Dati Sensibili Riservatezza e Oblio

capitolo scritto da: Federica Resta

Il punto della situazione

Nel 2017 ricorrono i vent'anni da quella che Stefano Rodotà definì la "rivoluzione silenziosa", ovvero l'entrata in vigore della prima normativa a tutela della privacy, con la contestuale istituzione della relativa Autorità Garante.

La circostanza è doppiamente significativa, perché il 2017 (e i suoi primi sei mesi, che in questo contributo analizziamo) coincide anche con il momento di più intensa preparazione in vista dell'applicazione del nuovo quadro giuridico europeo, a partire dal 25 maggio 2018. La fascia temporale che consideriamo in questo Rapporto è dunque anche l'occasione per descrivere l'evoluzione che ha interessato questo diritto, autonomizzatosi dal tradizionale right to be let alone- nella sua dimensione negativa di diritto all'intangibilità della propria sfera privata, - per arricchirsi di aspetti nuovi e inattesi. Grazie alla sua evoluzione, il diritto alla protezione dei dati personali si è dimostrato un insostituibile e concretissimo presidio di libertà, rispetto a forme di controllo tanto sottili quanto pervasive. Ciò che in origine si era portati a rappresentare, un po' semplicisticamente, come mera immunità da indebite ingerenze, si sarebbe rivelato, nel corso del tempo, un diritto dalle straordinarie e molteplici potenzialità. Capace di difendere i più vulnerabili da sempre nuove discriminazioni e stigmatizzazioni sociali, di garantire la libera costruzione della personalità, l'integrale rappresentazione dell'identità individuale, il corretto stabilirsi delle relazioni sociali, la sovranità su di sé, sulla propria immagine e sul proprio corpo, garanzia di equità sociale e redistribuzione del potere. E questo soprattutto nel momento in cui il conflitto tra mercato e diritti si gioca su di un terreno reso assai più complesso dalla crescente sostituzione dell'uomo con la macchina. Le videocamere si moltiplicano in ogni angolo nelle nostre città, per quella tentazione cui è sempre più difficile sfuggire, di delegare la sicurezza pubblica all'occhio elettronico e alla deterrenza che dovrebbe indurre il timore di essere costantemente sorvegliati. Come nel caso dei "totem" alla stazione centrale di Milano, si ricorre ai dati biometrici persino per analizzare l'effetto prodotto sul cittadino (ridotto a consumatore) da un determinato annuncio pubblicitario. La dematerializzazione del lavoro ne sta determinando quasi una de-umanizzazione, con la delega di attività e funzioni sempre più numerose a computer e robot. Lo smart-phone è usato sempre meno per telefonare e sempre più per racchiudere i frammenti più preziosi della nostra esistenza, tanto da divenire – come affermato dalla Corte suprema Usa – una "protesi" di ciascuno di noi.

I rilevanti mutamenti di contesto hanno contribuito quindi – come ha sottolineato il presidente del Garante, Antonello Soro- ad ampliare e arricchire il contenuto del diritto alla protezione dati, il cui nuovo statuto è ora sancito dal regolamento Ue n. 2016/679, che assieme alla direttiva 2016/680, relativa ai trattamenti di dati personali nel settore di giustizia e polizia, costituirà il nuovo quadro giuridico europeo in materia, essendo applicabile a partire dal prossimo maggio. Nel periodo che consideriamo, in cui intenso è – non solo a livello istituzionale – il lavoro di preparazione per l'applicabilità del nuovo quadro giuridico europeo, le decisioni del Garante e alcune scelte legislative

innovative hanno contribuito ad affermare principi importanti in materia, dall'oblio alle intercettazioni, dal cyberbullismo alla tutela dei minori nel contesto dei social network.

Giustizia, informazione, dignità

Il 14 giugno è stato approvato dalla Camera dei deputati, in via definitiva, con voto di fiducia, il ddl di riforma del processo penale che contiene anche una delega legislativa per la riforma della disciplina delle intercettazioni. I principali criteri direttivi della delega concernono la previsione di norme per la garanzia della riservatezza delle parti e, soprattutto, dei terzi, fondate anche sulla modifica della disciplina delle modalità di utilizzazione dei risultati delle intercettazione in sede cautelare e mediante una precisa scansione procedimentale per la selezione del materiale intercettativo nel rispetto del contraddittorio tra le parti e delle esigenze di indagine. Positiva, in particolare, è la previsione del dovere del pubblico ministero di garantire un'adeguata selezione degli atti da inviare al gip a sostegno della richiesta di misura cautelare, non ricomprendendovi le intercettazioni inutilizzabili, irrilevanti o comunque inerenti terzi estranei alle indagini e contenenti dati sensibili (purché non emergano elementi favorevoli all'indagato). Analogamente a quanto disponeva sul punto il ddl "Mastella", si prevede che tali dati siano conservati in apposito archivio riservato con facoltà di ascolto ed esame ma non di copia, da parte dei difensori e del giudice, e che siano sottoposti alla procedura di stralcio, nel contraddittorio delle parti. Importante è anche l'indicazione di non trascrivere nei brogliacci (salvo specifica autorizzazione del pubblico ministero) le stesse categorie di intercettazioni, così minimizzando il rischio di esfiltrazione di dati di terzi, sensibili o comunque non rilevanti ai fini investigativi.

Particolarmente innovativo è, poi, il criterio direttivo volto a disciplinare il ricorso ai captatori informatici a (esclusivi) fini intercettativi, su cui si era registrato un contrasto interpretativo, composto poi dalle Sezioni Unite della Cassazione nell'aprile 2016. La strutturale diversità di realizzazione di questo tipo di captazione rispetto a quelle tradizionali ha, infatti, evidenziato tutti i limiti dell'applicazione a tali fattispecie della disciplina pensata per le seconde. Queste ultime, infatti, sono concepite (in ossequio all'art. 15 della Costituzione) come limitate nel tempo, nello spazio, previste come residuali nel caso di ambientali domiciliari. Da remoto, invece, il controllo dell'indagato è talmente pervasivo da non avere più alcun limite (pertanto è stato definito "ubiquitario") né, del resto, possibilità di riscontro effettivo qualora si utilizzino determinati software capaci di alterare il contenuto del dispositivo in cui sono installati e di cancellare le tracce delle operazioni compiute.

Ancora, sulla scorta dell'emendamento Centaro al ddl "Alfano", si introduce una nuova fattispecie delittuosa consistente nella diffusione del contenuto di conversazioni o riprese audiovisive fraudolentemente captate e svolte in presenza dell'agente, al solo fine di recare danno alla reputazione o all'immagine altrui. Si impone la previsione di specifiche scriminanti per l'utilizzazione di tali captazioni nell'ambito di un procedimento amministrativo o giudiziario, per esercizio del diritto di difesa o del diritto di cronaca. La condotta qui tipizzata copre effettivamente una lacuna, dal momento che ad oggi, come confermato più volte anche dalla Cassazione, la registrazione abusiva di conversazioni da parte dell'interlocutore o comunque di chi vi abbia preso parte non integra alcuno specifico reato.

La privacy nell’era della sorveglianza costante

A due giorni dalla strage di Berlino, il 21 dicembre 2016, una coraggiosa sentenza della Corte di giustizia è intervenuta a chiarire ancora una volta e con più forza i termini del rapporto tra privacy e sicurezza. Il tema specifico è quello della conservazione dei dati di traffico (telefonico, telematico) e di localizzazione, per finalità di accertamento e repressione dei reati. Se con la sentenza Digital Rights di aprile 2014 la Corte aveva dichiarato invalida la stessa direttiva “Frattini” (2006/24/Ce) per violazione del principio di proporzionalità nel bilanciamento tra diritto alla protezione dei dati personali ed esigenze di pubblica sicurezza, con la pronuncia di oggi si traggono le conseguenze di quel principio rispetto alla legislazione interna.

I ricorsi decisi interessano, nello specifico, la disciplina svedese e quella britannica in materia di data retention, ma il principio affermato dalla Corte, con valenza generale, dichiara incompatibile con la stessa direttiva (lette alla luce della Carta di Nizza) ogni previsione interna che, per fini di contrasto dei reati: a) imponga la conservazione, generale e indiscriminata, di tutti i dati di traffico e relativi all’ubicazione degli utenti dei mezzi; b) legittimi l’accesso delle autorità nazionali competenti ai dati conservati per finalità ulteriori rispetto a quelle di contrasto dei “serious crimes”, in assenza di un previo vaglio giurisdizionale o comunque di un’autorità amministrativa indipendente e di garanzie relative alla conservazione dei dati nella Ue.

La Corte ribadisce l’invasività della misura, precisando che si tratta di dati che, pur non attingendo al contenuto della conversazione, forniscono comunque indicazioni importanti sulle comunicazioni intrattenute da ciascuno, sui loro destinatari e sulla loro frequenza, “profilando” la persona. L’accesso a tali dati, da parte dell’autorità pubblica, comporta dunque- ribadisce la Corte – una forte ingerenza nella vita privata dei cittadini, ingenerando peraltro in loro l’idea di essere esposti a una “costante sorveglianza” in quanto la conservazione e il successivo utilizzo dei dati stessi avviene a insaputa dell’interessato. Pertanto, osserva la Corte, solo la lotta ai “gravi reati” e' idonea a giustificare tale 'ingerenza nella vita privata dei cittadini. La deroga al principio di riservatezza delle comunicazioni (anche nei loro dati esteriori) non può dunque, affermano i giudici, divenire la regola.

Le discipline interne sulla data retention devono pertanto prevedere- oltre a misure di sicurezza idonee a minimizzare il rischio di abusi- l’accessibilità dei dati conservati solo da parte dell’autorità giudiziaria o da un’autorità amministrativa indipendente, in base a circostanze e procedure disciplinate dalla legge per esigenze di accertamento di gravi reati, notificando la misura all’interessato (come già affermato dalla Cedu nella sentenza Zakharov), non appena le esigenze investigative lo consentano.

Sotto questo profilo, andrebbe valutata l’opportunità di modificare la nostra disciplina, in particolare limitando le ipotesi di acquisizione dei dati conservati ai soli procedimenti per gravi reati (probabilmente i c.d. delitti distrettuali quali mafia, crimine organizzato, terrorismo, che nella normativa previgente consentivano una conservazione per un tempo maggiore), anche differenziando condizioni, limiti e termini di conservazione dei dati in ragione della particolare gravità del reato, del tipo di dato e della sua utilità investigativa . Andrebbe poi valutata l’opportunità di una maggiore giurisdizionalizzazione della procedura di acquisizione, prevedendo che essa sia disposta con decreto non già del pm ma del gip (come disponeva la precedente disciplina), da notificare all’indagato salvo esigenze di segretezza per particolari ragioni investigative.

Ma l’aspetto maggiormente innovativo della pronuncia concerne l’esigenza di rendere selettiva e mirata la stessa conservazione, limitandola in ragione del tipo di dato, del mezzo di comunicazione considerato, della durata della ritenzione, delle persone coinvolte (che devono avere un collegamento almeno indiretto con la commissione di gravi reati), finanche di criteri geografici che limitino la conservazione ad aree caratterizzate da rischi specifici (ad alta densità criminale, dunque!). Si tratta di criteri che finiscono con il mutare profondamente la natura stessa della data retention come misura preventiva e come tale applicabile a chiunque (a prescindere dal coinvolgimento in fatti di reato) e dovunque, in vista di un’acquisizione, soltanto eventuale, in sede giudiziaria.

Sotto questo aspetto dovrebbero essere modificate non soltanto la nostra disciplina ma anche quella di quasi i tutti gli Stati membri e finanche norme dell’Unione, anche recenti, che prevedono analoghe acquisizioni di dati personali “ a strascico”, generali e indifferenziate, nei confronti di chiunque e a prescindere da qualsiasi indizio di reità, in vista di una soltanto eventuale acquisizione a fini probatori. Si pensi alla recentissima direttiva sul PNR (passenger name record), che prevede la conservazione, analogamente massiva, dei dati relativi alla prenotazione di voli da parte di chiunque, in vista di possibili utilizzazioni in sede investigativa.

Ma i principi sanciti dalla Corte possono spiegare alcuni, sia pur limitati effetti anche sulle discipline interne relative alla data retention per esigenze di sicurezza nazionale. Se, infatti, è vero che questa materia è sottratta alla disciplina dell’Unione, è altrettanto vero che l’esimente della sicurezza nazionale non può essere invocata dagli Stati membri in assenza di adeguati presupposti e che un suo uso strumentale potrebbe radicare comunque la competenza dell’Unione.

Cyberbullismo

Il 17 maggio la Camera dei deputati ha approvato, in via definitiva, il disegno di legge sul cyberbullismo (ora l. 71/2017), che contiene alcune norme particolarmente innovative per la garanzia della dignità del minore, essendosi accantonate invece le disposizioni ispirate a una logica prettamente sanzionatoria nei confronti dell’autore di simili condotte.

Particolarmente rilevante è la peculiare tutela riparativa accordata alle vittime del cyberbullismo, volta anzitutto a rimuovere tempestivamente dal web i contenuti lesivi della dignità del minore, al fine di contenere i danni arrecatigli e prevenirne ulteriori.

Si è quindi prevista una specifica procedura, accelerata, dinanzi al Garante per la protezione dei dati personali, che consenta ai genitori di un minore (o allo stesso ultraquattordicenne) vittima di un atto di cyberbullismo, quando pure non siano integrati gli estremi di uno specifico reato, di ottenere una tutela rafforzata e celere da parte dell’Autorità. Qualora, infatti, il gestore del sito internet o comunque il titolare non abbia spontaneamente provveduto entro 72 ore o non sia identificabile, gli interessati potranno adire l’Autorità. Essa, entro 48 ore, potrà adottare provvedimenti inibitori e/o prescrittivi che garantiscano la dignità del minore rispetto a qualsiasi forma di violazione della sua persona, commessa in rete.

Importante anche la scelta sul sistema di prevenzione da delineare. Si prevede, in primo luogo, un

piano di azione integrato per la prevenzione e il contrasto del cyberbullismo, affiancato da un codice di autoregolamentazione per gli operatori della rete, volto in particolare a definire, attraverso un comitato di monitoraggio, procedure standard per la rimozione dei contenuti lesivi.

Inoltre, al fine di promuovere l'adozione di tecnologie *child-friendly*- capaci cioè di prevenire il fenomeno già in virtù della stessa configurazione dei dispositivi e dei sistemi di comunicazione –si prevede il conferimento di un marchio di qualità ai fornitori di servizi di comunicazione e ai produttori aderenti ai modelli e alle indicazioni fornite dal Tavolo tecnico incaricato di redigere il piano di azione integrato.

Determinante è poi l' "educazione digitale" dei minori, che si intende favorire quale elemento trasversale alle varie discipline curriculari, al fine di responsabilizzare gli stessi minori e di promuoverne la consapevolezza in ordine ai rischi – oltre che alle opportunità- correlati all'uso della rete.

Importante, in termini preventivi, è anche l'investimento sulla formazione del personale scolastico, ivi inclusa la nomina (prevista dalle varie proposte) del referente per il cyberbullismo, tenuto in particolare a coordinare le attività di contrasto e tutela nell'ambito della singola istituzione scolastica

Rilevante anche l'istituto dell'ammonimento, da parte del questore, del minore ultraquattordicenne che, mutuato dalla disciplina sullo stalking, potrebbe efficacemente contribuire, in questo caso, anche attraverso il coinvolgimento dei genitori, a responsabilizzare il minore autore di reato. Attivare, in queste forme "miti", l'attenzione dell'autorità pubblica già ai primi segnali di comportamenti violenti o ingiuriosi, può infatti efficacemente impedirne la degenerazione, evitando così anche di inserire il minore nel circuito della giustizia (penale) minorile.

?

Minori e social network

Il 23 febbraio il Garante per la protezione dei dati personali ha emanato un importante provvedimento relativo alla tutela della riservatezza, in particolare (ma non solo) dei minori nell'ambito dei social network. Il caso riguardava la pubblicazione, sul profilo Fb asseritamente "chiuso" di una donna, di due sentenze relative alla cessazione degli effetti civili del proprio matrimonio, nelle quali erano trattati aspetti riguardanti l'intimità della vita familiare concernenti, in particolare, la figlia minore (resa identificabile almeno nella cerchia degli "amici" della signora) e i suoi rapporti con il padre. Quest'ultimo riteneva tale pubblicazione lesiva della dignità della minore e ne richiedeva quindi la rimozione. Nel condividere la tesi del padre, in particolare, il Garante ha ritenuto irrilevante, ai fini del divieto di divulgazione "con qualsiasi mezzo" di notizie idonee a consentire l'identificazione di un minore coinvolto a qualsiasi titolo in procedimenti giudiziari, la distinzione tra profilo aperto e profilo chiuso nell'ambito del social network Facebook.

Si tratta di un'affermazione importante in quanto consente di evitare la denegatio tutelae altrimenti derivante dalla lettura restrittive delle norme del Codice privacy che, se applicate formalisticamente, avrebbero potuto indurre il Garante a non pronunciarsi sul caso, ritenendo che la circostanza

dell’avvenuta pubblicazione della sentenza in questione su di un profilo chiuso costituisse un trattamento per fini personali, come tale sottratto alle garanzie sancite dal Codice stesso.

In favore della propria decisione, il Garante ha anche richiamato l’opportunità di un’interpretazione delle norme alla luce dell’evoluzione tecnologica e della diffusione dei social network, strutturati per consentire comunicazione sistematica con estrema facilità. Ha inoltre osservato come non possa essere provata la natura chiusa del profilo e la sua accessibilità a un numero ristretto di “amici”, in ragione del fatto che esso è agevolmente modificabile, da “chiuso” ad “aperto” in ogni momento da parte del titolare, nonché della possibilità per qualunque “amico” ammesso al profilo stesso di condividere sulla propria pagina il post rendendolo, conseguentemente, visibile ad altri utenti (potenzialmente tutti gli utenti di Facebook). Si è quindi ritenuta la pubblicazione su Facebook di sentenze nelle quali erano citate minori, incompatibile con il divieto di pubblicazione “con qualsiasi mezzo” di notizie idonee a consentire l’identificazione di un minore coinvolto a qualsiasi titolo in procedimenti giudiziari (art. 50 del Codice) e con il divieto - cui soggiace “chiunque”- di diffusione dei dati idonei a rendere comunque identificabili, anche in via indiretta, i minori coinvolti e le parti di procedimenti in materia di famiglia (art. 52, c. 5 del Codice). E questo, anche considerando che l’estrema diffusività della divulgazione su internet aggrava notevolmente, rispetto a qualsiasi altro mezzo, la violazione dei diritti dell’interessato, anche perché le eventuali “regole” di privacy possono non essere applicate correttamente dall’utente o aggirate da navigatori esperti. I principi affermati in questo provvedimento – non limitati di per sé ai casi nei quali siano coinvolti minori – possono contribuire a rafforzare in misura significativa la tutela della dignità personale in rete, spesso pregiudicata da un uso poco consapevole dei social network.

Diritto all’oblio e condanne penali

Con decisione del 7 dicembre 2016, il Garante per la protezione dei dati personali ha riconosciuto il diritto alla deindicizzazione di notizie che, benché recenti, debbano tuttavia ritenersi obsolete perché non più adeguate agli sviluppi che la vicenda giudiziaria descritta abbia subito. Il diritto all’oblio potrebbe dunque esercitarsi anche a prescindere dal tempo trascorso, purché le notizie di cui si chiede la deindicizzazione forniscano un quadro non più aggiornato della persona cui si riferiscono, pregiudicandone la corretta rappresentazione.

Tale principio è stato affermato non solo in relazione a un’intervenuta archiviazione ma anche a una sentenza di “patteggiamento”, valorizzando altresì, rispetto a una pronuncia di condanna, il riconoscimento del beneficio della non menzione della sentenza nel casellario giudiziale. Con riferimento a tale ultimo aspetto, con decisione del 6 aprile, il Garante ha infatti precisato come tale beneficio possa essere di fatto vanificato dalla facile reperibilità in rete della notizia della condanna. Si tratta di decisioni importanti, in quanto improntate a un’interpretazione “forte” di quel diritto all’oblio ora codificato dal Regolamento generale e anticipato dalla sentenza della Corte di giustizia nel caso Costeja c. Google Spain del maggio 2014. L’affermazione del diritto alla deindicizzazione di notizie che, in ragione del mancato aggiornamento rispetto all’evoluzione che abbia caratterizzato la vicenda narrata, non possano più ritenersi esatte, a prescindere dal tempo trascorso, è infatti un principio di assoluto rilievo e denso di implicazioni soprattutto nel settore della cronaca giudiziaria. Ove il rischio maggiore prodotto dalle nuove tecnologie e, soprattutto, dalla combinazione tra rete e motori di ricerca, è proprio quello di schiacciare l’identità personale sulla veste di indagato, imputato,

condannato, assunta dall'interessato in un determinato momento. E questo, ignorando l'evoluzione che la vicenda giudiziaria (e quindi, di riflesso, la stessa identità dell'interessato) abbia subito.

Telemarketing

Nell'ambito del maxi-emendamento al ddl concorrenza su cui, il 3 maggio, il Governo ha posto e ottenuto al Senato la fiducia, è contenuta una norma sul telemarketing che rischia di legittimare rilevanti violazioni del diritto alla protezione dei dati personali dei cittadini. Essa, infatti, modificando il codice privacy, ammette la possibilità di effettuare chiamate promozionali in assenza del presupposto, altrimenti necessario, del consenso.

La norma ha una valenza generale: si riferisce infatti al "contatto" stabilito telefonicamente con l'"abbonato", dunque all'intestatario di una linea telefonica fissa o mobile (quest'ultima non suscettibile di iscrizione nel registro delle opposizioni salvo nei rarissimi casi di utenze inserite negli elenchi), a prescindere dalla sua inclusione nel registro stesso.

Dunque chiunque – sia iscritto nel registro o non lo sia perché intestatario di un'utenza mobile ovvero si sia comunque opposto alla ricezione di chiamate promozionali – potrà, in tal modo, essere destinatario di simili telefonate. L'unica, debolissima, tutela di cui disporrà sarà la manifestazione del proprio dissenso alla prosecuzione della chiamata in corso, senza tuttavia alcuna garanzia rispetto alle telefonate successive, potenzialmente infinite.

Si tratta di una norma che, dunque, liberalizza il telemarketing "selvaggio", non potendo in alcun modo ritenersi che essa si riferisca ai soli utenti di linee fisse non iscritte nel registro delle opposizioni..

Comprensibili, pertanto, le criticità manifestate in proposito dalle associazioni dei consumatori ma soprattutto dallo stesso Garante per la protezione dei dati personali, che ha auspicato una riforma della disciplina, anche nell'ambito dell'esame del ddl di riforma del registro delle opposizioni (A.S. 2603), attualmente all'esame della Commissione Lavori pubblici del Senato, che al contrario mira a rafforzare le garanzie dei cittadini rispetto al telemarketing. Al momento di licenziare queste bozze, risulta approvato in Commissione l'emendamento soppressivo della norma in questione. Scelta che, se confermata in Assemblea e nelle successive letture, consoliderebbe quella tendenza positiva recentemente riscontrata, anche a livello legislativo, nella materia della protezione dati.