AUDIZIONE DEL PRESIDENTE DEL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI
ANTONELLO SORO

AUDIZIONI INFORMALI NELL'AMBITO DELL'ESAME DEL DISEGNO DI LEGGE N. 2553 (ATTIVAZIONE DEL SERVIZIO SAFETY CHECK) E DEL DISEGNO DI LEGGE N. 2575 (DELEGA PER TRACCIABILITÀ AUTORI DI CONTENUTI NELLE RETI SOCIALI)

8^ COMMISSIONE DEL SENATO DELLA REPUBBLICA
11 APRILE 2017

I disegni di legge toccano due aspetti per certi versi speculari che è quanto mai utile trattare insieme: l'utilizzo della tecnologia a tutela dei diritti e della sicurezza il primo; l'esigenza di impedire che l'innovazione tecnologica venga utilizzata per violare, impunemente, l'altrui libertà, il secondo.

Il primo disegno di legge (AS 2553) introduce, per le reti di telecomunicazioni, lo specifico obbligo di mettere a disposizione un canale *safety check*, con cui lanciare l'allerta ai cellulari agganciati alle celle in una data area, in presenza di situazioni di rischio.

In passato il Garante ha ammesso tale possibilità, anche in assenza del consenso dell'interessato, in diverse occasioni, a partire da un provvedimento generale del 2003, in cui si è ammesso l'invio di sms di pubblica utilità in caso di disastri, calamità naturali o altre emergenze di ordine pubblico (inondazioni, terremoti, epidemie ecc.), previa deliberazione in tal senso della competente autorità amministrativa.

Si segnalava comunque la necessità di una norma legislativa che, fondando il potere di adozione di provvedimenti contingibili e urgenti, prevedesse anche la possibilità di derogare alla disciplina privacy.

Nel 2008 si è poi ammessa la possibilità di rintracciare persone disperse attraverso l'acquisizione dei dati di localizzazione dei cellulari, purché ovviamente i dati fossero trattati per i soli fini di ricerca e soccorso.

Nel 2013, poi, si è autorizzata l'Unità di crisi del Ministero degli affari esteri a far inviare, tramite sms, informazioni utili in situazioni di emergenza ai clienti italiani all'estero, (indicazione del numero unico dell'Ambasciata del Paese in cui si trovano, eventuali aree da evitare o punti di raccolta, comportamenti a rischio ecc.).

La modifica normativa proposta ripercorre, dunque, un sentiero in certa misura già tracciato, fornendo tra l'altro, in via generale, quella base legislativa che il Garante ha nei vari provvedimenti richiesto per legittimare la deroga al requisito del consenso.

In questo senso, condividendosi la ratio del disegno di legge, ci limitiamo solo a segnalare alcune possibili integrazioni, volte essenzialmente ad arricchirne il contenuto con riferimento ai profili privacy.

Come dimostra, infatti, la sede su cui si innesta la novella (codice delle comunicazioni elettroniche), il ddl è pensato essenzialmente per disciplinare il *safety check* quale servizio di pubblica utilità, prestazione obbligatoria da parte degli operatori delle telecomunicazioni.

A tali disposizioni è opportuno affiancare una previsione, anche di carattere generale (es., all'art. 2, c.1, cpv. ee-bis), secondo cui la funzione di *safety check* dev'essere svolta nel rispetto della disciplina di protezione dati, dunque osservando garanzie e principi generali quali quelli di finalità, proporzionalità, non eccedenza e minimizzazione, così da escludere, ad esempio, l'utilizzazione dei dati in questione per finalità diverse.

Ovviamente, il rispetto di tali principi deriva dal rango superiore della loro fonte (oggi il regolamento generale protezione dati), ma un'espressa previsione in tal senso conferirebbe indubbiamente maggiore organicità al testo.

Divenendo, poi, tale trattamento necessario da parte degli operatori per adempiere a un obbligo di legge, verrebbe meno il requisito del consenso dell'interessato, tanto nel sistema del Codice quanto in quello delineato dal nuovo regolamento.

Al fine di delineare con maggiore dettaglio le cautele da adottare per coniugare il diritto alla protezione dei dati personali con le esigenze di tutela della sicurezza e dell'incolumità pubbliche, è opportuno che il decreto cui l'art. 10 demanda la definizione di alcuni importanti profili attuativi sia emanato su parere anche del Garante.

Si consideri del resto che il Regolamento, che si applicherà a partire dal maggio 2018, prevede il parere delle autorità di protezione dati su tutti gli atti (anche) legislativi che incidano sulla materia: dunque l'attenzione a tali profili deve progressivamente entrare a far parte della nostra cultura anche istituzionale e il nostro parere, del procedimento normativo.

Conseguentemente, è opportuno ricomprendere, all'interno della disciplina dettata dal decreto attuativo, anche adeguate garanzie per la protezione dei dati personali e la definizione delle modalità del trattamento, che deve ovviamente limitarsi alle sole operazioni strettamente necessarie alla funzionalità del servizio, con l'esclusione dell'utilizzo dei dati stessi per altre finalità.

Il ddl AS 2575 delega invece il Governo all'adozione di norme idonee a garantire l'identificabilità degli autori di contenuti sui social network.

Sicuramente essi rappresentano il luogo della dimensione immateriale in cui si realizzano, con frequenza crescente, delitti in particolare contro l'onore e la dignità.

Quello dell'identificabilità degli autori di condotte illecite è, tuttavia, un problema generale del web, in particolare del deep o dark web, che costituisce il primo spazio di azione delle organizzazioni criminali.

Non a caso, nel nostro ordinamento, il ricorso a mezzi tesi ad impedire l'identificazione dei dati di accesso alle reti telematiche costituisce un'aggravante, la cui sfera di applicazione non è limitata ai social network o ad altre, determinate, zone del web.

Il tema dell'identificabilità dell'autore di condotte illecite potrebbe, dunque, essere affrontato in termini anche più generali sotto il profilo oggettivo, superando quella limitazione ai social network, che potrebbe anche risultare poco compatibile con il principio di ragionevolezza.

Per converso, l'indeterminatezza delle finalità perseguite dal sistema di identificazione proposto rischia di configgere con i principi di proporzionalità e minimizzazione del trattamento dei dati personali.

Un qualsiasi scopo non può, infatti, legittimare, una raccolta di dati così invasiva quale quella che è presumibile verrebbe disposta per garantire l'identificabilità degli autori, ma solo l'esigenza di tutelare interessi giuridici di rilevanza primaria può legittimare tale raccolta.

Si consideri che la Corte di giustizia ha invalidato la direttiva sulla data retention e alcune norme nazionali perché incompatibili con il principio di proporzionalità tra protezione dati ed esigenze investigative, in particolare limitando la possibilità di acquisizione dei dati di traffico alle esigenze di accertamento di reati di una certa gravità.

È dunque opportuno limitare le possibilità di identificazione a quelle strettamente necessarie alle finalità di accertamento dei reati, dei quali peraltro sarebbe opportuno selezionare le tipologie in base alla gravità, come richiesto dalla Corte di giustizia Ue.

È quindi auspicabile, anzitutto, sopprimere l'"anche" all'art.1, commi 1 e 2, lettera a), suscettibile di estendere eccessivamente e irragionevolmente le possibilità di identificazione anche a scopi che non lo legittimerebbero secondo il diritto europeo.

Quanto alla delega, essa sembra muoversi all'interno di margini alquanto ristretti, per ragioni di ordine tanto giuridico quanto tecnologico.

In primo luogo, infatti, come dimostra lo stesso criterio direttivo al comma 2, lett.b), le maggiori garanzie di identificabilità dovrebbero derivare da una revisione della normativa sulla conservazione dei dati di traffico, che tuttavia è in gran parte sottratta alla discrezionalità del legislatore nazionale.

Infatti, per un verso la disciplina della *data retention* per fini commerciali è contenuta nel regolamento e-privacy attualmente in discussione, che regola tipologia di dati (e metadati) suscettibili di conservazione, modalità e condizioni.

Per altro verso, la conservazione dei dati di traffico per finalità investigative è legittima unicamente nel rispetto della direttiva 680/2016 e dei principi sanciti dalla Corte di giustizia con le sentenze Digital Rights del 2014 e Tele2 dello scorso dicembre: proporzionalità tra privacy ed esigenze investigative; limitazione delle categorie di dati, dei tempi di conservazione e dei soggetti interessati dalla misura a quanto strettamente necessario per esigenze di contrasto di gravi reati.

Con la sentenza Tele2, peraltro, la *data retention* è stata ritenuta illegittima proprio in quanto massiva, dovendo invece essere applicata, secondo la Corte, in modo da rivolgersi ad ambiti oggettivi, soggettivi (persino territoriali) caratterizzati da specifici fattori di rischio.

Da generalizzata e "a strascico" quale è sempre stata concepita, la conservazione dei dati di traffico dovrà dunque divenire mirata, selettiva.

Anche la parificazione della durata della conservazione dei dati di traffico telefonico e telematico (portando anche quest'ultima a 24 mesi), se non giustificata da specifiche esigenze investigative, potrebbe risultare incompatibile con l'interpretazione forte del principio di proporzionalità sancita dalla Corte.

Lo sviluppo del criterio di delega sub b) dovrebbe dunque muoversi in un ambito alquanto ristretto, salvo ovviamente prevedere il ricorso a eventuali *tecnologie* che, pur alle condizioni indicate, consentano una più efficace identificazione degli autori di reato.

E qui emergono alcune criticità di ordine tecnologico con cui dobbiamo necessariamente confrontarci, considerando che la principale modalità indiretta di identificazione on-line si avvale

dell'indirizzo IP, qualificato dalla Corte di giustizia come dato personale anche nella sua componente "dinamica" (sentenza Breyer dell'ottobre 2016).

La mera registrazione a siti quali, in particolare, i social network, mediante indicazione di un indirizzo e-mail non è, infatti, di per sé idonea a garantire la reale identificazione dell'utente.

Al di là del ricorso deliberato a tecniche di elusione, dunque, gli ostacoli maggiori all'identificazione degli autori di illeciti on-line si presentano oggi, essenzialmente, in due ipotesi.

La prima attiene all'illegittimo sfruttamento di una connessione altrui, ottenuta mediante intrusione in una rete di terzi (ad es., mediante un accesso wi-fi non adeguatamente protetto) ovvero l'utilizzo, anche legittimo, di un accesso wi-fi "libero", ovvero disponibile a ciascuno in assenza di autenticazione informatica o altra forma di protezione della connessione aerea (wireless).

Dal momento che, come dispone il decreto legge 69/2013, l'offerta di accesso ad internet mediante wi-fi non richiede l'identificazione dell'utilizzatore, in questi casi si può solo risalire al soggetto amministrativamente responsabile della rete mediante la cui connessione sia stata realizzata la condotta illecita, ma non all'autore materiale di quest'ultima.

La seconda difficoltà deriva dall'esaurimento degli indirizzi IP nel sistema IPv4, che comporta l'impossibilità di assegnazione di un indirizzo IP univoco a ciascun utente, con la conseguente difficoltà nell'identificazione degli autori di condotte illecite on-line.

In assenza del passaggio massivo al sistema IPv6, che consentirebbe di ovviare a tale criticità, la soluzione adottata da diversi fornitori consiste nell'assegnazione, con tecniche di Network Address Translation (nat), di indirizzi IP "a grappolo", ovvero attribuendo un unico indirizzo a una pluralità di utenti.

Ciò fa ovviamente venir meno il requisito dell'univocità dell'indirizzo IP prescritto dalla normativa vigente, anche a fini di certezza nell'identificazione degli autori delle condotte on-line.

Né, del resto, sembra praticabile la soluzione paventata da alcuni, consistente nell'associazione IPv4 pubblico e indirizzo IP di destinazione, che come è stato chiarito sin dal 2008, non è un dato suscettibile di conservazione per fini di giustizia da parte dei fornitori di servizi di comunicazione elettronica accessibili al pubblico.

Benché apparentemente "esterno" alla comunicazione, tale dato coincide di fatto, in molti casi, con il "contenuto" cui l'utente ha avuto accesso consentendo, tra l'altro, di ricostruire direttamente o indirettamente relazioni personali o sociali, convinzioni religiose, orientamenti politici, abitudini sessuali e stato di salute.

Peraltro, l'associazione indirizzo IPv4/IP di destinazione rischia comunque di non consentire neppure l'identificazione univoca dell'utente nel caso di siti molto frequentati (social network in primo luogo), con il rischio di ingenerare un falso affidamento sull'efficacia a fini investigativi di tale tecnica.

E proprio la scarsa idoneità dell'indirizzo IP di destinazione a garantire, pur in associazione con l'indirizzo IPv4, la corretta identificazione dell'utente, renderebbe la conservazione di tali dati difficilmente compatibile con il requisito della stretta proporzionalità tra privacy ed esigenze investigative richiesto dalla Corte di giustizia.

Il passaggio al sistema IPv6 parrebbe dunque, in questo senso, una soluzione tecnica auspicabile per garantire l'effettiva univocità dell'assegnazione degli indirizzi IP, che rappresenta oggi il principale strumento di identificazione indiretta degli utenti in rete.

Per altro verso, dal momento che la maggior parte dei social network e degli internet service provider è situata oltre i confini della nostra giurisdizione, ai fini dell'acquisizione dei dati necessari all'identificazione degli autori di condotte illecite in rete è sempre più spesso indispensabile la cooperazione giudiziaria internazionale.

In questo senso è significativo l'impegno assunto dalla Commissione Ue, per agevolare e armonizzare gli strumenti per l'acquisizione in sede giudiziaria di elementi probatori anche digitali, in ragione dell'insufficienza delle attuali procedure di assistenza giudiziaria e degli accordi internazionali di settore.

La realtà digitale, per sua natura defisicizzata, è infatti strutturalmente refrattaria ai confini delle giurisdizioni e la tutela dei diritti on-line non può che presupporre:

- la cooperazione delle autorità di contrasto nella ricostruzione di condotte inevitabilmente trasfrontaliere,

- il superamento del rigido criterio territoriale ai fini del riconoscimento delle garanzie degli utenti della rete,

- la complessiva armonizzazione dei sistemi giuridici dei vari Paesi.

Il diritto alla protezione dei dati personali è, in un certo senso, emblematico di questo processo di "universalizzazione".

I limiti della competenza normativa su base territoriale sono stati, infatti, in certa misura superati dal regolamento generale che, consolidando le acquisizioni giurisprudenziali (a partire dai casi Weltimmo e Costeja), ha esteso l'applicabilità della disciplina europea anche ai soggetti stabiliti al di fuori dell'Unione, qualora essi offrano beni o servizi agli individui ivi residenti o ne controllino il comportamento (*target principle*).

L'armonizzazione dei vari sistemi di tutela è stata definitivamente realizzata, a livello europeo, con lo stesso regolamento, che nasce proprio dall'esigenza di superare le asimmetrie rese possibili dal recepimento non del tutto uniforme della direttiva 95/46.

L'accordo Privacy shield sul trasferimento negli Usa dei dati dei cittadini europei, faticosamente concluso nel 2016, ha creato le premesse per un processo di più larga convergenza nel riconoscimento del diritto fondamentale alla protezione dei dati.

Tuttavia le prime scelte adottate in materia dalla nuova Amministrazione degli Stati Uniti, in contrasto con quella precedente- nel segno di una vera e propria monetizzazione della privacy on-line da parte degli internet service provider, potrebbero allargare lo iato tra Europa e Stati Uniti.

Un accenno al problema prima solo richiamato, del ricorso deliberato a tecniche di elusione in grado di vanificare anche l'univoca assegnazione di indirizzi IP.

L'uso di tecniche di cifratura delle connessioni, di reti private virtuali e di altri strumenti di anonimizzazione degli accessi, come quelli realizzabili con la rete TOR, è alla portata dell'utente un po' più esperto e ovviamente della criminalità organizzata.

Nello stesso tempo, questi strumenti di anonimato sono stati promossi anche da Paesi occidentali quale mezzo di protezione del dissenso in regimi dittatoriali o comunque non rispettosi dei diritti umani.

Gli stessi strumenti vitali per l'esercizio della libertà di espressione in determinati Paesi sono, quindi, suscettibili di un duplice uso, per fini leciti e non, con una contraddizione a oggi irrisolta tra la tendenza a rendere più sicura la rete rafforzandone le caratteristiche di accountability e l'esigenza di consentire la libertà di espressione on-line anche in spazi ostili.