CONSIGLIO NAZIONALE FORENSE

Conferenza internazionale" **Sicurezza e linguaggio dell'odio. Tutela della persona e protezione dei dati personali: i diritti nell'era dei social media**" 14.09.17

Considero molto importante la scelta di orientare il dibattito, per il primo G7 dell'Avvocatura, sul tema della protezione dati, quale presupposto – così leggiamo il sottotitolo- dell'effettiva tutela della persona.

Ed è significativo discuterne a vent'anni dall'introduzione nel nostro ordinamento di questo nuovo diritto, che ha dimostrato, nel corso del tempo, le sue molte potenzialità: la capacità, soprattutto, di tutelare i più vulnerabili da sempre nuove discriminazioni, di garantire la libera costruzione della personalità, la sovranità su di sé, sulla propria immagine e sul proprio corpo.

E di fronte alla tentazione della delega alla tecnologia persino delle più grandi e complesse questioni, proprio questo diritto può consentirci di non smarrire il senso del limite, riportando la persona al centro di uno sviluppo altrimenti tirannico e disumanizzante, per misurare l'innovazione anche secondo i criteri della sostenibilità sociale e dell'ammissibilità etica, oltre che giuridica.

Del resto, proprio a fronte dell'aumento delle diseguaglianze sociali e alla difficoltà del diritto di stare al passo con l'innovazione, la protezione dati si è rivelata spesso indispensabile per garantire un corretto equilibrio tra mercato e individuo, informazione e dignità, tecnica e vita, determinismo e libertà.

Mai come rispetto alla protezione dati, infatti, il contenuto del diritto è così strettamente legato al contesto in cui esso si esercita e, quindi, all'evoluzione tecnologica che vi incide.

Così, ad esempio, i diritti alla deindicizzazione e alla portabilità costituiscono due aspetti della protezione dati inimmaginabili, almeno nei termini attuali, anche solo pochi anni fa, perché nati appunto nell'era "digitale".

Del resto, le nuove tecnologie hanno mutato non solo forma e sostanza dei diritti, ma la stessa articolazione geopolitica dei poteri e il rapporto tra pubblico e privato.

Le grandi imprese del web hanno acquisito poteri la cui rilevanza non si esaurisce sul piano economico o commerciale ma assume sempre di più una caratura sociale, che finisce per concorrere con il diritto pubblico per antonomasia.

Significativa in tal senso l'iniziativa di Google, volta a suggerire a chi appaia a rischio di radicalizzazione (per aver digitato parole espressive di una tendenza filo-jihadista), contenuti di segno opposto, volti a dissuadere da propositi violenti.

Si individuano dunque, attraverso la profilazione, soggetti a rischio e se ne promuove la de-radicalizzazione con una contro-narrazione.

Difficile immaginare un'attribuzione, a soggetti privati, di funzioni più tipicamente espressive dell'autorità pubblica quali quelle, appunto, propriamente preventive e, poi, "rieducative".

Tutto ciò in un contesto in cui i gestori dei siti internet sono chiamati a promuovere un'importante opera di prevenzione della propaganda filo-jihadista rimuovendo – come prevede la direttiva antiterrorismo 541/2017- i contenuti filo-terroristi, fermo restando il diritto di ricorrere giudizialmente avverso le decisioni di rimozione. Garanzia, questa, che nel nostro ordinamento- ove tale misura era già stata introdotta nel 2015 – è stata rafforzata affidando la richiesta di oscuramento non all'iniziativa del singolo ma all'ordine dell'autorità giudiziaria.

Ma altrettanto rilevante è la funzione di composizione di diritti fondamentali quali, in particolare, la libertà di espressione e la dignità, assegnata in prima istanza ai big tech sul terreno dell'hate speech, a seguito dell'accordo con la Commissione Ue con cui i gestori si sono impegnati a rimuovere i "contenuti d'odio".

E non meno importante è la funzione assunta proprio da Google nel rapporto tra informazione e oblio attraverso le procedure di de-listing.

I gestori di piattaforme sono del resto chiamati, dalla recente legge sul cyberbullismo, a un'importante quanto complessa risposta alle istanze per la rimozione di contenuti asseritamente illeciti, ove in gioco sono da un lato la libertà di espressione e dall'altro la dignità personale.

Ovviamente, in nessuno di questi casi viene compresso il ruolo dell'autorità pubblica.

Avverso le decisioni dei gestori è, e deve essere, sempre proponibile -per far valere i propri diritti- istanza all'autorità pubblica, sia essa giudiziaria o Autorità di protezione dati, come nel caso del cyberbullismo e dell'oblio.

La responsabilizzazione dei grandi protagonisti del web è certamente un processo positivo, perché concorre a minimizzare il rischio di un uso violento della rete: ma dobbiamo ribadire con assoluta chiarezza che spetta allo Stato e alle istituzioni democraticamente legittimate, impedire che essa, da spazio di promozione dei diritti di tutti, divenga terreno su cui si può impunemente violare la dignità, soprattutto dei soggetti più fragili.

In questo senso è davvero significativo l'accostamento, già dal titolo stesso di questo incontro, della sicurezza alla libertà di espressione (di cui ovviamente il linguaggio d'odio è la negazione, più che il limite esterno).

Non solo perché proprio su questi campi stanno emergendo i profili più nuovi del diritto contemporaneo, ma anche perché si tratta di due settori cruciali per lo Stato di diritto.

Da un lato, infatti, la libertà di espressione (sancita, non a caso, dal primo emendamento della Costituzione americana) rappresenta la pietra angolare delle democrazie, in particolare nel suo rapporto con la dignità soprattutto se considerata in ordinamenti, quali il nostro e quello tedesco, nati dopo l'esperienza dei totalitarismi che tali due diritti insieme hanno violato.

E' significativo che il dibattito più fecondo su reati di opinione, dignità e manifestazione del pensiero sia nato proprio in Germania, ove l'illiceità del negazionismo, ad esempio, è stata fondata sin dal 1994 proprio sulla dignità di ciascun ebreo, violata appunto da espressioni volte a negare l'avvenuta realizzazione della Shoah.

E proprio la costituzione tedesca, all'indomani dell'esperienza nazista, si apre con l'enunciazione del diritto alla dignità di ciascuno. E nega tutela a chi l'altrui dignità violi, con l'istigazione all'odio, al razzismo, alla discriminazione.

Sulla sicurezza, per altro verso, soprattutto in tempi di terrorismo "immanente", si misura la qualità delle democrazie. La costanza, l'efferatezza, l'ubiquitarietà delle azioni jihadiste, che finiscono con il "globalizzare le vittime" rappresentano, infatti,

una minaccia ininterrotta, da affrontare con strategie preventive nuove perché adeguate a un fenomeno assolutamente non comparabile con quello, già noto, dell'eversione e del terrorismo interno .

Cardine di queste strategie non può che essere un uso accorto della tecnologia, che non può certo divenire un fattore competitivo di vantaggio per i criminali rispetto agli inquirenti, solo per la difficoltà del diritto di stare al passo con la rapidità dell'evoluzione tecnologica.

E, infatti, nella dimensione digitale il rapporto tra libertà e sicurezza, privacy e prevenzione, assume forme nuove e costringe a ripensare categorie giuridiche consolidate.

Si pensi, ad esempio, al tentativo di coniugare la possibilità di identificazione degli autori di reati on-line (anche nel "web" che non sia deep né dark) con l'esigenza – ribadita anche dalla direttiva antiterrorismo- di non attribuire ai provider un ruolo di sorveglianza preventiva delle informazioni scambiate in rete.

Un altro fronte su cui recentemente è emersa con forza l'asimmetria tra diritto e tecnologia è quello delle intercettazioni mediante captatori, che evidenzia come la particolare tecnologia utilizzata, in assenza di una specifica regolamentazione, rischi di trasformare un mezzo investigativo "circoscrivibile" e controllabile in uno strumento di sorveglianza talmente pervasivo da risultare "ubiquitario".

Sono esempi, questi, di come la tecnologia digitale in tutte le sue declinazioni sia una preziosa risorsa, cui attingere soprattutto a fini investigativi, purché entro i limiti che ne garantiscano la sostenibilità democratica.

Ed è proprio questo il nodo da sciogliere, soprattutto in un contesto, quale appunto quello odierno, di terrorismo "immanente", in cui il rischio più grande è quello di normalizzare l'emergenza e, con essa, la compressione dei diritti e delle libertà che ne consegue.

Non penso che la strada giusta sia quella francese, della codificazione dell'emergenza in Costituzione o comunque di leggi ispirate allo stato di eccezione che, come insegnano i casi americano e, ancora una volta francese, non sono riuscite a impedire stragi e violenza.

E non dobbiamo vivere nel perenne incubo dell'uomo di vetro ma piuttosto considerare- con saggezza- il grado di libertà cui si può rinunciare, senza divenire schiavi del terrore e senza neppure soccombere.

Dovrebbe essere evidente che, in questo tempo difficile, il problema non è più tanto l'acquisizione dei dati quanto la capacità di metterli in relazione, analizzarli (come del resto sembrerebbero dimostrare molti recenti attentati, gli autori dei quali erano tutt'altro che ignoti ai servizi di intelligence).

Questo vale a maggior ragione in un ordinamento, quale quello europeo, in cui il diritto alla sicurezza – coniato significativamente come tale- è sancito, nella stessa disposizione, accanto al diritto alla libertà (art. 6 della Carta di Nizza), per realizzare appunto quello "spazio di libertà, sicurezza e giustizia" cui alludono i Trattati .

L'accostamento tra sicurezza e libertà è, in questo senso, tutt'altro che casuale.

Esso, infatti, configura ciascuno dei due diritti come limite interno dell'altro, bene giuridico inviolabile, nel suo nucleo essenziale, neppure per la salvaguardia del suo reciproco.

Tale binomio esclude dunque l'ammissibilità di politiche europee o nazionali che sacrifichino le libertà oltre quanto strettamente indispensabile per la salvaguardia della sicurezza di ciascun cittadino. Su questo equilibrio la Corte di giustizia ha costruito l'architrave del rapporto tra strumenti investigativi e, in particolare, protezione dati, quale diritto di libertà maggiormente inciso dai primi nell'epoca della costante connessione.

La giurisprudenza sulla data retention, con le sentenze Digital Rights e Tele2 è in questo senso significativa.

Con l'ultima pronuncia, in particolare, la Corte ha dichiarato incompatibile con il diritto europeo ogni previsione nazionale che non limiti la data retention ad esigenze di contrasto di gravi delitti, nei confronti di soggetti coinvolti, in qualche misura, in attività criminose, notificando la misura all'interessato non appena le esigenze investigative lo consentano.

La lettura forte del principio di proporzionalità ha dunque, in questo caso, determinato un profondo mutamento della stessa natura della data retention, da misura preventiva e come tale applicabile a chiunque, in mezzo di ricerca della prova "individualizzante".

Si tratta, dunque, di una invalidazione delle varie forme di acquisizioni di dati personali " a strascico", nei confronti di chiunque e a prescindere da indizi di reità, che, sebbene non estesa al campo della sicurezza nazionale (sottratto alla competenza dell'Unione) non può su questo non spiegare alcun effetto.

Principalmente perché neppure nei settori rimessi alla competenza nazionale può ammettersi una totale negazione dei principi di diritto fondativi dell'ordinamento europeo, tale da violare quel nucleo incomprimibile dei diritti fondamentali, intangibile secondo l'art. 52 della Carta di Nizza.

Meno sensibile a questi principi si è tuttavia dimostrato il legislatore, tanto europeo quanto nazionale.

Il primo, infatti, omettendo di sostituire la disciplina invalidata dalla Corte nel 2014 con una conforme alle sue statuizioni, ha di fatto rimesso tale onere al livello nazionale. E se è vero che il legislatore interno non dispone certo di piena discrezionalità in materia, dovendo conformarsi alle indicazioni della Corte, è altrettanto vero che in molti Stati stanno prevalendo spinte securitarie poco inclini al rispetto del principio di proporzionalità tra sicurezza e privacy.

La recente proposta di una norma che, in Italia, ammette la conservazione dei dati di traffico telefonico, telematico e delle chiamate senza risposta indifferentemente per sei anni, pur limitandone l'acquisizione giudiziale solo ai procedimenti per reati distrettuali, è in questo senso significativa.

Tale norma pare difficilmente compatibile con quel principio di proporzionalità tra esigenze investigative e protezione dati sancito dalla Corte di giustizia e declinato, tra l'altro, come esigenza di differenziazione della conservazione in ragione del tipo di dato, del contesto investigativo e della gravità dei reati da accertare.

E non possono non esprimersi riserve sulla reale utilità di una conservazione, protratta così a lungo nel tempo, di una quantità di dati così elevata e sicuramente assai vulnerabile, viste anche le carenze che spesso caratterizzano i sistemi di sicurezza dei gestori.

La strada da seguire è invece ancora una volta quella tracciata da Corte di giustizia e Cedu: le tecniche d'indagine vanno certamente adeguate alla portata della minaccia attuale, ma vanno utilizzate nella maniera tanto più utile in termini di prevenzione, quanto più sostenibile sotto il profilo democratico.

Bisogna dunque essere più efficaci, non meno liberi.

Ed essere più efficaci, allora, vuol dire soprattutto coordinare l'azione investigativa (ciò che pare sia mancato nel caso della Rambla di Barcellona) e adeguare il diritto a quella tecnologia in continua evoluzione, che è una delle risorse strategiche dei terroristi.

Ma senza illudersi di poter delegare a un algoritmo le strategie di indagine, che devono basarsi su di una raccolta selettiva, non "a strascico" - acritica perché generalizzata - dei dati personali e sull'ineliminabile "fattore umano", capace esso solo di dare senso e forma a masse di dati, altrimenti prive di alcun significato.

Qui sta la sfida, mettere al centro la persona, alfa e omega , punto di riferimento ineludibile per governare questo nostro tempo difficile: per il quale nessuno di noi possiede ricette facili.