Senato della Repubblica

1^ Commissione

AS 1900 e abbinati

Audizione del Presidente del Garante per la protezione dei dati personali

PASQUALE STANZIONE

Roma, 12 gennaio 2021

Ringrazio, anzitutto, la Commissione per quest'occasione di confronto e per la sensibilità dimostrata rispetto ai profili privacy del fenomeno della disinformazione, sul quale il Garante torna a pronunciarsi in seconda lettura. Anticipo che mi concentrerò sui profili non toccati dal mio predecessore nell'audizione di marzo scorso alla Camera (di cui peraltro condivido appieno il contenuto), al fine di fornire alla Commissione un quadro ancora più completo.

Sotto un profilo di metodo, preciso che non mi soffermerò sulla scelta del ricorso a un'inchiesta parlamentare istituendo, appunto, una Commissione con i poteri di cui all'art. 82 Cost., né sul carattere bicamerale o meno, la durata, la composizione, che sono tutti temi evidentemente esulanti dalla competenza del Garante e oggetto di una valutazione squisitamente politico-istituzionale.

Il contributo che il Garante può offrire sul punto, attiene specificamente all'ambito oggettivo dell'inchiesta parlamentare e, dunque, all'analisi del fenomeno che spetterà, poi, all'istituenda Commissione sceverare in ogni suo aspetto.

In entrambe le proposte di legge l'oggetto dell'inchiesta parlamentare sembra ben definito, salvo forse volerlo estendere a un aspetto di più recente emersione e su cui il Garante sta

conducendo un'istruttoria ad hoc: **il *deep nude***. Si tratta dell'uso di tecniche di intelligenza artificiale (fondate appunto sul *deep learning*) per realizzare immagini di nudo a partire da volti o comunque figure di persone determinate (persino minorenni), anche reperiti in rete. Tali immagini vengono spesso utilizzate a fini ritorsivi, quale strumento di abuso e coartazione dell'altrui volere, nel quadro di condotte tuttavia non del tutto riconducibili al delitto di *revenge porn* (art. 612-ter c.p.) soprattutto per il presupposto richiesto della previa realizzazione o sottrazione di immagini destinate a rimanere private. Tale requisito sembra escludere l'applicabilità della norma a materiale artefatto, tanto più che ove l'ordinamento ha inteso far riferimento a simili innesti di immagini lo ha generalmente espressamente previsto (si pensi alla pedopornografia virtuale, ex art. 600-quater.1 c.p.)

Questi limiti della norma penale suggeriscono, pertanto, l'opportunità di un intervento normativo ad hoc, eventualmente anche riespandendo (come prima della riforma di cui al d.lgs. 101/2018) **l'ambito applicativo del delitto di trattamento illecito** di dati personali (art. 167 del Codice), che offrirebbe una tutela ad ampio spettro rispetto a molteplici forme di lesione dell'identità personale realizzate abusando dei relativi dati. In tal senso, tra i requisiti di illiceità speciale suscettibili di integrare il delitto andrebbe reintrodotto quello relativo alla omessa acquisizione del consenso (espunto, salvo per i casi di *telemarketing*, dalla riforma del 2018), così coprendo molteplici ipotesi (le più frequenti) di violazioni della persona perpetrate in rete.

Si potrebbe inoltre cogliere l'occasione per estendere ai delitti di trattamento illecito l'applicabilità dell'**aggravante** – ora circoscritta ai soli delitti contro la libertà sessuale – di cui all'art. 609 - duodecies c.p., del **ricorso a mezzi tesi ad impedire l'identificazione dei dati di accesso alle reti telematiche**, al fine di contrastare l'uso ritorsivo e criminoso che spesso viene fatto dell'anonimato.

Un riferimento al deep nude, quale oggetto dell'inchiesta parlamentare, potrebbe farsi anche con un emendamento aggiuntivo all'art.2, c.1. lettera g) del ddl n. 1900, nella parte in cui allude agli effetti dello sviluppo dell'i.a. sull'attività di disinformazione.

Ma al di là dello specifico profilo del *deep nude*, cui potrebbe essere estesa l'inchiesta parlamentare, entrambe le proposte, comunque, ben la indirizzano verso l'analisi di una pluralità di temi tra i quali l'attività di disinformazione in ambito sanitario (su cui è intervenuta in modo specifico la Commissione con la comunicazione del 10 giugno 2020, "*Tackling COVID-19 disinformation – Getting the facts right*".), la correlazione tra disinformazione e illeciti consumeristici o antitrust, *l'hate speech* e la manipolazione dell'opinione pubblica, le procedure adottate dai gestori per la gestione delle istanze di rimozione e dei reclami, nonché le forme possibili di co- e *self-regulation*, promosse del resto da tempo dalla Commissione Ue.

Entrambi i disegni di legge ben colgono, dunque, il profilo sistemico e, viceversa, le implicazioni personali; **il rischio sociale e il pregiudizio individuale** connesso alla disinformazione quale degenerazione patologica dell'eccesso informativo, distorsione della "parresia" della rete. Pur nella varietà degli ambiti che tocca, il tema delle *fake news* (certo non nato con la rete, ma da essa mutato così profondamente da assumere forme radicalmente nuove) sottende due questioni essenziali che l'istituenda Commissione potrà, in particolare, se vuole, approfondire: **la responsabilizzazione delle piattaforme e la tutela individuale.**

L'esigenza della responsabilizzazione dei "poteri privati" delle piattaforme è emersa, con maggiore nettezza, dopo *Cambridge Analytica*, sul terreno delicatissimo della **manipolazione dell'opinione politico-elettorale (**tema su cui peraltro Agcom e Garante hanno iniziato un proficuo confronto). Le ultime elezioni presidenziali americane, con i sistemi di *fact checking* adottati

anche da *blog* e *social network* per contrastare le *fake news* hanno dimostrato ulteriormente la centralità delle piattaforme nella formazione dell'opinione politica di cittadini sempre più adusi a informarsi sui canali telematici. Ma anche questo tipo di strategie non risolve, molto probabilmente, il nodo di fondo del "*nudging*" venuto alla luce con *Cambridge Analytica*, ovvero dell'influenza del *microtargeting*; delle notizie e finanche della propaganda elettorale selettivamente proposte all'utente, in base al suo profilo di elettore stilato dall'algoritmo con il pedinamento digitale della sua attività in rete. E' il fenomeno che Sunstein ha definito del "***Daily me***", ovvero della presentazione del reale modellata, da parte dell'algoritmo, secondo la categoria (di consumatore, utente, elettore) cui esso ritenga di ascrivere il soggetto, con effetti inevitabilmente distorsivi sul pluralismo informativo e sulla stessa autodeterminazione individuale.

Non sono rari, poi, i messaggi politici fondati sulle "**verità alternative**": argomentazioni in cui l'oggettività dei fatti è assai meno influente nel formare la pubblica opinione rispetto all'emotività e alle convinzioni personali. Questa riduzione della verità a narrazione più o meno efficace, ha effetti tutt'altro che trascurabili rispetto all'informazione politica, favorendo la diffusione di false rappresentazioni sulle quali, poi, si fondino opinioni politiche e, persino, scelte elettorali. L'invio di contenuti specificamente ritagliati sul modo di essere, pensare, agire, desumibili dal comportamento on line dell'utente rilevato dall'algoritmo, può infatti avere una valenza manipolativa del suo pensiero non paragonabile a nessun monopolio dell'informazione perché, appunto, capace di adattarsi così perfettamente al pensiero del "bersaglio" da anticiparne il giudizio e limitarne fortemente l'autodeterminazione.

Il contrasto di tali fenomeni distorsivi passa, in primo luogo, dalla prevenzione dell'illecito sfruttamento dei dati degli utenti che ne è alla base e per il quale, ad esempio, il Garante, ha sanzionato

Facebook nel caso *Cambridge Analytica*. La rilevanza di tale metodo di contrasto è tale che la disciplina europea (Reg.Ue, Euratom, n. 1141/2014, come modificato dal regolamento 2019/493) sanziona oggi, espressamente, **l'uso illecito di dati personali per condizionare i risultati elettorali**, spesso - come pare accaduto per l'elezione di Donald Trump - persino da parte di potenze straniere.

Ma, al di là dei profili più strettamente "privacy", innovazioni di sistema potrebbero derivare dal **Digital Services Act**, il progetto di regolamento da poco presentato dalla Commissione che recepisce alcune delle più rilevanti misure introdotte – anche in ordine alle procedure di rimozione dei contenuti illeciti – dalla legge tedesca sui social network, dalla *loi Avia* di giugno scorso come emendata dal *Conseil Constitutionnel*, nonché da discipline unionali di settore. Il DSA introduce alcuni obblighi, soprattutto di carattere proattivo, in capo alle piattaforme on line, diversamente modulati sulla base del numero di utenti attivi, nel segno di una loro responsabilizzazione di tipo preventivo. Ribadendo - e, anzi, rafforzando con una nuova *Good Samaritan Clause* – l'esenzione di responsabilità secondaria dei gestori rispetto agli illeciti commessi dagli utenti sulle proprie piattaforme e il doveroso divieto di monitoraggio generale e preventivo sui contenuti. Il DSA compensa tuttavia questo *safe harbor* con degli obblighi di regolamentazione tali da minimizzare il rischio di violazioni o da contenerne, comunque, gli effetti pregiudizievoli. A tal fine s'impone l'istituzione (diversamente modulata in ragione, appunto, della rilevanza della piattaforma) di procedure interne di decisione delle istanze di rimozione di contenuti illeciti o comunque contrari alle policies aziendali, con obblighi di motivazione e reclamabilità delle scelte adottate, nonché con la devoluzione delle controversie ad organi di AdR dotati di requisiti adeguati di indipendenza.

In tal senso, si "positivizza" il percorso compiuto dalla giurisprudenza nel segno di una maggiore responsabilizzazione del

gestore (si pensi alla figura pretoria dell'hosting attivo), volta a impedire che la rete, con la forza della condivisione virale e l'ubiquitarietà dei suoi servizi, divenga la cassa di risonanza di violazioni le più diverse dei diritti individuali. Del resto, la rinuncia all'introduzione di una forma, sia pur limitata, di responsabilizzazione del gestore rischia di riflettere uno slittamento dell'idea di **libertà su quella di anomia,** ignorando che l'assenza di regolazione, in un contesto privo di ogni limite all'espansione del potere privato, non produce eguaglianza ma subalternità agli imperativi del mercato.

Il crinale stretto su cui si muove il Digital Services Act è il mantenimento dell'opzione di fondo sottesa alla direttiva 2000/31, ovvero il regime generale di responsabilità (solo) condizionata del gestore– con il correlativo divieto di monitoraggio generale dei contenuti- coniugato, tuttavia, con una serie di obblighi procedurali e sostanziali espressivi tanto del principio di *accountability* quanto del canone di *responsibility*.

La proposta della Commissione interviene in un momento di accentuata esigenza di ascrizione alle grandi piattaforme di responsabilità almeno pari alla rilevanza del potere (non solo economico) dalle stesse esercitato. Si pensi, in tal senso, alla responsabilità (oggettiva) di Amazon per l'intermediazione svolta rispetto alla vendita di un prodotto difettoso, affermata nel **caso Bolger** dalla sentenza del 13 agosto 2020 del Quarto Distretto della Corte d'appello della California, fondata sull'affidamento riposto dagli utenti nella qualità dei prodotti ospitati dalla piattaforma. Benché non scevra da criticità, questa sentenza riflette indubbiamente l'esigenza (avvertita persino nell'ordinamento dove questo regime di responsabilità, solo condizionata, dei gestori è nato), di circondare il potere delle piattaforme di un sistema adeguato di limiti e responsabilità.

In tale contesto, è significativa la scelta della Commissione di non cedere al modello della responsabilità oggettiva della piattaforma per i servizi intermediati o i contenuti diffusi dagli utenti, pur non rinunciando a una revisione della disciplina in senso maggiormente rigorista (si pensi al principio del *know your business customer*, che impone alle piattaforme di valutare adeguatamente l'affidabilità dei professionisti cui concedono spazi). La cifra di questa novella legislativa risiede, dunque, nel passaggio dalla (sola) responsabilità alla responsabilizzazione, che potrebbe avere effetti determinanti – come si è notato anche nei lavori prodromici alla redazione del *draft* di DSA - anche sul terreno della disinformazione, con particolare riguardo **agli obblighi di trasparenza sull' *online advertisement* e sui suggerimenti commerciali**. La disinformazione e i conseguenti effetti manipolativi sono, del resto, specifici pericoli sistemici di cui il DSA impone la valutazione, nell'ambito di un'analisi del rischio connesso all'attività svolta, al fine di modulare conseguentemente le garanzie da adottare, ivi inclusi i codici di condotta cui attenersi.

L'obbligo di motivazione delle decisioni adottate e la loro reclamabilità dovrebbero contribuire, poi, a rendere più trasparente l'esercizio, da parte delle piattaforme, del potere di rimozione, che se non adeguatamente circoscritto e reso appunto 'visibile' e sindacabile, rischia di renderle **arbitre dei diritti in rete.** Anche il tema della responsabilizzazione delle piattaforme può essere, indubbiamente, oggetto di analisi da parte della Commissione, soprattutto al fine di fornire contributi da parte del Parlamento nazionale in fase ascendente.

Degli **effetti individuali** della distorsione informativa in rete - comprensivi anche, nel loro amplissimo spettro, dell'*hate speech*, come chiariscono gli stessi disegni di legge – si è detto già l'essenziale, con riguardo soprattutto all'estensione dell'ambito oggettivo di applicazione del delitto di trattamento illecito di dati personali. Basti, ora, rilevare l'opportunità di approfondire il tema della **tutela remediale dell'utente leso da contenuti illeciti on**

line. Come dimostrano i casi dell'oblio e del cyberbullismo, il meccanismo fondato sulla richiesta al gestore di rimozione e la successiva istanza al Garante in caso di inerzia o rigetto, è **un utile strumento di tutela dei diritti della personalità on line**. Esso, infatti, coniuga l'esigenza della pronta rimozione dei contenuti (soprattutto in caso di adesione spontanea del provider) **con la riserva all'autorità pubblica della decisione in ultima istanza**, nel contraddittorio delle parti.

Si tratta di un complessivo bilanciamento che risponde alle esigenze sottolineate dalla Corte di giustizia e dalla Corte europea dei diritti dell'uomo, quest'ultima in particolare con alcune sentenze che hanno sancito addirittura, in capo agli Stati, un **obbligo positivo di assicurare misure idonee a tutelare la dignità personale** (cfr., in particolare, Delfi c. Estonia del 2015). Si potrebbe dunque riflettere sull'estensione di tale disciplina a casi quali *l'hate speech* (come prevedeva la pdl Moretti AC 2049 della scorsa legislatura), la diffusione di false notizie lesive dell'identità individuale (come prevedeva il ddl Zanda AS 3001 della stessa legislatura) e lo stesso *deep nude*. In tal modo si consentirebbe al Garante di fornire una tutela effettiva alle vittime di questi illeciti, anche agendo direttamente sulle piattaforme (a rigore non qualificabili come titolari del trattamento realizzato dagli utenti sui loro profili).

Apprezzo, infine, il rilievo assegnato dai ddl al ruolo che **l'educazione (al) digitale** assume nella prevenzione dei fenomeni variamente distorsivi della rete, tra i quali anche la disinformazione. E' un aspetto dirimente soprattutto per la formazione delle future generazioni, che per quanto native digitali necessitano ancora di una capillare sensibilizzazione verso i rischi cui la rete ci espone e da cui la rete stessa deve essere liberata, perché torni ad essere quello spazio di libertà e democrazia di cui abbiamo sempre più bisogno.