

La tutela preventiva rispetto alla violenza realizzata on line è stata, però, dal Garante accordata anche rispetto alle potenziali vittime di revenge porn, richiedendo ai gestori di bloccare il caricamento, da parte di terzi, di loro immagini sessualmente esplicite.

Si è in tal modo anticipata la soglia di tutela in situazioni in cui, altrimenti, ogni rimedio successivo rischia di essere, per quanto tempestivo, pur sempre tardivo.

Analoga esigenza di prevenzione ha, del resto, indotto il Garante a rimarcare, rispetto a un noto caso di cronaca, l'illiceità, potenzialmente anche penale, della diffusione, sia pur mediante chat, di immagini di vittime di abusi sessuali.

Anche nel 2020, del resto, l'Italia si è confermata come secondo Paese europeo per incidenza degli stalkerware, programmi informatici in grado di realizzare un vero e proprio spionaggio in danno, generalmente, del partner.

Si tratta di espressioni ulteriori di quella violenza informatica di genere per il cui contrasto è necessaria la sinergia di tutti gli attori istituzionali e della società civile, affinché la tecnica, da presupposto di emancipazione non divenga invece strumento di abuso e rafforzamento di rapporti di dominio sulla persona.

L'effettiva responsabilizzazione delle piattaforme in funzione di tutela della privacy degli utenti è stata, peraltro, l'oggetto di un'azione trasversale e attenta del Garante, che ha indotto anche alla prescrizione di rimedi effettivi a fronte di data breach che hanno interessato due importanti social network.

E' stata inoltre avviata un'istruttoria nei confronti di Clubhouse per accertare la complessiva legittimità del trattamento dalla stessa svolto, anche rispetto a dati biometrici (timbro e tonalità della voce) e a quelli dei minorenni.

Le varie direzioni in cui si è mossa l'azione del Garante sono state, nel complesso, volte a declinare il principio di accountability sempre più in chiave di tutela degli utenti, funzionalizzandolo alla garanzia della persona.

7. Libertà personale, tecnica e dignità

Le applicazioni dell'intelligenza artificiale - per le quali la Bozza di regolamento europeo propone un'articolata disciplina per promuoverne uno sviluppo "conforme ai valori dell'Unione" - sono sempre più rilevanti dal punto di vista quantitativo e qualitativo.

Ad esse e alla loro pretesa neutralità si affidano decisioni significative, assecondando quella che Eric Sadin definisce "svolta ingiuntiva della tecnica", sempre più demiurgica, predittiva e quindi performativa, che rischia di privarci della "vertigine della libertà" (Kierkegaard).

Ciò induce, spesso, a sottovalutare i rischi derivanti dall'inclusione, nel processo algoritmico, di inferenze viziate dalle stesse precomprensioni da cui le macchine ci avrebbero dovuto liberare.

Quando poi i bias discriminatori caratterizzano - come la cronaca in particolare statunitense ha dimostrato - algoritmi utilizzati, anche solo in parte, nell'esercizio della potestà punitiva, i rischi che ne conseguono diventano ancor più intollerabili.

Queste considerazioni, tra le altre, sono sottese agli stringenti limiti posti dallo schema di regolamento - oltre che dal Consiglio d'Europa - al ricorso al riconoscimento facciale in luoghi pubblici da parte delle autorità di contrasto, idoneo più di altri a degenerare in forme di sorveglianza di massa, di cui quelle cinesi - con i loro sistemi di rilevazione persino delle emozioni - sono espressione significativa.

Lo stesso d.lgs. 51 del 2018 - di cui si attende, da ormai troppo tempo, il regolamento attuativo - ha valorizzato, anche con specifiche norme incriminatrici, l'esigenza di prevenire implicazioni discriminatorie dell'intelligenza artificiale e di circondarne, comunque, l'uso in ambito di polizia con garanzie essenziali per la dignità e per la libertà della persona.

Sulla base di questi presupposti, il Garante ha ritenuto inammissibile l'attivazione, per fini di sicurezza

pubblica, di un sistema di riconoscimento facciale carente di previsione normativa adeguata e delle correlative garanzie rispetto alla sorveglianza indiscriminata suscettibile di conseguirne.

L'estensione, potenzialmente indeterminata, dell'ambito della rilevazione biometrica avrebbe infatti comportato un netto cambio di paradigma nell'attività di contrasto.

Esso avrebbe dunque necessitato quantomeno di un'univoca previsione normativa, in grado di ricondurre misure altrimenti massive nel solco del canone di proporzionalità, circoscrivendone l'ambito sulla base di specifiche esigenze di prevenzione.

Per altro verso, il Garante ha avviato un'istruttoria nei confronti di Clearview - società statunitense specializzata nel riconoscimento facciale a partire da dati acquisiti tramite web scraping - per accertare l'eventuale illiceità di un trattamento spesso prodromico a quello poi svolto dalle autorità di contrasto di molti Paesi, che sovente si avvalgono di tali servizi.

Ma la tecnica, il cui uso è stato esteso dalla pandemia, ha amplificato ulteriormente, in un ambito

già di per sé delicatissimo; quello dell'esecuzione penale, le vulnerabilità, per condizione e per contesto, che il Garante ha inteso proteggere.

A seguito di un'iniziativa congiunta con il Garante nazionale dei diritti delle persone private della libertà, direttori e operatori penitenziari sono stati invitati all'adozione di alcune essenziali garanzie per la tutela della riservatezza dei colloqui svolti via Skype dai detenuti, coniugando il rispetto del divieto di controllo auditivo con l'esigenza di verifica dell'identità degli interlocutori.

L'iniziativa si colloca all'interno di una più ampia e organica collaborazione intrapresa con il predetto Garante, per assicurare anche a soggetti in una particolare condizione di vulnerabilità quali i detenuti, i migranti ristretti nei CPR (Centri di permanenza per i rimpatri), gli ospiti delle REMS (Residenze per l'esecuzione delle misure di sicurezza), la componente essenziale della dignità che è il diritto alla privacy.

Diritto che fa parte, segnatamente, del "bagaglio" di diritti inviolabili che il detenuto porta con sé lungo tutto l'arco dell'esecuzione della pena (Corte cost., sent. 26/1999).

Ma la dignità della persona nell'ambito della giustizia penale e della sua comunicazione è assicurata, in particolare, dal rispetto della presunzione d'innocenza.

Esso sarà auspicabilmente rafforzato con il recepimento della direttiva (UE) 343/2016, volta a imporre agli Stati obblighi positivi di tutela del diritto degli indagati o degli imputati a non essere presentati in pubblico come colpevoli, anche mediante il ricorso a mezzi di coercizione fisica, prima dell'effettivo accertamento di responsabilità.

8. L'identità, tra cronaca e oblio

Rispetto alla dignità delle persone soggette a misure coercitive il Garante ha riscontrato, anche quest'anno, diverse violazioni da parte dei media, tanto più gravi in quanto riguardano la persona - qualunque reato abbia commesso - in un momento di tale vulnerabilità.

Mai come in relazione a questi aspetti il giornalismo deve assolvere al suo alto dovere di informazione nel rispetto del canone di essenzialità, senza cedere alla tentazione della spettacolarizzazione e del

sensazionalismo che rischia di far degenerare la pietra angolare delle democrazie (la libertà d'informazione, appunto), in gogna mediatica.

Lo ha ben ricordato il Presidente della Corte costituzionale, con riferimento alla più ampia esigenza di rispetto, nell'ambito della cronaca giudiziaria, della presunzione d'innocenza in favore degli indagati.

Analoga esigenza di essenzialità è stata espressa rispetto ad eccessi informativi riscontratisi nella cronaca e, in particolare, nella descrizione dei rapporti sentimentali intercorsi tra la vittima e la persona indagata per il suo omicidio, ultronea e pregiudizievole per il marito ma, soprattutto, per la figlia minorenne della donna.

Ai fini del legittimo esercizio della funzione informativa è, del resto, essenziale il rispetto dei principi di lealtà e correttezza, dei quali si sono riscontrate alcune violazioni nel ricorso, da parte del giornalista, ad artifici e raggiri per occultare indebitamente la finalità informativa della ripresa sotto l'apparenza di conversazioni confidenziali.

La rilevanza delle regole deontologiche è, del resto, tale che ogni loro violazione integra gli estremi

di un illecito amministrativo, la cui deterrenza auspichiamo possa anche contribuire a un più rigoroso rispetto di questi essenziali criteri regolativi, per un'informazione completa, ma rispettosa della dignità personale.

Rilevanti sono le decisioni assunte rispetto ai reclami sul diritto all'oblio (che rappresentano una quota significativa degli 8.984 riscontri complessivamente forniti a reclami o segnalazioni).

In quest'ambito si è precisato come la deindicizzazione della notizia possa rappresentare un utile strumento per coniugare la tutela dell'identità nel suo percorso dinamico e il diritto all'informazione, che verrebbe leso laddove notizie superate dall'evoluzione dei fatti venissero rimosse dagli archivi on-line dei giornali.

Ad essi, del resto, la Cassazione ha riconosciuto copertura costituzionale in quanto funzionali alla ricerca storica e, ad un tempo, espressione della più generale libertà di manifestazione del pensiero.

Si è poi consolidato l'indirizzo volto a riconoscere i presupposti della deindicizzazione di notizie inerenti il procedimento penale, allorché al soggetto siano state con-

cesse la non menzione della condanna o la riabilitazione, proprio al fine di consentirne il reinserimento sociale.

Quest'obiettivo sarebbe, infatti, irrimediabilmente vanificato dall'indiscriminata reperibilità, in rete, di quei dati giudiziari il cui oblio è necessario per consentire a ciascuno di essere anche altro da ciò che è stato.

Lo sguardo solo retrospettivo della rete, annientando la complessità di ogni percorso di vita, rischia altrimenti di risolversi in uno stigma perenne e deformante, tale da privare il condannato di quella "incomprimibile possibilità di recupero" in cui si esprime la dignità (come ha insegnato il Cardinale Martini).

9. Riforme, innovazione, cultura della privacy

Il 2020 si è caratterizzato, a livello globale, per il record negativo degli attacchi informatici, agevolati dall'incremento del ricorso ai canali telematici per effetto della pandemia e assurti, poche settimane fa, a veri e propri atti ostili nell'ambito del conflitto per il dominio cibernetico.

Alcune ricerche (Osservatorio Cybersecurity di

Exprivia) sottolineano come, nel primo trimestre 2021 in Italia si siano già verificati 349 reati informatici, in crescita del 47% rispetto al 2020, compresivi di furto dei dati nel 70% dei casi.

Nel corso dell'anno, sono stati notificati al Garante oltre 1387 data breach, alcuni dei quali particolarmente rilevanti per la tipologia di dati, anche di carattere sanitario, esfiltrati o per il numero di soggetti interessati.

Il DIS (Dipartimento informazioni per la sicurezza) ha registrato nel 2020, in Italia, un generale incremento delle aggressioni (+20%), rivolte nell'83 % dei casi a soggetti pubblici.

Ciò conferma la già rilevata vulnerabilità di sistemi informatici, quali in particolare quelli della pubblica amministrazione, progettati al di fuori di un piano organico d'innovazione comprensivo tra l'altro di adeguate garanzie privacy, come dimostra l'incidenza delle violazioni riscontrate dal Garante nel settore pubblico, anche rispetto a obblighi centrali quali quelli di corretta designazione del responsabile della protezione dati.

Il che dimostra come la protezione dei dati sia un fattore abilitante primario, un presupposto ineludibile anche per la cybersecurity, in quanto tutela ciò che, come il dato, rappresenta l'elemento costitutivo essenziale dell'"infosfera".

Tale consapevolezza è alla base della collaborazione con il Dis (da estendere alla neo-istituita Agenzia per la cybersicurezza nazionale, come prevede lo stesso decreto-legge) ulteriormente sviluppata quest'anno nel solco di un'innovazione più volte addotta, in ambito europeo, a modello da seguire.

E tuttavia, la stessa consapevolezza dovrebbe permeare la visione complessiva delle riforme da promuovere, per un'innovazione sostenibile anche in termini di garanzie, nella direzione "inclusiva" tracciata anche dal Digital Compass.

Solo una reale sinergia tra la cybersecurity e la protezione dei dati può, infatti, garantire che il processo di digitalizzazione avvenga senza pregiudizio per la sicurezza nazionale (oggi assicurata ulteriormente, per i profili cyber, dal Perimetro), ma anche per la riservatezza e la dignità individuale.

Le carenze (soprattutto in termini di sicurezza e minimizzazione) inizialmente riscontrate ma poi, grazie all'interlocuzione con il Garante, in larga parte colmate, rispetto all'App io, dimostrano quanto il rispetto della disciplina privacy sia determinante per la complessiva sostenibilità del processo di digitalizzazione.

Da questo punto di vista, le riforme indicate dal PNRR (Piano nazionale di ripresa e resilienza) - tra le quali l'innovazione digitale occupa, comprensibilmente, una posizione centrale - devono essere realizzate considerando anche, tra i parametri essenziali, la protezione dei dati, quale fattore di vantaggio competitivo per il sistema-Paese e, assieme, presupposto di legittimazione dell'azione pubblica.

Inscrivere nel processo riformatore adeguate garanzie per la privacy vuol dire, infatti, infondere nei cittadini fiducia nell'operato delle pubbliche amministrazioni e, ad un tempo, favorire un'innovazione "sicura" e, per ciò, competitiva perché scevra da rischi, oltre che non regressiva in termini di diritti e di libertà.

Nella progettazione delle riforme e nel loro concreto attuarsi sarà, dunque, indispensabile il

dialogo istituzionale e la consultazione del Garante, che lungi dal rappresentare un ostacolo, ha dimostrato di essere il fattore determinante di ogni innovazione riuscita.

Non si confondano le prerogative di un'Autorità indipendente prevista, a tutela di un diritto fondamentale, direttamente dai Trattati europei, con mero formalismo o, peggio, con un presunto freno all'azione di riforma cui invece il Garante ha sempre fornito un contributo costruttivo, per essere assieme più efficaci, ma non meno liberi.

Il tassello ulteriore è, poi, la promozione di una cultura della protezione dei dati, che - anche grazie allo strumento dei codici di condotta, la cui adozione nei vari settori si sta perfezionando - dovrebbe divenire oggetto di un vero e proprio processo d'introiezione, affinché la compliance assurga a forma e regola dell'azione di soggetti privati e pubblici.

In questa direzione il Garante ha valorizzato notevolmente la propria attività di comunicazione ed esteso i canali di accessibilità: l'Autorità è divenuta, soprattutto in questi primi tre anni di applicazione

del nuovo quadro giuridico europeo, sempre più un'istituzione "di prossimità", oltre che di garanzia.

La protezione dei dati, rappresentando un fattore reputazionale sempre più determinante, costituisce del resto un volano per lo sviluppo e la competitività di aziende che sappiano mostrarsi compliant e anche per questo va promossa.

Rilevanti, per quantità e qualità, sono invece ancor oggi le violazioni riscontrate in ambito privato, laddove le sanzioni più elevate (di 16.800.000 e 12.250.000 euro rispetto a due operatori telefonici) sono state irrogate, anche quest'anno, principalmente per telemarketing selvaggio, che si conferma essere fenomeno endemico, radicato nella dinamica dei rapporti commerciali.

E questo anche grazie a un'articolata rete di attori economici, quasi un "sottobosco" di sub-fornitori, operanti spesso in condizioni di più complessiva illegittimità, anche sotto il profilo lavoristico, come noi stessi abbiamo potuto verificare in almeno un caso.

Uno strumento importante di tutela sarà rappresentato dall'estensione del Registro delle

opposizioni alle utenze mobili, così da contrastare buona parte di questo fenomeno, idoneo a determinare turbamenti anche significativi nella vita privata soprattutto dei soggetti più fragili, come gli anziani, in danno dei quali può risolversi addirittura, nei casi peggiori, in vere e proprie truffe.

10. La tutela delle persone vulnerabili

Se i termini sono gli analizzatori dei tempi, quasi signa temporum, la vulnerabilità s'iscrive a pieno titolo nel loro nòvero.

La vulnerabilità designa persone, fenomeni e situazioni per i quali si evoca il concetto di ferita, di lesione, sia dal punto di vista fisico che da quello psicologico.

E tuttavia, il problema non si può risolvere nell'identificazione del gruppo o della categoria che assorbe tutti gli interessi che fanno capo a coloro che vi appartengono, ma piuttosto bisogna rivalutare la specificità della persona e dei suoi interessi, spirituali e materiali.

Si tratta, in sostanza, di guardare all'homme situé, alla persona in situazione, alla persona concreta

ed alle esigenze che in concreto prospetta.

E' il passaggio dal soggetto - astratto, espresso in una categoria - alla persona.

E proprio la tutela delle persone vulnerabili - nelle forme più tradizionali e in quelle, più recenti, indotte dalla tecnica - ha rappresentato il tratto caratterizzante l'attività del Garante in questo primo anno e auspichiamo possa contraddistinguere l'intero nostro mandato, nella direzione di una civiltà digitale inclusiva.

La protezione dei dati può rappresentare, infatti, un prezioso strumento di difesa della persona da vecchie e nuove discriminazioni e di riequilibrio dei rapporti sociali, nella direzione dell'eguaglianza e della pari dignità sociale indicate dalla nostra Costituzione.

In questo senso, la protezione dei dati si sta dimostrando anche e sempre più determinante per un governo sostenibile della tecnica; perché la democrazia non degeneri, in altri termini, in algocrazia.

Ringrazio tutte le Autorità che hanno voluto offrirci sostegno, nonché la Guardia di Finanza per la consolidata cooperazione.

Ciò che abbiamo realizzato deve moltissimo al contributo quotidiano di tutto il personale del Garante, che anche per questo ringrazio sentitamente.

Alla Vicepresidente Ginevra Cerrina Feroni, ai Colleghi Guido Scorza e Agostino Ghiglia, al Segretario generale e ai miei validi collaboratori - con tutti i quali abbiamo condiviso un anno di attività tanto complessa quanto importante - rivolgo infine un ringraziamento speciale, con l'auspicio di continuare ad essere l'istituzione centrale per la democrazia che aveva immaginato Stefano Rodotà.

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

stampa:
Tiburtini Srl


GPDP
GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI